Arjeh M. Cohen

Coxeter groups

Notes of a MasterMath course, Fall 2007

January 25, 2008

TU/e
Eindhoven
The Netherlands

Preface

These notes cover eight lectures on Coxeter groups, given at a MasterMath Course in Utrecht, Fall 2007. Each chapter corresponds to a lecture. The idea was to show some general group-theoretical techniques and, at the same time, the strength of these techniques in the particular case of Coxeter groups. Word rewriting, linear representations, and permutation representations are the main examples of the techniques I had in mind. The first of these techniques is exemplified by the beatiful proof of the automaticity of Coxeter groups, the gist of which appears in Chapter 7. The fact that Coxeter groups are linear (but very little representation theory) can be found in Chapter 3, where the famous reflection representation is treated. The main example of permutation representations for Coxeter groups uses the reflection representation and is concerned with root systems, in Chapter 4, a key component of the automaticity result. The role of Coxeter groups in other parts of mathematics comes to play in Chapters 6 on Weyl groups and 8 on buildings.

It was a pleasure working with the class. I am very grateful to Jos in't panhuis for his help with the exercises and his careful reading of the text.

Contents

1. Introduction

In this lecture we discuss how groups are represented and why Coxeter groups stand out among all groups. It is the introduction to a series of seven lectures on Coxeter groups, with an eye towards general group theory.

1.1 Representing a group

How do you describe an abstract group G in such a way that you can compute with it? In an abstract form, it is a set, often also denoted by G, a distinguished element $1 \in G$ and an associative map $G \times G \to G$, called multiplication, such that 1 is the identity and each element x has an inverse with respect to 1. We almost always write xy for the product of x and y in G. The inverse of an element $x \in G$ is unique and often denoted x^{-1}, so the inverse is a map $G \to G$. It is often useful to have the inverse map explicitly given.

The most straightforward approach to the question how to describe a group is the multiplication table. See Table 1.1 for an example in the case where the group is the direct product of two (cyclic) groups of order 2, known as Klein's Four group.

$\cdot$	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

Table 1.1. The multiplication table of Klein's Four group

But, if you go beyond small examples, this answer is not very satisfactory. For an infinite group, the data is infinite. Typically, a solution would be to give the set of elements, the multiplication, and the inverse map by algorithms. For a finite group, the amount of data needed for the multiplication table

is in the order of $|G|^3$, which puts a group like the Monster group M (see Theorem 1.7.1(v) for the significance of this group), of size

$$\begin{aligned}&2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71\\ &= 808017424794512875886459904961710757005754368000000000\\ &\approx 8 \cdot 10^{53},\end{aligned}$$

outside the scope of our planet, as the number of particles (say atoms) on earth is estimated to be smaller.

In this course, we will discuss three ways of describing groups more efficiently:

- as a presentation, by means of generators and relations
- as a permutation group, by means of generating permutations (for finite groups)
- as a linear group, by means of generating matrices

1.2 Finitely presented groups

An easy way to represent a group is by generators and relations. It has major disadvantages because questions like deciding whether two representatives stand for the same group element are hard, even impossible to answer in general. In order to define a presentation, we need the notion of a free group, which we will deal with more carefully in Lecture 2. For the time being we will work with the *free group* $\mathrm{F}(A)$ on an alphabet as follows. Consider the alphabet $A \cup A^{-1}$, where A^{-1} is the set of symbols a^{-1} disjoint from A, one for each $a \in A$. As a set, $\mathrm{F}(A)$ consists of all words in $A \cup A^{-1}$ without occurrences of the kind aa^{-1} or $a^{-1}a$ for $a \in A$. Such words will be called *reduced*. Multiplication on $\mathrm{F}(A)$ is given by concatenation followed by removal of all forbidden occurrences so as to obtain a reduced word, and in which the empty word 1 is the identity element. The fact that $\mathrm{F}(A)$ is a group requires a proof. This proof will be postponed till Lecture 2; it hinges on the uniqueness of the reduced word for a given element of $\mathrm{F}(A)$. Elements of $\mathrm{F}(A)$ are called words (on A).

Definition 1.2.1 A *group presentation* $\langle A \mid R \rangle$ is made up of a set A of *generators* and a set R of *relations*. Here a relation is an expression of the form $w_1 = w_2$, where w_1 and w_2 are elements of the free group $\mathrm{F}(A)$. The group $\langle A \mid R \rangle$ is then defined as the quotient group of the free group $\mathrm{F}(A)$ on the generating symbols from A by the normal subgroup generated by all $w_1 w_2^{-1}$ for each expression $w_1 = w_2$ occurring in R.

A group presentation $\langle A \mid R \rangle$ is said to be *finite* if both A and R are finite. It is said to be a *presentation of* G (or G is said to have presentation $\langle A \mid R \rangle$) if G is a group isomorphic to $\langle A \mid R \rangle$. The group is called *finitely presented* if it has a finite presentation.

Every group has a presentation. Not every group has a finite presentation; see Exercise 1.8.3.

Example 1.2.2 (Cyclic groups) A presentation for the cyclic group of infinite order, that is, the free group on one generator, is

$$\langle \{a\} \mid \{\} \rangle.$$

It is a presentation of the additive group $\mathbb{Z}^+$ of the integers.

Of course, no group has a unique presentation. Another presentation of the cyclic group of infinite order is

$$\langle \{a, b\} \mid \{b = 1\} \rangle.$$

Adding the relation $a^m = 1$, we find the cyclic group of order m:

$$\langle \{a\} \mid \{a^m = 1\} \rangle.$$

It is a presentation of the additive group $(\mathbb{Z}/m\mathbb{Z})^+$ of the integers modulo m.

Example 1.2.3 (Dihedral groups) Let $m \in \mathbb{N}$. By Dih_{2m} we denote the group with presentation

$$\langle \{a, b\} \mid \{a^2 = 1, b^2 = 1, (ab)^m = 1\} \rangle.$$

Using the braces to indicate sets becomes tiresome and is often deleted; so, to the above way of writing the group presentation, we prefer

$$\langle a, b \mid a^2 = 1, b^2 = 1, (ab)^m = 1 \rangle.$$

Set $c = ab$. (Note the ambiguity: the right hand side represents an element of $\mathrm{F}(A)$, but we often interpret it as an element of Dih_{2m}. To avoid ambiguity, we often specify in which group the identity is supposed to hold.) We claim that, as a set

$$\mathrm{Dih}_{2m} = \{a^i c^j \mid \{i \in \{0, 1\}, j \in \{0, 1, \ldots, m-1\}\}.$$

For, each a following a power of c can be commuted to the front:

$$c^k a = (ab)^k a = a(ba)^k = a(b^{-1}a^{-1})^k = a((ab)^{-1})^k = ac^{-k} = ac^{m-k},$$

so each element is of the form $a^i c^j$ for some $i, j \in \mathbb{N}$. Now, keeping into account that $a^2 = 1$ and $c^m = 1$, we see that there is no harm in restricting the values of i and j as in the claim.

The claim establishes that Dih_{2m} is a group of order at most $2m$. Is it of order precisely $2m$? And if so, how to prove it? The answer needs the following basic result and is given in Example 1.2.5.

Theorem 1.2.4 *Suppose $\phi : A \to G$ is a map from the alphabet A to the group G. Then ϕ can be uniquely extended to a group homomorphism $\phi : \mathrm{F}(A) \to G$. Let $\langle A \,|\, R\rangle$ be a group presentation such that $\phi(w_1) = \phi(w_2)$ is satisfied for each expression $w_1 = w_2$ in R. Then ϕ induces to a homomorphism of groups $\langle A \,|\, R\rangle \to G$.*

Proof. Let $\phi : A \to G$ be as stated. Put $\phi(a^{-1}) = \phi(a)^{-1}$ for each $a \in A$. If $v \in \mathrm{F}(A)$, then v is a reduced word $a_1 a_2 \cdots a_n$ for certain $a_i \in A \cup A^{-1}$, and we set

$$\phi(v) = \phi(a_1)\phi(a_2)\cdots\phi(a_n).$$

It is straightforward from the construction of $\mathrm{F}(A)$ that ϕ is a homomorphism of groups. For, if $b_1 b_2 \cdots b_m$ is a reduced word for $w \in \mathrm{F}(A)$, then $vw = a_1 \cdots a_{n-r} b_{r+1} \cdots b_m$, where a_{n-k} and b_{k+1} are each other's inverses for $k = 0, \ldots, r-1$, and r is maximal with this property. Then

$$\begin{aligned}
&\phi(vw)\\
&= \phi(a_1)\cdots\phi(a_{n-r})\phi(b_{r+1})\cdots\phi(b_m)\\
&= \phi(a_1)\cdots\phi(a_{n-r})\left(\phi(a_{n+1-r})\cdots\phi(a_n)\phi(b_1)\cdots\phi(b_r)\right)\phi(b_{r+1})\cdots\phi(b_m)\\
&= \left(\phi(a_1)\cdots\phi(a_{n-r})\phi(a_{n+1-r})\cdots\phi(a_n)\right)\left(\phi(b_1)\cdots\phi(b_r)\phi(b_{r+1})\cdots\phi(b_m)\right)\\
&= \phi(a_1\cdots a_n)\phi(b_1\cdot\cdots\cdot b_m)\\
&= \phi(v)\phi(w).
\end{aligned}$$

By the assumed behaviour of ϕ on the expressions from R, the elements $w_1 w_2^{-1}$ belong to $\operatorname{Ker}\phi$. But $\operatorname{Ker}\phi$ is a normal subgroup and so contains the normal subgroup N of $\mathrm{F}(A)$ generated by all $w_1 w_2^{-1}$ for $w_1 = w_2$ an expression in R. By the First Isomorphism Theorem, this means that ϕ factors through $\mathrm{F}(A)/N$; in other words, ϕ is the composition $\overline{\phi} \circ \pi$ of a homomorphism $\overline{\phi} : \mathrm{F}(A)/N \to G$ and the natural quotient map $\mathrm{F}(A) \to \mathrm{F}(A)/N$. Now $\overline{\phi}$ is the required homomorphism $\langle A \,|\, R\rangle \to G$. □

Example 1.2.5 (Dihedral group presentations) Let $m \in \mathbb{N}$, $m \geq 2$. By Sym_m we denote the group consisting of all permutations of $\{1, \ldots, m\}$, a set which we denote by $[m]$. The map $\tau_m : [m] \to [m]$ sending $i \in [m]$ to $m+1-i$ is an involution, that is, an element of order 2, in Sym_m. In the subgroup of Sym_m generated by τ_{m-1} and τ_m, denoted $\langle \tau_{m-1}, \tau_m \rangle$, we have the following relations.

$$\tau_m^2 = 1,\ \tau_{m-1}^2 = 1,\ (\tau_m \tau_{m-1})^m = 1.$$

The first two equations reflect that τ_m and τ_{m-1} are involutions, and the third relations follows from $\tau_m \tau_{m-1} = (1, 2, \ldots, m)$.

In other words, τ_m and τ_{m-1} satisfy the relations for a and b as given in Example 1.2.3. By Theorem 1.2.4, there is a homomorphism of groups

$$\overline{\phi} : \mathrm{Dih}_{2m} \to \langle \tau_m, \tau_{m-1} \rangle$$

determined by $\overline{\phi}(a) = \tau_m$ and $\overline{\phi}(b) = \tau_{m-1}$. As τ_m and τ_{m-1} are images of $\overline{\phi}$, the whole group $D = \langle \tau_m, \tau_{m-1} \rangle$ is in the image of Dih_{2m} under $\overline{\phi}$, so $|\mathrm{Dih}_{2m}| \geq |D|$. But D contains the cycle $\tau_m\tau_{m-1}$ of order m, and the involution τ_m outside $\langle \tau_m\tau_{m-1} \rangle$. Therefore, $|D| \geq 2m$, so $|\mathrm{Dih}_{2m}| \geq 2m$. But we already know $|\mathrm{Dih}_{2m}| \leq 2m$; see Example 1.2.3. The conclusion is that both Dih_{2m} and D have order $2m$ and that $\overline{\phi}$ is an isomorphism. This is an efficient presentation for the group of permutations $\langle \tau_m, \tau_{m-1} \rangle$.

Remark 1.2.6 According to the Atlas of Finite Simple Groups, [9], a presentation for the Monster group M is

$$\langle a, b, u \mid a^2 = 1, b^3 = 1, (ab)^{29} = 1, u^{50} = 1, \\ (au^{25})^5 = 1, (ab^2(b^2a)^5b(ab)^5b)^{34} = 1; u = (ab)^4(abb)^2 \rangle.$$

As the last relation expresses u as a word in the generators a and b, it follows from this presentation that M is a quotient of $\mathrm{F}(\{a, b\})$, or, equivalently (by Theorem 1.2.4), generated by two elements. Being non-Abelian, M cannot be generated by a single element.

On the one hand, this presentation is indeed efficient in the sense that it needs little storage space on a computer. On the other hand, it is not clear how it can help to convince you that we are dealing with a finite simple group of the order indicated in Section 1.1. Even for the trivial group there are many complicated presentations; see Exercise 1.8.2 for a moderate example.

We present another application of Theorem 1.2.4.

Proposition 1.2.7 *Let S_n be the alphabet $\{s_1, \ldots, s_n\}$ and consider the set T_n of relations*

$$\begin{aligned} s_i^2 &= 1 \\ s_i s_j &= s_j s_i \quad \text{if} \quad |i - j| > 1 \\ s_i s_j s_i &= s_j s_i s_j \quad \text{if} \quad |i - j| = 1 \end{aligned}$$

Then the map $S_n \to \mathrm{Sym}_{n+1}$ given by $s_i \mapsto (i, i+1)$ extends to a presentation of Sym_{n+1} by $\langle S_n \,|\, T_n \rangle$.

Proof. Consider the map $\phi : S_n \to \mathrm{Sym}_{n+1}$ given by $\phi(s_i) = (i, i+1)$ for $i \in [n]$. It is not hard to verify that the relations listed in the statement hold for the images of s_i under ϕ in Sym_{n+1}.

By Theorem 1.2.4 ϕ determines a group homomorphism $\phi : \langle S_n \,|\, T_n \rangle \to \mathrm{Sym}_{n+1}$. It is easy to verify that Sym_{n+1} is generated by $\phi(S_n)$. So ϕ is surjective. Now $|\mathrm{Sym}_{n+1}| = (n+1)!$, so, for a proof that ϕ is an isomorphism, it suffices to show $|\langle S_n \,|\, T_n \rangle| \leq (n+1)!$ If $n = 1$, the group $\langle S_1 \,|\, T_1 \rangle = \langle s_1 \,|\, s_1^2 = 1 \rangle$ is cyclic of order 2, as required. We proceed by induction on n.

Suppose $n > 1$. We claim that each element x of $\langle S_n \,|\, T_n \rangle$ can be represented by a word $s_k s_{k+1} \cdots s_n s_{n+1} w$ with $w \in \langle s_1, \ldots, s_n \rangle$. Once this is

established, we note that w lies in a quotient of the group with presentation $\langle S_{n-1} \,|\, T_{n-1}\rangle$; so, by the induction hypothesis, there are most $n!$ different choices for w. Left of w the choices for x are limited by $k \in [n+1]$. Consequently, there are at most $(n+1) \cdot n! = (n+1)!$ words representing distinct elements of $\langle S_n \,|\, T_n\rangle$, so $|\langle S_n \,|\, T_n\rangle| \leq (n+1)!$, as required.

It remains to prove the claim. Let $x \in \langle S_n \,|\, T_n\rangle$. Consider a word in $\mathrm{F}(S_n)$ representing x. If s_{n+1} does not occur, there is nothing to show. Suppose therefore that $x = vs_k s_{k+1} \cdots s_n s_{n+1} w$ is an expression of minimal length for x with w free of s_{n+1} and k and the length of v as small as possible (in this order). If v is the empty word, we are done. Otherwise we can write $v = us_j$ for some $j \in [n]$. If $j < k-1$, then

$$vs_k \cdots s_n w = us_j s_k \cdots s_n w = us_k \cdots s_n s_j w,$$

with $s_j w \in \langle s_1, \ldots, s_n\rangle$ contradicting the minimality of v.

If $j = k$, we can reduce the length of the word for x by removing the double occurrence of s_k (and obtain the word uv for x), as $s_k^2 = 1$ belongs to S_n. This contradicts the minimality of the length of our representative word.

If $j = k+1$, we have $s_{k+1}s_k s_{k+1} \cdots s_n s_{n+1} = s_k s_{k+1} s_k s_{k+2} \cdots s_n s_{n+1} = s_k s_{k+1} s_{k+2} \cdots s_n s_{n+1} s_k$ and so x is represented by $us_k s_{k+1} s_{k+2} \cdots s_n s_{n+1} s_k w$, with $s_k w \in \langle s_1, \ldots, s_n\rangle$, again contradicting the minimality of v.

Suppose therefore, $j > k+1$. Then

$$\begin{aligned} s_j s_k s_{k+1} \cdots s_n s_{n+1} &= s_k s_{k+1} \cdots s_j s_{j-1} s_j s_{j+1} \cdots s_n s_{n+1} \\ &= s_k s_{k+1} \cdots s_{j-1} s_j s_{j-1} s_{j+1} \cdots s_n s_{n+1} \\ &= s_k s_{k+1} \cdots s_{j-1} s_j s_{j+1} \cdots s_n s_{n+1} s_{j-1} \\ &= s_k s_{k+1} \cdots s_n s_{n+1} s_{j-1} \end{aligned}$$

and we can reason as in the previous case. Thus, v must be the empty word; this proves the claim. □

Example 1.2.8 The group $\mathrm{SL}(\mathbb{Z}^2)$ consists of all 2×2 matrices with integer entries and determinant 1. It is generated by the following two interesting elements (proving this is Exercise 1.8.6).

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

The center of this group consists of the scalar multiplications by 1 and -1, and so has order 2. The quotient group of $\mathrm{SL}(\mathbb{Z}^2)$ by this center is denoted $\mathrm{PSL}(\mathbb{Z}^2)$. Denote by A and B the images of the above two matrices in $\mathrm{PSL}(\mathbb{Z}^2)$. Obviously, $A^2 = 1$ and $B^3 = 1$, so there is a group homomorphism

$$\langle a, b \,|\, a^2 = 1, b^3 = 1\rangle \to \mathrm{PSL}(\mathbb{Z}^2)$$

sending a to A and b to B. Surprisingly, this homomorphism is an isomorphism. The proof of this statement will not be given here.

1.3 Permutation groups

The group of all permutations of a set X is denoted by $\mathrm{Sym}(X)$ and called the symmetric group on X. We have already encounterd Sym_n, which is $\mathrm{Sym}([n])$ in the current notation. If X is infinite, we can still speak of $\mathrm{Sym}(X)$ as the group of all bijections of X, but things are more subtle, for instance because of the existence of the proper normal subgroup $\mathrm{FSym}(X)$ of $\mathrm{Sym}(X)$ consisting of all finitary permutations, that is, all permutations moving only a finite number of elements of X.

Definition 1.3.1 Let G be a group and X a set. A *permutation representation* of G on X is a group homomorphism $\alpha : G \to \mathrm{Sym}(X)$. In this case, X is referred to as a *G-set*. Such a permutation representation is called *faithful* if α is injective. In this case, G or rather its isomorphic image $\alpha(G)$ is called a *permutation group*. The size of X is called the *degree* of the representation.

Let $x \in X$. The set $\{\alpha(g)x \mid g \in G\}$ is called the *G-orbit*, notation Gx, of x in X. The permutation representation is called *transitive* if there is only one G-orbit in X. The *stabilizer* of x in G, notation G_x, is the subgroup $\{g \in G \mid \alpha(g)x = x\}$ of G.

The following theorem shows how to construct permutation representations on the collection of cosets gH ($g \in G$) of H in G.

Theorem 1.3.2 (Cayley's Theorem) *If G is a group and H is a subgroup of G, then left multiplication, considered as the map $L_H : G \to \mathrm{Sym}(G/H)$ given by $L_H(g) = (kH \mapsto gkH)$, is an homomorphism of groups $G \to \mathrm{Sym}(G/H)$. Its kernel is the biggest normal subgroup of G contained in H, that is, $\bigcap_{g\in G} gHg^{-1}$.*

Proof. This is Exercise 1.8.7. □

As a consequence, every finite group G can be viewed as a group of permutations. For, take G to be any finite group and $H = 1$, the trivial group (again, we leave out braces and write 1 instead of $\{1\}$). Then, as sets G and $G/1$ can be identified and the kernel of L_1 is the trivial subgroup of G. By the First Isomorphism Theorem, the image of G under L_1 in $\mathrm{Sym}(G)$ is isomorphic to G, so we have an embedding (that is, an *injective homomorphism*) of G in $\mathrm{Sym}(G)$.

For the cyclic group of prime order p, there is no smaller degree than p for a faithful permutation representation. For, the group has no nontrivial proper subgroups. See Exercise 1.8.8.

Remark 1.3.3 In terms of size, the embedding $G \to \mathrm{Sym}(G)$ is not very impressive: the degree is as large as the group itself. At the same time, we see that, for a simple group G, we can take H to be any proper subgroup. For the Monster group M, the best choice is the centralizer of a particular involution,

a subgroup H related to the Baby Monster, another group appearing in Theorem 1.7.1, for which the size of M/H (known as the *index* of H in M) is $97,239,461,142,009,186,000 \approx 9.7 \cdot 10^{19}$. This number is still too big for treatment by computer.

For computational purposes, permutation groups are given by means of generating permutations. If B is a set of permutations on X, then $\langle B \rangle$ denotes the subgroup of $\mathrm{Sym}(X)$ generated by B; it can be constructed by starting from B, adding 1, and successively adding all products and inverses of elements already obtained.

1.4 Linear groups

The general linear group on a vector space V, denoted $\mathrm{GL}(V)$, will be introduced in Exercise 1.8.1. If V is of dimension n over the field $\mathbb{F}$, this group can be explicitly described as the set of all square matrices of size n and nonzero determinant with entries in $\mathbb{F}$.

Definition 1.4.1 A *linear representation* of a group G is a group homomorphism $G \to \mathrm{GL}(V)$, where V is a vector space. Here $\mathrm{GL}(V)$ is the group of all invertible linear transformations from V to V. Our interest is in finite-dimensional vector spaces. If V is known, we also speak of a linear representation on V. If we want to specify the field $\mathbb{F}$ underlying V, we talk about linear representations over $\mathbb{F}$. In case $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$, we speak of *real* and *complex* representations, respectively. The dimension $\dim V$ of V is called the *degree* of the representation.

Example 1.4.2 Consider the following real 2×2-matrices.

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} \sin\frac{2\pi}{m} & \cos\frac{2\pi}{m} \\ \cos\frac{2\pi}{m} & -\sin\frac{2\pi}{m} \end{pmatrix}$$

These matrices satisfy the following relations:

$$A^2 = 1, \quad B^2 = 1, \quad (AB)^m = 1.$$

In particular, A and B are invertible linear transformations and generate the subgroup $\langle A, B \rangle$ of $\mathrm{GL}(\mathbb{R}^2)$, the group of all real invertible 2×2-matrices. By Theorem 1.2.4, there is a homomorphism $\mathrm{Dih}_{2m} \to \langle A, B \rangle$ sending a to A and b to B. By an argument similar to the one for $\langle \tau_n, \tau_{n-1} \rangle$ in Example 1.2.5, we can argue that $\langle A, B \rangle$ has order at least $2m$, and derive from this that Dih_{2m} is isomorphic to $\langle A, B \rangle$. In particular, Dih_{2m} can also be represented as a group of invertible real matrices.

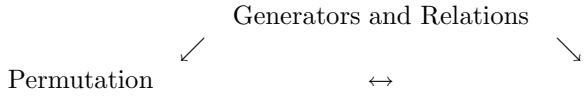
Remark 1.4.3 Every finite group can be represented as a linear group. This follows from the results in Section 1.5. Another proof follows from the construction of the group algebra; see Exercise 1.8.11. The minimal degree of a faithful real representation of the Monster is $196,883$.

1.5 Transitions between representations

If G is a finite group given by a set of generating permutations or matrices, its multiplication table can be determined (at least, in principle), and so a presentation by means of generators would be $\langle G \,|\, T\rangle$, where T consists of all equations $gh = k$ for $g, h, k \in G$: the multiplication table.

Thus there are effective, albeit very inefficient, methods of finding a presentation by generators and relations when given a permutation or linear representation for a given finite group G.

In this section, we discuss the other transitions between the three ways of representing a group. These are visualized in the following triangle.



By Theorem 1.2.4 Let $G = \langle A \,|\, R\rangle$ be given by means of generators and relations. Then there are several techniques for trying to build up the permutation representation of G on the cosets in G of a subgroup H specified by generators. In general, there is very little we can say about H and there is no guarantee that $\bigcap_{g\in G} gHg^{-1}$ is trivial, so it may well be that the homomorphism $G \to \mathrm{Sym}(G/H)$ is not injective; see Cayley's Theorem 1.3.2. But, even more seriously, there is no algorithm that allows us to determine even if G is trivial on the basis of A and R alone. The only positive aspect is that, if we know G is finite, it will take a finite number of computational steps to determine the image of G in $\mathrm{Sym}(G/H)$. The process of determining G/H is called *coset enumeration*. It has been discussed in the MasterMath lectures on Computer Algebra. Here we only give a very simple example.

Example 1.5.1 Let $m \in \mathbb{N}$, $m > 1$. Consider the dihedral group Dih_{2m} introduced in Example 1.2.3, with presentation

$$\langle a, b \,|\, a^2 = 1, b^2 = 1, (ab)^m = 1\rangle.$$

Let H be the subgroup of Dih_{2m} generated by b. So H has order 1 or 2. Coset enumeration starts with the coset, labelled 1, corresponding to H. It is an attempt to construct the Schreier graph $\Sigma(\mathrm{Dih}_{2m}, H, A)$, whose vertex set is Dih_{2m}/H and in which the ordered pair (gH, kH) of cosets is an edge labelled x for $x \in A$ with $xg \in kH$. So, in our example, (H, aH) is an edge labeled a, so the vertex aH is labelled 2 and our Schreier graph under construction

is the single ordered edge $(1, 2)$. To be precise, we have no guarantee as yet that the vertices 1 and 2 coincide; in other words, at some point we need to exclude $a \in H$. But the idea of coset enumeration is to proceed building the graph, while checking the relations regularly and collapsing the graph if vertices will coincide as a result. An easy instance is $bH = H$, leading to the loop $(1, 1)$ with label b. Another easy instance is a^2H, which should collapse with H as $a^2 = 1$. In fact, as a and b are involutions, the Schreier graph at hand may be viewed as having undirected edges: if (gH, kH) is an edge labelled x, then so is (kH, gH).

Next, consider neighbors of 2. Only left multiplication by b might give a new coset $3 = b2 = ba1$. If $m = 2$, then $ba1 = ab1 = a1$, and the Schreier graph completes on the vertex set [2].

Suppose $m = 3$. Proceed with a again to get $4 = aba1$. Now $aba1 = bab1 = ba1 = 3$, so the Schreier graph completes on the vertex set [3].

In general, the will find m nodes, labelled $1, 2, \ldots, m$ with $ai = i + 1$ if i is odd, $bi = i + 1$ if i is even. At the end, for m even, $bm = (ba)^{m/2}1 = (ab)^{m/2}1 = (ab)^{m/2-1}a1 = m$ and, for m odd, $am = a(ba)^{(m-1)/2}1 = (ab)^{(m+1)/2}1 = (ba)^{(m-1)/2}1 = m$. This completes a graph as depicted in Figure 1.1.

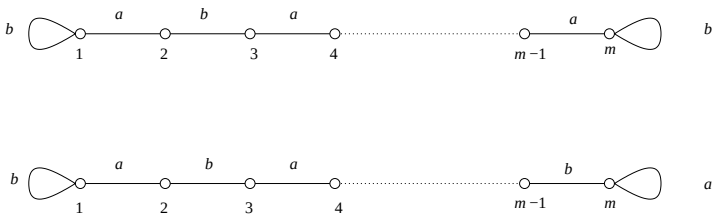


Fig. 1.1. The Schreier graph $\Sigma(\mathrm{Dih}_{2m}, \langle b\rangle, \{a, b\})$ for m even and m odd

Now read off the permutations representing the actions of a and b from the Schreier graph. For m even:

$$a \mapsto (1, 2)(3, 4) \cdots (m - 1, m)$$
$$b \mapsto (2, 3)(4, 5) \cdots (m - 2, m - 1)$$

and for m odd:

$$a \mapsto (1, 2)(3, 4) \cdots (m - 2, m - 1)$$
$$b \mapsto (2, 3)(4, 5) \cdots (m - 1, m)$$

These permutations are easily verified to satisfy the defining relations of Dih_{2m} and hence, by Theorem 1.2.4, we have a group homomorphism $G \to \mathrm{Sym}([m])$. The image of H under this homomorphism is of order 2 and so H itself has that order. Finally, the order of Dih_{2m} is the number m of cosets of

H in G multiplied by the order of H, which is 2. The result, $|\mathrm{Dih}_{2m}| = 2m$, has also been established in Example 1.2.5.

Each finite group G is isomorphic to a real linear group, that is, a group of real invertible matrices of finite dimension. To see this, use Cayley's Theorem 1.3.2. It enables us to assume that G is a subgroup of $\mathrm{Sym}(X)$. Now take the real vector space $V = \mathbb{R}^X$ of all real functions $X \to \mathbb{R}$. Observe that V has dimension $|X|$. For $g \in G$ and $f \in V$, write gf for the real function $X \to \mathbb{R}$ given by

$$(gf)x = f(g^{-1}x) \qquad (x \in X),$$

and set $\rho_g = (f \mapsto gf)$.

Proposition 1.5.2 *For every permutation group G on X, the map $g \mapsto \rho_g$ is a faithful homomorphism of groups $G \to \mathrm{GL}(V)$.*

Proof. First, note that ρ_g is a linear map $V \to V$. Indeed, if $f_1, f_2 \in V$ and $\alpha, \beta \in \mathbb{R}$, then, for each $x \in X$,

$$\begin{aligned}(\rho_g(\alpha_1 f_1 + \alpha_2 f_2))x &= (g(\alpha_1 f_1 + \alpha_2 f_2))x = (\alpha_1 f_1 + \alpha_2 f_2)(g^{-1}x)\\ &= \alpha_1(f_1(g^{-1}x)) + \alpha_2(f_2(g^{-1}x))\\ &= \alpha_1((gf_1)x)) + \alpha_2((gf_2)x)\\ &= (\alpha_1(gf_1))x + (\alpha_2(gf_2))x = ((\alpha_1(gf_1)) + (\alpha_2(gf_2)))x\\ &= (\alpha_1\rho_g(f_1) + \alpha_2\rho_g(f_2))x\end{aligned}$$

and so $\rho_g(\alpha_1 f_1 + \alpha_2 f_2) = \alpha_1\rho_g(f_1) + \alpha_2\rho_g(f_2)$.

Next, observe that $g \mapsto \rho_g$ is a homomorphism of groups. For, $(\rho_{g_1g_2}f)x = ((g_1g_2)f)x = f((g_1g_2)^{-1}x) = f(g_2^{-1}(g_1^{-1}x)) = (g_2f)(g_1^{-1}x) = (g_1(g_2f))x = (\rho_{g_1}\rho_{g_2}f)x$ whenever $g_1, g_2 \in G$, $f \in V$ and $x \in X$, which shows that $\rho_{g_1g_2} = \rho_{g_1}\rho_{g_2}$.

Finally we verify that the homomorphism is faithful. Suppose $g \in \mathrm{Ker}\,\rho$, that is, ρ_g is the identity on V. For $x \in X$, let δ_x be the function in V with value 1 on x and value 0 on all points distinct from x. Then $\delta_x(y) = \rho_g\delta_x(y) = \delta_x(g^{-1}y)$ for all $y \in X$, which forces $gy = y$ for all $y \in X$. In particular, $g = 1$, which shows $\mathrm{Ker}\,\rho = 1$. □

The dimension of the representation space is equal to $|X|$. If G is infinite, we can still find infinite-dimensional representations this way.

Suppose that G is a subgroup of $\mathrm{GL}(V)$ for some finite-dimensional complex vector space V. Can we turn G into a permutation group? Of course, we could use Cayley's Theorem directly. But a more natural approach would be to pick a vector $v \in V$ and study its orbit $Gv = \{gv \mid g \in G\}$. Recall from basic group theory that the stabilizer in G of a vector v in V is the group $G_v = \{g \in G \mid gv = v\}$.

Proposition 1.5.3 *Let G be a finite subgroup of $\mathrm{GL}(V)$ for some vector space V. Then there is a finite G-invariant subset X of V such that the map $G \to \mathrm{Sym}(X)$ obtained by restricting each $g \in G$ to X is a faithful permutation representation of G.*

Proof. If V is finite-dimensional, simply take a basis B of V and consider the union of B and all its translates under G, that is $\bigcup_{g\in G} gB$.

For V of arbitrary dimension, pick a nonzero vector $v \in V$. The permutation representation of G on Gv is equivalent to left multiplication on the cosets of G_v in G. The kernel of this representation is $K_v = \bigcap_{h\in G} hG_vh^{-1}$. If K_v is the trivial subgroup of G, then the homomorphism $G \to \mathrm{Sym}(Gv)$ is injective and G is a permutation group on Gv. Otherwise, there is a vector $v_1 \in V$ moved by K_v. Now take $X = Gv \cup Gv_1$. The kernel of the action $G \to \mathrm{Sym}(X)$ is strictly contained in K_v. As G is finite, recursion will lead to a finite set T of vectors such that the kernel of the action of G on $X = \bigcup_{t\in T} Gt$ is trivial. □

In a real vector space V we can even find a copy of the regular representation, as the set $V \setminus \bigcup_{g\in G\setminus\{1\}} C_V(g)$ is non-empty. To see this, observe that each fixed point set $C_V(g) = \{v \in V \mid gv = v\}$ for nontrivial $g \in G$ is a proper subspace of V.

1.6 Coxeter groups

Although presentations in general can be very difficult, particular kinds of presentations can be very convenient. Our lectures will be primarily concerned with the following set of presentations.

Definition 1.6.1 Let $M = (m_{ij})_{1\le i,j\le n}$ be a symmetric $n \times n$ matrix with entries from $\mathbb{N} \cup \{\infty\}$ such that $m_{ii} = 1$ for all $i \in [n]$ and $m_{ij} > 1$ whenever $i \neq j$. The *Coxeter group* of type M is the group

$$W(M) = \langle \{s_1, \ldots, s_n\} \mid \{(s_is_j)^{m_{ij}} = 1 \mid i, j \in [n],\ m_{ij} < \infty\}\rangle$$

We often write S instead of $\{s_1, \ldots, s_n\}$ and, if no confusion is imminent, W instead of $W(M)$. The pair (W, S) is called the *Coxeter system* of type M.

Example 1.6.2 The two lowest rank cases lead to some familiar groups and one new group.
(i). If $n = 1$, then $M = (1)$ and $W(M) = \langle s_1 \mid s_1^2 = 1\rangle$, the cyclic group of order 2.
(ii). If $n = 2$, then $M = \begin{pmatrix} 1 & m \\ m & 1 \end{pmatrix}$ and $W(M) = \mathrm{Dih}_{2m}$ for some $m \in \mathbb{N} \cup \{\infty\}$. The Coxeter matrix is indicated by $\mathrm{I}_2(m)$. For $m = 2$, this is the Klein Four group of Table 1.1. For $m = \infty$, this is a new group, called the *infinite dihedral group.*

Example 1.6.3 The presentation of Sym_{n+1} in Proposition 1.2.7 can be recast as follows. By A_n we denote the Coxeter matrix

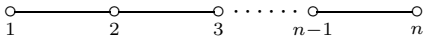
$$\begin{pmatrix} 1 & 3 & 2 & 2 & \cdots & \cdots & 2 \\ 3 & 1 & 3 & 2 & \cdots & \cdots & 2 \\ 2 & 3 & 1 & 3 & \cdots & \cdots & 2 \\ 2 & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 2 & \cdots & \cdots & 3 & 1 & 3 & 2 \\ 2 & \cdots & \cdots & 2 & 3 & 1 & 3 \\ 2 & \cdots & \cdots & 2 & 2 &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

of square size n. Then $W(\mathrm{A}_n)$ is a presentation of Sym_{n+1}. (Note that we blur the distinction between presentation and group.)

For $n = 2$, the Coxeter matrix A_2 coincides with $\mathrm{I}_2(3)$, and so $\mathrm{Sym}_3 \cong \mathrm{Dih}_6$.

Notation 1.6.4 The Coxeter matrix $M = (m_{ij})_{1 \leq i,j \leq n}$ is often described by a labelled graph $\Gamma(M)$ whose vertex set is $[n]$ and in which two nodes i and j are joined by an edge labeled m_{ij} if $m_{ij} > 2$. If $m_{ij} = 3$, then the label 3 of the edge $\{i, j\}$ is often omitted. If $m_{ij} = 4$, then instead of the label 4 at the edge $\{i, j\}$ one often draws a double bond. This labelled graph is called the *Coxeter diagram* of M.

The data stored in the Coxeter matrix M can be reconstructed from the Coxeter diagram, and so the Coxeter diagram and the Coxeter matrix can be identified. For instance, the diagram of A_n is

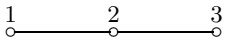
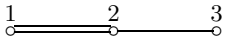
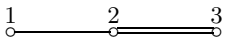
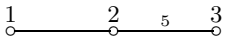
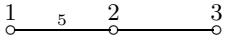


.

Example 1.6.5 The Platonic solids in real Euclidean space are closely linked to Coxeter groups. The automorphism groups of these Platonic solids, in some sense, are Coxeter groups. In the course of our lectures, it will be clear how the Platonic solids can be brought forward from the presentations defining the corresponding Coxeter groups. Here is a taste of what will happen. Let M be one of the matrices from Table 1.2.

Let $W = W(M)$ and set $H = \langle s_2, s_3 \rangle$. By enumeration of cosets we find W/H to have the same number of elements as the corresponding Platonic solid has vertices. Now define a graph on W/H by stipulating that the cosets gH and kH are adjacent whenever $k^{-1}g \in Hs_1H$. Observe that this relation is indeed symmetric, so it defines a graph. This graph is called the Cayley graph $\Gamma(W, H, \{s_1\})$. More generally, for a subgroup H of a group G and a subset S equal to $S^{-1} = \{s^{-1} \mid s \in S\}$, we can defined $\Gamma(G, H, S)$ similarly. Notice the difference with the Schreier graph. The group W acts as a group of automorphisms on the Cayley graph. In general, this is not the case for the Schreier graph.

Table 1.2. Coxeter diagrams related to Platonic solids

Platonic solid	Coxeter diagram	diagram notation
tetrahedron		A_3
cube		
octahedron		B_3
icosahedron		H_3
dodecahedron		

The Cayley graph can also be obtained from the Platonic solid by calling two vertices adjacent if they are distinct and lie on a common edge of the solid. Thus, the incidence structure of vertices, edges, and —with a little more thought— also the faces of the Platonic solid can be fully reconstructed from the Coxeter group.

Figure 1.2 shows the relationship between the Cayley graph $\Gamma = \Gamma(W, 1, S)$, for W of type B_3 and the cube P. A vertex of Γ is visualized as a point in the face of the cube P to which it belongs and nearest to the edge and vertex of P to which it belongs. It is joined by a dashed line to the unique Cayley vertex in the same face with the same nearest edge of P. It is joined by a dotted line to the unique Cayley vertex in the same face with the same nearest vertex, and with a full line to the unique Cayley vertex belonging to the same vertex and edge of P. Not all vertices are drawn: only those on the three visible faces of P.

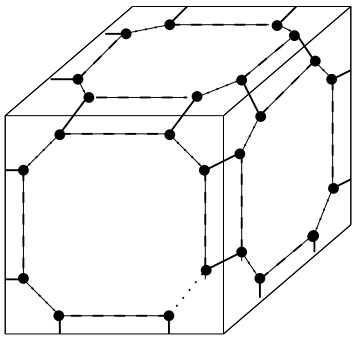


Fig. 1.2. The Cayley graph $\Gamma(W, 1, S)$ for W of type B_3 drawn on the cube.

Example 1.6.6 The Coxeter groups appearing in Example 1.6.5 are all finite. Table 1.3 lists some Coxeter diagrams with infinite Coxeter groups related to regular tilings of the plane.

Table 1.3. Coxeter diagrams related to planar tilings

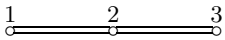
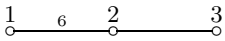
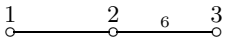
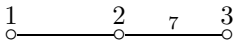
$\mathbb{E}^2$ tiling	Coxeter diagram	diagram notation
quadrangles		$\widetilde{\mathrm{B}}_2$
hexagons		$\widetilde{\mathrm{G}}_2$
triangles		

Figure 1.3 shows a regular tiling of the Euclidean plane by triangles.

Example 1.6.7 Besides tilings of the Euclidean plane, regular examples of the hyperbolic plane can also be produced by means of Coxeter groups. For instance, the Coxeter diagram



leads to a Coxeter group whose Cayley graph can be represented in the hyperbolic plane as depicted in Figure 1.4.

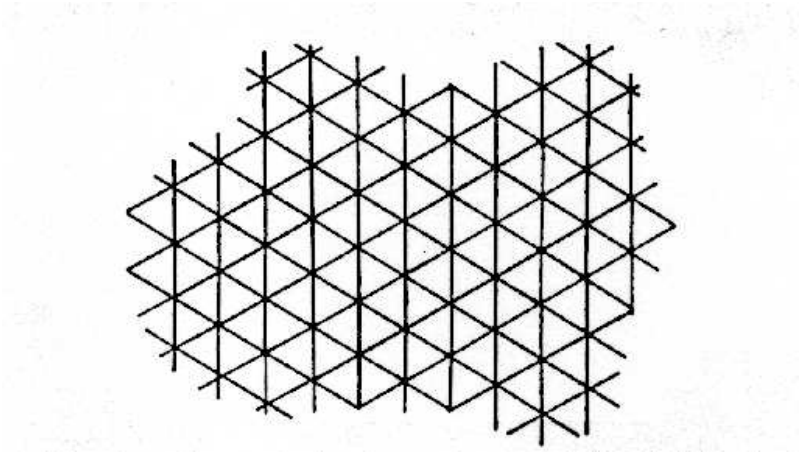


Fig. 1.3. Tiling by triangles

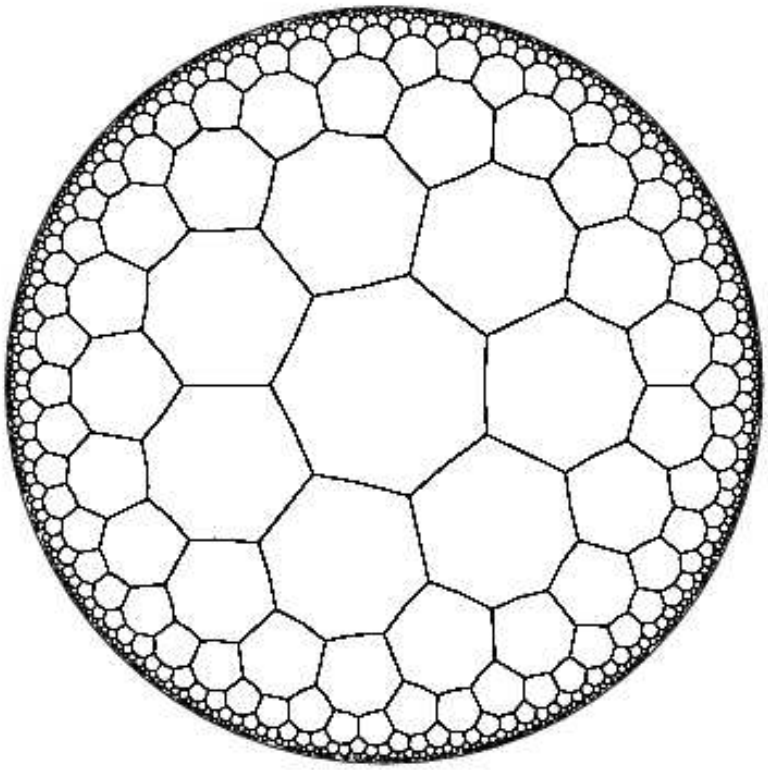


Fig. 1.4. Hyperbolic tiling by heptagons

1.7 Why Coxeter groups?

Coxeter groups turn out to be a very interesting class of groups. They behave very nicely in many respects; we name three.

1. Coxeter groups have nice solutions to the word problem. The *word problem* is the quest for an algorithm that decides whether two words in the generators of a presentation represent the same element in the group. For finitely presented groups in general, this problem cannot be solved by an algorithm. This topic will be addressed in Lectures 2 and 8.
2. Coxeter groups have faithful linear representations as groups generated by reflections. Among the groups occurring in this way are all real finite linear groups generated by reflections. Some of these groups are groups of symmetries of the regular polytopes in Euclidean space. We will prove the faithfulness in Lecture 3, classify the finite Coxeter groups in Lecture 6, and discuss further remarkable properties of the reflection representation in Lecture 7.

3. There are abstract analogues of the regular polytopes as discussed in Section 1.6 for each of the Coxeter groups, in the guise of combinatorial geometries built from the presentation; they possess dazzlingly beautiful and simple properties. Some aspects will appear in Lectures 4 and 5.

Besides beauty, their significance for other major results in mathematics, such as the classification of complex simple Lie algebras, of Lie groups and of algebraic groups motivates our choice of Coxeter groups as a topic for this course. To illustrate this, we present (without a shred of proof—the proof occupies more than 15,000 journal pages) the most important result in finite group theory that we know.

Recall that a simple group is a group whose only normal subgroups are the group itself and the trivial subgroup. The names of the groups occurring in the conclusion are not important for an understanding of the gist of the result. If N is a proper nontrivial normal subgroup of G, then G can be rebuilt from the groups N and G/N together with a prescription of how to piece these two parts together. By recursion, this leads us to the smallest building blocks: the simple groups.

Theorem 1.7.1 (Classification of Finite Simple Groups) *Every finite simple group is isomorphic to (at least) one of the following groups.*

(i) *A cyclic group of prime order*
(ii) *An alternating group* Alt_n *for some* $n \geq 5$
(iii) *The nonabelian simple section of a Chevalley group* $\mathrm{A}_{n-1}(q) = \mathrm{SL}(n,q)$ *for* $n \geq 3$ *and* $(n,q) \neq (2,2), (2,3)$, $\mathrm{B}_n(q) = \mathrm{O}(2n+1,q)$ *for* $n \geq 2$, $\mathrm{C}_n(q) = \mathrm{Sp}(2n,q)$ *for* $n \geq 3$, $\mathrm{D}_n(q) = \mathrm{O}^+(2n,q)$ *for* $n \geq 4$, $\mathrm{E}_6(q)$, $\mathrm{E}_7(q)$, $\mathrm{E}_8(q)$, $\mathrm{F}_4(q)$, $\mathrm{G}_2(q)$
(iv) *The nonabelian simple section of a twisted Chevalley group* ${}^2\mathrm{A}_{n-1}(q) = \mathrm{U}(n,q)$ *for* $n \geq 3$, ${}^2\mathrm{B}_2(2^{2m+1})$ *for* $m \geq 1$, ${}^2\mathrm{D}_n(q) = \mathrm{O}^-(2n,q)$ *for* $n \geq 4$, ${}^3\mathrm{D}_4(q)$, ${}^2\mathrm{E}_6(q)$, ${}^2\mathrm{F}_4(2^{2m+1})$ *for* $m \geq 0$, ${}^2\mathrm{G}_2(3^{2m+1})$ *for* $m \geq 1$
(v) *A sporadic group* M_{11}, M_{12}, M_{22}, M_{23}, M_{24}, J_2, Suz, HS, McL, Co_3, Co_2, Co_1, He, Fi_{22}, Fi_{23}, Fi'_{24}, HN, Th, B, M, J_1, O′N, J_3, Ly, Ru, J_4

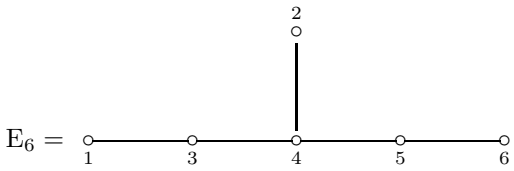
The series occurring in (i) and (ii) are the elementary examples of finite simple groups, with which you have already made acquaintance. The 26 groups listed in (v) are quite sensational, but we will put them aside as singular phenomena. The Monster group M is the biggest among these. Most of the symbols refer to mathematicians who have discovered or constructed these groups.

The bulk of the groups are the series in (iii) and (iv). We will illustrate the nature of these groups by means of the example $\mathrm{A}_{n-1}(q) = \mathrm{SL}(n,q)$, whose simple section is $\mathrm{PSL}(n,q)$. Here, $\mathrm{SL}(n,q)$ stands for the group $\mathrm{SL}(\mathbb{F}_q^n)$ as introduced in Example 1.2.8, and so is the group of all $n \times n$ matrices over the field $\mathbb{F}_q$ of order q (a prime power) whose determinant equals 1. Thus, $\mathrm{SL}(n,q)$

coincides with the group $\mathrm{SL}(\mathbb{F}_q^n)$ introduced in Exercise 1.8.1. This group need not be simple as the center is the subgroup μ_n of all scalar multiplications $\lambda \mathrm{id}_n$ with $\lambda^n = 1$, which is non-trivial if and only if $\gcd(n, q-1) > 1$. The quotient with respect to the normal subgroup μ_n however is simple if $n \geq 2$ and $(n, q) \neq (2, 2), (2, 3)$.

The group T of all diagonal matrices within $\mathrm{SL}(n, q)$ has order $(q-1)^{n-1}$. It is a normal subgroup of the group N of all monomial matrices in $\mathrm{SL}(n, q)$. If $q > 2$, then N is the full normalizer of T in $\mathrm{SL}(n, q)$, that is, $N = \{g \in \mathrm{SL}(n, q) \mid gTg^{-1} = T\}$. (Do you see why $q = 2$ gives an exception?) By construction, T is a normal subgroup of the normalizer and its quotient group N/T is isomorphic to Sym_n, the symmetric group on $[n]$. This is the Coxeter group of type A_{n-1}. It is no coincidence that $\mathrm{SL}(n, q)$ is als named $\mathrm{A}_{n-1}(q)$.

Similary, the symbols A_n, B_n, C_n, D_n, E_n, F_4, G_2 in (iii), all refer to Coxeter types of groups occurring as the quotient of the normalizer of a maximal diagonizable subgroup T by T. Those in (iv) are supplied with a superscript preceeding the symbol. These refer to symmetries of the Coxeter matrix. For example, the diagram



has an automorphism of order 2, which plays a role in the definition of the group ${}^2\mathrm{E}_6(q)$. The superscript refers to the order of the diagram automorphism. These groups are variations of those in (ii) that we shall not go into any further. The point we are trying to make here is that, for an understanding of the finite simple groups (or Lie groups, of which the series (iii) and (iv) are finite analogues), Coxeter groups are a key tool.

1.8 Exercises

Section 1.1

Exercise 1.8.1 (Cited in Section 1.4) Let V be a vector space over a field $\mathbb{F}$ of dimension n. By $\mathrm{GL}(V)$ we denote the set of all invertible linear transformations of V.

(a) Prove that $\mathrm{GL}(V)$, with the usual composition of maps as multiplication, is a group.
(b) Let $\mathbb{F} = \mathbb{F}_q$, the finite field of q elements. Establish the following formula for the order of $\mathrm{GL}(V)$.

$$|\mathrm{GL}(V)| = \prod_{i=1}^{n} (q^n - q^{i-1}).$$

(*Hint:* Use the fact that the number of elements of $\mathrm{GL}(V)$ is equal to the number of bases of V.)

(c) By $\mathrm{SL}(V)$ we denote the subset of $\mathrm{SL}(V)$ of all linear transformations of determinant 1. Prove that $\mathrm{SL}(V)$ is a normal subgroup of $\mathrm{GL}(V)$.

(d) Let $\mathbb{F} = \mathbb{F}_q$, the finite field of q elements. Establish the following formula for the order of $\mathrm{SL}(V)$.

$$|\mathrm{SL}(V)| = q^{\binom{n}{2}} \prod_{i=2}^{n} (q^i - 1).$$

Section 1.2

Exercise 1.8.2 (A presentation of the trivial group) (Cited in Remark 1.2.6) Show that

$$\langle a, b \,|\, aba^{-1} = b^2, bab^{-1} = a^2 \rangle$$

is a presentation of the trivial group.

Exercise 1.8.3 (Cited in Definition 1.2.1) Show that the additive group of the rational numbers $\mathbb{Q}$ is not finitely generated (and hence not finitely presented).

Exercise 1.8.4 Adopt the setting of Example 1.2.3. Prove that

$$\langle a, c \,|\, a^2 = 1, (ac)^2 = 1, c^m = 1 \rangle$$

is another presentation of Dih_{2m}.
(*Hint:* Interpret c as ab and use Theorem 1.2.4 in two ways.)

Exercise 1.8.5 Let $m \in \mathbb{N}$, $m \geq 3$, and let τ_k be as in Example 1.2.5. Prove that $\langle \tau_m, \tau_{m-1}, \tau_{m-2} \rangle = \mathrm{Sym}_m$.
(*Hint:* Use the element $\tau_{m-2}\tau_{m-1}\tau_m\tau_{m-1}$ and show that the generators of Sym_m as given in Proposition 1.2.7 belong to $\langle \tau_m, \tau_{m-1}, \tau_{m-2} \rangle$.)

Exercise 1.8.6 Prove the statement of Example 1.2.8 that the two displayed matrices generate $\mathrm{SL}(\mathbb{Z}^2)$.

Section 1.3

Exercise 1.8.7 Prove Theorem 1.3.2.

Exercise 1.8.8 For $m \in \mathbb{N}$, let G be the cyclic group of order m.

(a) Prove that, if m is prime, the group G does not embed in Sym_n for $n < m$.

(b) Suppose $m = p \cdot q$ with $\gcd(p, q) = 1$. Show that G embeds in the direct product $\mathrm{Sym}_p \times \mathrm{Sym}_q$. Conclude that G has a faithful permutation representation of degree $p + q$.

Exercise 1.8.9 What is the minimal degree of a faithful permutation representation of Dih_{2m}?
(*Hint:* Adopt the setting of Example 1.2.3 and use Exercise 1.8.8 to find the minimal degree needed to embed c.)

Section 1.4

Exercise 1.8.10 What is the minimal degree of a faithful real linear representation of Dih_{2m}?

Exercise 1.8.11 (Cited in Remark 1.4.3) Let G be a finite group and $\mathbb{F}$ a field. By $\mathbb{F}[G]$ we denote the following algebra over $\mathbb{F}$. As a set, it consists of all formal linear combinations

$$\sum_{g \in G} \lambda_g g \qquad \text{with} \qquad \lambda_g \in \mathbb{F}.$$

The vector space structure on $\mathbb{F}[G]$ consists of coordinatewise addition and scalar multiplication; so $\dim(\mathbb{F}[G]) = |G|$. The multiplication is the bilinear extension of the group multiplication.

(a) Verify that $\mathbb{F}[G]$ is an algebra over $\mathbb{F}$.
(b) For $g \in G$, denote by L_g left multiplication by g:

$$L_g \left(\sum_{h \in G} \lambda_h h \right) = \sum_{h \in G} \lambda_h gh.$$

Establish that the map $g \mapsto L_g : G \to \mathrm{GL}(\mathbb{F}[G])$ is a faithful linear representation of G.

Section 1.5

Exercise 1.8.12 Let $n \in \mathbb{N}$, $n > 1$. View Sym_n as a permutation group on $[n]$ in the natural way. Consider the map ρ of Proposition 1.5.2.

(a) Show that there is a vector $v \in V$ fixed by all elements in the ρ image of Sym_n.
(b) Show that the linear span U of all vectors of the form $\sum_{i \in [n]} \lambda_i \delta_i$ with $\sum_i \lambda_i = 0$ is a linear subspace of V invariant under the ρ image of Sym_n.
(c) Prove that the map $\rho^U : \mathrm{Sym}_n \to \mathrm{GL}(U)$ given by $\rho^U_g = (\rho_g)|_U$ (the restriction to U of ρ_g) is a faithful linear representation of Sym_n.

Section 1.6

Exercise 1.8.13 Let $\alpha, \beta \in \mathbb{R}$ with $\alpha^2 + \beta^2 = 1$ and set $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $B = \begin{pmatrix} \alpha & \beta \\ \beta & -\alpha \end{pmatrix}$ and write $C = AB$.

(a) Show that $\langle A, B \rangle$ is a quotient group of Dih_∞.
(b) Determine the normal subgroups of Dih_∞.
(c) Derive that every proper quotient group of Dih_∞ is isomorphic to Dih_{2m} for some $m \in \mathbb{N}$.
(d) Show that C is diagonalizable (over $\mathbb{C}$) with eigenvalues $\lambda = e^{i\phi\pi}, \lambda^{-1} = e^{-i\phi\pi}$ for some $\phi \in (0, 1]$ such that $2\beta = \lambda + \lambda^{-1}$.
(e) For which values of α and β do we have $\langle A, B \rangle \cong \mathrm{Dih}_\infty$?
(*Hint:* Which restrictions on α, β force $C^m \neq 1$ for all $m \in \mathbb{N}$?)

Exercise 1.8.14 (Cited in Lemma 2.2.1) Let (W, S) be a Coxeter system of type M.

(a) Prove that there is a homomorphism of groups $\mathrm{sg} : W \to \{\pm 1\}$ determined by $\mathrm{sg}(s) = -1$ for each $s \in S$.
(b) Let K be a connected component of the graph M' obtained from M by omitting all edges with an even label. Prove that there is a homomorphism of groups $\mathrm{sg}_K : W \to \{\pm 1\}$ determined by $\mathrm{sg}_K(s) = -1$ for each $s \in K$ and $\mathrm{sg}_K(s) = 1$ for each $s \in S \backslash K$.
(c) Show that two members of S are conjugate in W if and only if they belong to the same connected component of the graph M' of (b).

Section 1.7

Exercise 1.8.15 Let $n \geq 2$ and let $\mathbb{F}$ be a field. We have seen that, for $\mathbb{F}$ finite, the Coxeter group $W(\mathrm{A}_{n-1})$ is isomorphic to Sym_n and to the quotient of the subgroup N of monomial matrices in $\mathrm{SL}(\mathbb{F}^n)$ of a diagonal subgroup T of $\mathrm{GL}(\mathbb{F}^n)$ by T. This statement also holds for $\mathbb{F}$ an arbitrary field. Now denote by M the subgroup of all monomial matrices in $\mathrm{GL}(\mathbb{F}^n)$. Thus N is a subgroup of M.

(a) Show that Sym_n embeds in M.
(b) Derive from this embedding that Sym_n embeds in N if $\mathbb{F}$ has characteristic 2.
(c) Consider the linear representation $\rho : \mathrm{Sym}_n \to \mathrm{GL}(\mathbb{F}^n)$ introduced in Lemma 1.5.2 for $\mathbb{F}$ a field with characteristic distinct from 2. (See also Exercise 1.8.12.) Show that $\det(\rho_g)$ is the sign of the permutation $g \in \mathrm{Sym}_n$.
(d) Prove that for n odd and $\mathbb{F}$ a field with characteristic distinct from 2, there is an embedding of Sym_n in N.
(e) For which values of n is Sym_n embeddable in N if the characteristic of $\mathbb{F}$ is distinct from 2?

1.9 Notes

Section 1.2. A very accessible introduction to presentations of groups by generators and relations is [21].

Section 1.3. Books like [30, 43] concentrate fully on permutation groups.

Section 1.4. Not every infinite group is a linear group. For instance, the automorphism group of a free group on three generators is not linear; see [16]. Every finite linear group has a faithful orbit on vectors. It is not true however, that every finite linear group has a faithful orbit on 1-spaces, although the number of counterexamples is small; see [31].

Section 1.5. The process of coset enumeration is not an algorithm as it will not always terminate. If the finitely presented group is known to be finite, then the process will terminate in a finite number of steps. See [8].

There is a process similar to coset enumeration for trying to make linear representations of a group starting from a presentation by generators and relations, but it is less frequently used. See [24].

Section 1.6. A very thorough and basic reference for Coxeter groups is [2]. A very good textbook on the subject is [20]. Figure 1.4 is from [42].

Section 1.7. The most comprehensive introduction to the Classification of Finite Simple Groups is probably [17], which is followed by a series of volumes intended to supply a full proof. Today volume 6 is the latest of the as yet unfinished series.

2. Presentations

In this lecture we focus on presentations of groups by means of generators and relations. In Section 1.6 we defined Coxeter groups in this way. In this chapter, we derive from this definition some of the basic properties of Coxeter groups. But, before going into Coxeter groups, we look at the basics of presentations of group by generators and relations. In particular, we start with a more fundamental treatment of the free group on a set A than the one given in Section 1.2.

2.1 Free groups

As we saw in Section 1.2, free groups are needed for the definition of group presentations. In order to discuss free groups, we introduce free monoids.

Definition 2.1.1 Let A be an alphabet, that is, a set of symbols. The set $\mathrm{M}(A)$ of all words over this alphabet, including the empty word, denoted by ε, is a monoid with ε as the unit and concatenation for multiplication. It is called the *free monoid* over A.

The function $l : \mathrm{M}(A) \to \mathbb{N}$ denotes *length*. So $l(a_1 \cdots a_q) = q$ if $a_1, \ldots, a_q \in A$. The empty word ε has length 0. The set A is the subset of words of $\mathrm{M}(A)$ of length 1. To emphasize its dependence on A, we sometimes write l_A instead of l.

The notion free refers to properties like those recorded in the following proposition.

Proposition 2.1.2 *For each monoid M generated by a set B of elements, and each map $\phi : A \to B$, there is a unique homomorphism of monoids $\phi' : \mathrm{M}(A) \to M$ extending ϕ.*

Proof. Let $w \in \mathrm{M}(A)$. Then there is a unique expression $w = a_1 a_2 \cdots a_q$ with $a_1, a_2, \ldots, a_q \in A$. The element $w = \varepsilon$ corresponds to the case where $q = 0$. We set

$$\phi'(w) = \phi(a_1)\phi(a_2)\cdots\phi(a_q). \tag{2.1}$$

Interpreting the empty product as the unit element in M, we find $\phi'(\varepsilon) = 1$. Clearly ϕ' is a monoid homomorphism $\mathrm{M}(A) \to M$ extending ϕ. As for uniqueness, the definition of monoid homomorphism requires that the unit element maps to the unit element $\phi'(\varepsilon) = 1$ and the multiplicative rule for a homomorphism forces (2.1). □

If we start with the monoid M generated by a subset B, we can take $A = B$ and $\phi : A \to B$ the identity map. The proposition shows that every monoid generated by a set B is the quotient of the free monoid on B. As a result, each element of M can be represented by a word in B, that is, an element of $\mathrm{M}(B)$. The representative is easy to store on a computer. It may be hard though, to decide whether (or not) two words represent the same element of M. Finding an algorithm for deciding this is called the *word problem*. In its greatest generality, this problem is undecidable in the sense that there is no such algorithm (for a Turing machine—the most common theoretic model for computers). For certain special classes of groups, like Coxeter groups, there are satisfactory solutions.

Definitions 2.1.3 An equivalence relation $\sim$ on a monoid M is called a *congruence* if $x \sim y$ implies $uxv \sim uyv$ for all $x, y, u, v \in M$. The set $M/\sim$ of equivalence (also called congruence) classes in M with respect to $\sim$ has a well-defined multiplication $\cdot$ by means of $\widetilde{x} \cdot \widetilde{y} = \widetilde{xy}$, where $x, y \in M$ and $\widetilde{x}$ denotes the class of x. This turns $M/\sim$ into a monoid with unit $\widetilde{\varepsilon}$. This monoid is called the quotient monoid of M with respect to $\sim$.

An extreme example of a congruence relation is $\sim = M \times M$. The quotient monoid of M with respect to this relation is the trivial monoid. As an intersection of congruence relations is again a congruence relation, we can define the *congruence relation generated* by a relation as the intersection of all congruence relations containing it.

Now suppose $X = A \cup A^{-1}$ is a disjoint union of two sets A and A^{-1} which are in bijective correspondence by means of $\cdot^{-1} : A \to A^{-1}$. So A^{-1} consists of the symbols a^{-1} for $a \in A$. We will also write $(a^{-1})^{-1} = a$ for $a \in A$, so the map $x \mapsto x^{-1}$ is defined on all of X. We will use the congruence relation $\sim$ generated by $xx^{-1} \sim \varepsilon$ for each $x \in X$ to define $\mathrm{F}_1(A)$ as the monoid $\mathrm{M}(X)/\sim$.

The word problem for $\mathrm{M}(X)/\sim$ is easily solved. Recall from Section 1.2 that a word in $\mathrm{M}(X)$, where $X = A \cup A^{-1}$, is reduced if no xx^{-1} occurs in it for any $x \in X$.

Lemma 2.1.4 *For a set A, put $X = A \cup A^{-1}$ and consider $\mathrm{F}_1(A) = \mathrm{M}(X)/\sim$. By removing all occurrences xx^{-1} from a word $w \in \mathrm{M}(X)$ in any order, we obtain a unique reduced word in $\widetilde{w}$.*

Proof. First consider the monoid $\mathrm{M}(X)/\sim$. Every generator $\widetilde{x}$ with $x \in X$ has inverse $\widetilde{x^{-1}}$ and so each element of $\mathrm{M}(X)/\sim$ has an inverse. This implies that $\mathrm{M}(X)/\sim$ is a group.

We will prove that, by removing occurrences xx^{-1} from a word $w \in \mathrm{M}(X)$ in any order, we obtain a unique reduced word in $\widetilde{w}$ (as defined in Section 1.2). This then establishes that the multiplication defined on $\mathrm{F}(A)$ coincides with the multiplication on $\mathrm{M}(X)/\sim$ expressed in terms of the unique congruence class representatives (the reduceed words). This will suffice for the proof of the first statement.

We proceed by induction on $l(w)$, the length of w as a word in X. If w is reduced, there is nothing to prove. So, we may assume that $w = uxx^{-1}v$ for certain $x \in X$ and $u, v \in \mathrm{M}(X)$. Suppose that w reduces to the reduced word r. In view of the induction hypothesis, it will suffice to show that any reduction to r can be re-arranged in such a way that $w \Rightarrow uv$, that is, removing the above occurrence of xx^{-1}, is the first step of the reduction. Let's call this step S. If S occurs in a reduction, the steps prior to S do not touch the occurrence xx^{-1} in the sense that they take place entirely in u or entirely in v; so we can swap the order of events so as to start with S and still reach r.

Since xx^{-1} does not occur in r, there is at least one stage in which either the letter x or x^{-1} in $uxx^{-1}v$ is removed. This can only happen if x^{-1} preceeds x, so $u = u'x^{-1}$, or if x follows x^{-1}, so $v = xv'$. In the first case, the step $w = u'(x^{-1}x)x^{-1}v \Rightarrow u'x^{-1}v$ (removal of $x^{-1}x$) has the same effect as S and similarly for the second case. In this way, we can ensure that S takes place in the reduction from w to r and we can finish by invoking the previous paragraph. □

As a consequence, we can view $\mathrm{F}_1(A)$ as the set of reduced words in $\mathrm{M}(X)$ with multiplication the multiplication in $\mathrm{M}(X)$ followed by a reduction of the product to a reduced word. This is precisely the construction of $\mathrm{F}(A)$ in Section 1.2.

Proposition 2.1.5 *The group* $\mathrm{F}(A)$ *is well defined and isomorphic to* $\mathrm{F}_1(A)$. *It is the free group on* A *in the sense that it is generated by* A *and, for any group* G *generated by a set* B *and every map* $\phi : A \to B$, *there is a unique homomorphism* $\mathrm{F}(A) \to G$ *extending* ϕ.

Proof. The first statement is derived above. Proving the second statement is part of Exercise 2.4.2. □

Recall the notions Coxeter group and Coxeter system from Definition 1.6.1. At this stage, it is not clear that the generators s_i, s_j are distinct elements of W for $i \neq j$. It will be shown to hold later (in Theorem 2.3.5(i)). We often write $r_1, r_2, \ldots$ for arbitrary elements of $S = \{s_i \mid i \in [n]\}$.

Remark 2.1.6 Instead of considering the Coxeter group $W(M)$ as a quotient of the free group $\mathrm{F}(S)$, where $S = \{s_1, \ldots, s_n\}$, it makes sense to exploit the fact that S consists of elements of order at most 2 and to view $W(M)$ as a quotient of the group

$$\mathrm{FI}(S) = \langle S \mid \{s^2 = 1 \mid s \in S\}\rangle$$

by the normal subgroup generated by all images in $\mathrm{FI}(S)$ of the words $(s_i s_j)^{m_{ij}}$ in $\mathrm{M}(S)$ for $i, j \in [n]$ with $m_{ij} < \infty$. For, by Exercise 2.4.3(a), the word problem for $\mathrm{FI}(S)$ has an easy solution, as follows. If $w \in \mathrm{M}(S)$, a *repetition* in w is an occurrence of ss in w for some $s \in S$. A word without repetitions is called *simple*. Removal of all repetitions, from w leads to a unique simple word w' with the same image in $\mathrm{FI}(S)$ without repetitions. Now two words in $\mathrm{M}(S)$ represent the same element of $\mathrm{FI}(S)$ if and only if the corresponding simple words are equal. Alternatively, we can view $\mathrm{FI}(S)$ as the subset of $\mathrm{M}(S)$ consisting of all simple words with product the composition of the product in $\mathrm{M}(S)$ with the reduction to a simple word.

In conclusion, in order to study words representing elements of $W(M)$, we will work with words in $\mathrm{M}(S)$ and often reduce representatives to simple words. We will write δ_M or just δ for the monoid homomorphism $\mathrm{M}(S) \to W(M)$ that assigns to s in $\mathrm{M}(S)$ the element s in $W(M)$. It is surjective and its restriction to the set of simple words can also be interpreted as a group homomorphism $\mathrm{FI}(S) \to W(M)$.

Definition 2.1.7 A word of minimal length in the inverse image under δ of an element $w \in W(M)$ will be called a *minimal expression* for w. The length of a minimal expression for $w \in W$ is called the *length* of w, and also denoted $l(w)$.

Example 2.1.8 If $M = \mathrm{B}_2 = \mathrm{I}_2(4)$ (see Example 1.6.2), then $W(M)$ is the dihedral group of order eight, $S = \{s_1, s_2\}$ has cardinality two, $\mathrm{M}(S)$ is infinite (the monoid of all words in two letters). Minimal expressions for the elements of W are 1, s_1, s_2, s_1s_2, s_2s_1, $s_1s_2s_1$, $s_2s_1s_2$, and $s_1s_2s_1s_2$. The lengths of the corresponding elements of W are 0, 1, 1, 2, 2, 3, 3, 4. The last expression is equivalent to $s_2s_1s_2s_1$ in the sense that, in W, we have $s_1s_2s_1s_2 = s_2s_1s_2s_1$.

2.2 Length on Coxeter groups

We collect some basic and useful observations on the length function of a Coxeter group.

Lemma 2.2.1 *Let (W, S) be a Coxeter system. For $s \in S$ and $w \in W$, we have $l(sw) = l(w) \pm 1$.*

Proof. Clearly, $l(sw) \leq 1+l(w)$ and $l(w) = l(s(sw)) \leq 1+l(sw)$, so $l(w)-1 \leq l(sw) \leq l(w)+1$. It remains to show that the parities of $l(w)$ and $l(sw)$ differ.

Write $S = \{s_1, \ldots, s_n\}$ and let $(m_{ij})_{1\leq i,j\leq n}$ be the Coxeter matrix of (W, S). By Exercise 1.8.14(i) there is a homomorphism $\mathrm{sg} : W \to \{\pm 1\}$ of groups (the latter being the multiplicative subgroup of the rationals of order 2) determined by $\mathrm{sg}(r) = -1$ for each $r \in S$. If $w = r_1 \cdots r_q$ is an expression for w, then $\sigma(w) = \sigma(r_1) \cdots \sigma(r_q) = (-1)^q$. In particular, $(-1)^q$ does not depend on the expression chosen and equals $(-1)^{l(w)}$. This implies $(-1)^{l(sw)} = \mathrm{sg}(sw) = \mathrm{sg}(s)\sigma(w) = (-1)^{l(w)+1}$. Hence $l(sw) \equiv l(w) + 1 \pmod 2$, that is, the parities of $l(sw)$ and $l(w)$ differ. □

Definition 2.2.2 Let $T \subseteq S$. If $w \in W$ satisfies $l(jw) > l(w)$ for all $j \in T$, then w is called *left T-reduced*. The set of all left T-reduced elements of W is denoted by ${}^T W$. Similarly, for $K \subseteq S$, an element $w \in W$ is called *right K-reduced* if $l(wk) > l(w)$ for all $k \in K$, and W^K denotes the set of all right K-reduced elements of W.

Let $W = \langle S \rangle$. As indicated before, for $T \subseteq S$, we denote the length function on the subgroup $\langle T \rangle$ of W with respect to the generating set T.

Lemma 2.2.3 *Let (W, S) be a Coxeter system. For each $w \in W$ and $T \subseteq S$, the following properties hold.*

(i) There are $u \in \langle T \rangle$ and $v \in {}^T W$ such that $w = uv$ and $l(w) = l(u)+l(v)$.
(ii) If $w \in \langle T \rangle$, then $l(w) = l_T(w)$.

Proof. Consider the subset D of $\langle T \rangle \times W$ consisting of all pairs (u, v) with $w = uv$ and $l(w) = l(u)+l(v)$ such that $l(u) = l_T(u)$. This set is nonempty, as it contains $(1, w)$. Let (u, v) be an element of D with $l(u)$ maximal. Suppose $t \in T$ is such that $l(tv) < l(v)$. Then $v = tv'$ for some $v' \in W$ with $l(v) = l(v')+1$ and so $w = (ut)v'$ is a decomposition of w with $l(w) \leq l(ut)+l(v') \leq (l(u) + 1) + (l(v) - 1) = l(w)$, whence $l(ut) = l(u) + 1$. Now $l(ut) \leq l_T(ut) \leq l_T(u) + 1 = l(u) + 1 = l(tu)$. Therefore, $(ut, v') \in D$ with $l(ut) > l(u)$, a contradiction. We conclude that $v \in {}^T W$. This proves (i).

If $w \in \langle T \rangle$, then the proof of (i) gives a decomposition $w = uv$ with $u \in \langle T \rangle$ and $v \in {}^T W$ such that $l(w) = l(u) + l(v) = l_T(u) + l(v)$. But now $v \in \langle T \rangle \cap {}^T W = \{1\}$, so $w = u$ and $l(w) = l_T(w)$, as required for (ii). □

The study of Coxeter groups can be reduced to irreducible types, as follows.

Definition 2.2.4 When we talk about a *connected component* of a Coxeter matrix M, we view M as a labelled graph. In other words, a connected component of M is a maximal subset J of $[n]$ such that $m_{jk} = 2$ for each

$j \in J$ and $k \in [n]\backslash J$. If M has a single connected component, it is called *connected* or *irreducible*. A Coxeter group W over a Coxeter diagram M is called *irreducible* if M is connected.

If J is a subset of the nodes of M, we also let J stand for the labelled graph induced on J by M; in other words, the matrix $M|_{J\times J}$. In particular, we write $W(J)$ for the Coxeter group of type J.

Proposition 2.2.5 *Let W be a Coxeter group of type M and let $J_1, \ldots, J_t$ be a partition of the vertex set of the labelled graph M into connected components. Then $W(M) \cong W(J_1) \times W(J_2) \times \cdots \times W(J_t)$.*

Proof. By induction on the number of connected components and application of Exercise 2.4.7. □

2.3 The reflection representation

Let (W, S) be a Coxeter system of type M and write $n = |S|$. We will construct a real linear representation of W of degree n such that the images of the elements of S are reflections in $\mathbb{R}^n$.

Definition 2.3.1 A *reflection* on a real vector space V is a linear transformation on V fixing a subspace of V of codimension 1, called its *mirror* and having a nontrivial eigenvector with eigenvalue -1, called a *root* of the reflection.

See Exercise 2.4.9 for an idea how to construct reflections.

Fix a Coxeter matrix $M = (m_{ij})_{i,j\in[n]}$. Let V be a real vector space with basis $(e_i)_{i\in[n]}$. Denote by B_M, or just B if M is clear from the context, the symmetric bilinear form on V determined by

$$B(e_i, e_j) = -2\cos(\pi/m_{ij}) \tag{2.2}$$

for $i, j \in [n]$, with the understanding that $B(e_i, e_j) = -2$ if $m_{ij} = \infty$. The form is indeed symmetric as $m_{ij} = m_{ji}$ for $i, j \in [n]$.

Definition 2.3.2 We call B_M the *symmetric bilinear form associated with* M. Let Q_M, or just Q, be the quadratic form determined by B, i.e.,

$$Q(x) = \frac{1}{2}B(x, x)$$

for all $x \in V$. We call Q_M the *quadratic form associated with* M.

For $x = \sum_i x_i e_i$ we have $Q(x) = -\sum_{i,j\in[n]} x_i x_j \cos(\pi/m_{ij})$. The bilinear form B is linked to Q via

$$Q(x+y) = Q(x) + Q(y) + B(x,y)\ .$$

We use the form B to define reflections in $\mathrm{GL}(V)$ preserving B. Here are some general properties of B and these reflections.

Proposition 2.3.3 *For the symmetric bilinear form B associated with the Coxeter matrix M, and for the linear transformations ρ_i $(i \in [n])$ given by*

$$\rho_i(x) = x - B(x, e_i)e_i \quad (x \in V), \tag{2.3}$$

the following assertions hold.

(i) $B(e_i, e_i) = 2$ *for all* $i \in [n]$.
(ii) $B(e_i, e_j) \leq 0$ *for all* $i, j \in [n]$ *with* $i \neq j$, *with equality if and only if* $m_{ij} = 2$, *or, equivalently,* i *and* j *are non-adjacent in the labelled graph* M.
(iii) For each $i \in [n]$, *the transformation* ρ_i *is a reflection on* V *with mirror* $e_i^\perp := \{x \in V \mid B(x, e_i) = 0\}$ *and root* e_i.
(iv) For all $x, y \in V$ *we have* $B(\rho_i x, \rho_i y) = B(x, y)$.
(v) The order of $\rho_i\rho_j$ *equals* m_{ij}.

Proof. (i) and (ii) are obvious from the definition of B.

(iii). This follows from Exercise 2.4.9.

(iv). By straightforward computation.

$$\begin{aligned} B(\rho_i x, \rho_i y) &= B(x - B(x,e_i)e_i, y - B(y,e_i)e_i)) \\ &= B(x,y) - B(x,e_i)B(e_i,y) - B(x,e_i)B(y,e_i) \\ &\qquad + 2B(x,e_i)B(y,e_i)B(e_i,e_i) \\ &= B(x,y). \end{aligned}$$

(v). The linear subspace $\mathbb{R}e_i + \mathbb{R}e_j$ of V is invariant under ρ_i and ρ_j. Writing $b = B(e_j, e_i)$ we can express the matrices of these linear transformations on the basis e_i, e_j as

$$\rho_i : \begin{pmatrix} -1 & -b \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \rho_j : \begin{pmatrix} 1 & 0 \\ -b & -1 \end{pmatrix},$$

so $\rho_i\rho_j$ has matrix

$$\begin{pmatrix} -1+b^2 & b \\ -b & -1 \end{pmatrix}.$$

The characteristic polynomial of this matrix is $\lambda^2 - (b^2-2)\lambda + 1$, which, in view of (2.2), factors as $(\lambda - \exp^{2\pi \mathrm{i}/m_{ij}})(\lambda - \exp^{-2\pi \mathrm{i}/m_{ij}})$, where $\mathrm{i}^2 = -1$.

Suppose $m_{ij} = \infty$. Then the above matrix is not the identity, so $(\lambda - 1)^2$ is the minimal polynomial of the matrix, and so the matrix must be of infinite order. Hence $\rho_i \rho_j$ has infinite order.

Suppose $m_{ij} < \infty$. The restriction of Q to $\mathbb{R}e_i + \mathbb{R}e_j$ is

$$\begin{aligned} Q(x_i e_i + x_j e_j) &= x_i^2 - 2x_i x_j \cos(\pi/m_{ij}) + x_j^2 \\ &= (x_i - x_j \cos(\pi/m_{ij}))^2 + x_j^2 \sin^2(\pi/m_{ij}). \end{aligned}$$

This computation shows that Q is positive definite on $\mathbb{R}e_i + \mathbb{R}e_j$, and so $V = (\mathbb{R}e_i + \mathbb{R}e_j) + (e_i^\perp \cap e_j^\perp)$. In view of (iii), the order of $\rho_i \rho_j$ is the order of its restriction to $\mathbb{R}e_i + \mathbb{R}e_j$. The above formula for the characteristic polynomial of this restriction of $\rho_i \rho_j$ shows that its eigenvalues on that subspace are $\exp^{2\pi \mathrm{i}/m_{ij}}$ and $\exp^{-2\pi \mathrm{i}/m_{ij}}$, which are primitive m_{ij}-th roots of unity. Therefore, the order of $\rho_i \rho_j$ is equal to m_{ij}. □

Example 2.3.4 Going back to the octahedron of Example 1.6.5 where $M = \mathrm{B}_3$, we see that, with respect to the basis e_1, e_2, e_3 we have

$$B(x, y) = 2x_1y_1 + 2x_2y_2 + 2x_3y_3 - \sqrt{2}x_1y_2 - \sqrt{2}x_2y_1 - x_2y_3 - x_3y_2 \ .$$

So B is positive definite. After a coordinate transformation to an orthonormal basis, ρ_1, ρ_2, and ρ_3 can be seen to be the reflection symmetries of a regular cube.

Theorem 2.3.5 *Let M be a Coxeter matrix of dimension n.*

(i) The mapping $w \mapsto \rho_w$ given by $\rho_w = \rho_1 \cdots \rho_q$ whenever $w = r_1 \cdots r_q$ with $r_j \in S$ $(j = 1, \ldots, q)$ defines a linear representation of $W(M)$ on V preserving B.

(ii) The mapping $[n] \to \{\rho_i \mid i \in [n]\}$ sending i to ρ_i is a bijection.

(iii) The restriction of ρ to the subgroup $\langle s_i, s_j \rangle$ of $W(M)$ is faithful for all $i, j \in [n]$.

Proof. (i). By Proposition 2.3.3(iii), (v), the subgroup of $\mathrm{GL}(V)$ generated by the ρ_i, $i \in [n]$, satisfies the defining relations of W. According to Theorem 1.2.4, $s_i \mapsto \rho_i$ determines a unique group homomorphism $\rho : W \to \mathrm{GL}(V)$ obeying the given equations. Finally, ρ preserves B due to Proposition 2.3.3(iv).

Assertions (ii) and (iii) follow directly from Proposition 2.3.3(v). □

Definition 2.3.6 If (W, S) is a Coxeter system of type M, the corresponding linear representation $\rho : W \to \mathrm{GL}(V)_B$ of Theorem 2.3.5 is called the *reflection representation* of W.

The *radical* of B_M is the following linear subspace of V.

$$V^\perp = \{x \in V \mid B_M(x, y) = 0 \text{ for all } y \in V\}$$

Proposition 2.3.7 *If W is an irreducible Coxeter group of type M and if E is a proper invariant subspace of V with respect to the reflection representation ρ of W on V, then E is contained in the radical of B_M.*

Proof. We claim that $e_i \notin E$ for $i \in [n]$. To see this, set $J = \{i \in [n] \mid e_i \in E\}$. We need to show that $J = \emptyset$. As E is a proper subspace of V, we have $J \neq I$. If $J \neq \emptyset$, then, since W is irreducible, we may assume that there exist $s \in J$, $t \in [n]\backslash J$ with $B(e_s, e_t) \neq 0$. Then $\rho_t e_s = e_s - B(e_s, e_t)e_t$ and so $B(e_s, e_t)e_t = e_s - \rho_t e_s$ is in E. Therefore $e_t \in E$, whence $t \in J$, a contradiction. Hence, $J = \emptyset$, so the claim holds.

Next, let $x \in E$. If $i \in [n]$, then $B(x, e_i)e_i = x - \rho_i x \in E$. But $e_i \notin E$, so $B(x, e_i) = 0$ for all $i \in [n]$. Thus, $x \in V^\perp$, which establishes $E \subseteq V^\perp$. □

Example 2.3.8 Direct products of Coxeter groups appear in elementary geometry. For instance, in the Euclidean space $\mathbb{E}^3$, let Π be a double vertical prism with a regular horizontal basis that is a polygon of n sides. Here double indicates that the pyramid above the horizontal basis plane is the reflection of the one under it. Then the group of isometries of Π is the Coxeter group of type $\mathrm{A}_1 \oplus \mathrm{I}_2(n)$.

By the way, this example, with $n = 3$, shows that an abstract Coxeter group does not uniquely determine its Coxeter diagram. For, $W(\mathrm{A}_1 \dot\cup \mathrm{I}_2(3))$ is the dihedral group of order 12 and hence isomorphic to $W(\mathrm{I}_2(6))$. See Exercise 2.4.6(b) for another example.

Recall from Definition 2.2.4 the notion of irreducibility for Coxeter groups. In the theory of linear representations, the notion of irreducibility also exists.

Definition 2.3.9 A linear representation $\phi : G \to \mathrm{G}(V)$ of a group G on a vector space V over the field F is called *irreducible* if there is no linear subspace of V invariant under $\phi(G)$ except for $\{0\}$ and V.

Such a linear representation is called *absolutely irreducible* if the representation remains irreducible after each extension of the field of scalars of V.

A representation is called *semisimple* (also known as *completely reducible*) if it is the direct sum of irreducible representations.

Example 2.3.10 The cyclic group $\langle c \rangle$ of order n has a two-dimensional real linear representation in which the generator c is mapped onto

$$\phi(c) := \begin{pmatrix} \cos(2\pi/n) & \sin(2\pi/n) \\ -\sin(2\pi/n) & \cos(2\pi/n) \end{pmatrix} .$$

This representation is irreducible but not absolutely irreducible as, over $\mathbb{C}$, the subspace $\mathbb{C}(1,i)^\top$ is invariant under $\langle c\rangle$. The representation is semisimple over both $\mathbb{R}$ and $\mathbb{C}$.

Example 2.3.11 (The infinite dihedral group) Let $n = 2$ and $m_{12} = \infty$. The linear representation ρ of $W(M)$ occurs in $V = \mathbb{R}^2$. The form B and the matrices ρ_1 and ρ_2 on the basis $\{e_1, e_2\}$ appear in the proof of Proposition 2.3.3(v) with $i = 1$ and $j = 2$. The vector $e_1 + e_2$ is orthogonal to all of V and spans the linear subspace $\mathrm{Rad}(B) := V^\perp$. In particular, ρ is a *reducible representation* in the sense that it leaves invariant a nontrivial proper linear subspace of V. As $\mathbb{R}e_1 + \mathbb{R}e_2$ is the only 1-dimensional ρ-invariant subspace of V, the representation is not semisimple.

Proposition 2.3.3(ii) tells us that, if $W(M)$ is not irreducible, the reflection representation ρ is reducible. The converse does not hold as we saw in Example 2.3.11. There is however, the following partial converse.

Corollary 2.3.12 *Suppose that W is a Coxeter group. Then the following three statements are equivalent.*

(i) $\mathrm{Rad}(B) = 0$.
(ii) The reflection representation of W is irreducible.
(iii) The reflection representation of W is absolutely irreducible.

Proof. The equivalence of (i) and (ii) is immediate from Proposition 2.3.7. Since, clearly (iii) implies (ii), we only need to show that irreducibility implies absolute irreducibility. Suppose that the reflection representation of W is irreducible. Then the argument of the proof of Proposition 2.3.7 applies equally well to the vector space V after extension of the scalars to a field containing $\mathbb{R}$, showing again that an invariant subspace of the vector space over the extended field lies in the radical of B. Since the radical of B over the extension field has the same dimension as over $\mathbb{R}$, it must be trivial. Hence, also over the extension field, there are no invariant subspaces, so the representation is absolutely irreducible. □

2.4 Exercises

Section 2.1

Exercise 2.4.1 A free monoid F on an alphabet A can be defined as a monoid generated by a set A with the property stated in Proposition 2.1.2: for each monoid M generated by a set B of elements, and for each map $\phi : A \to B$, there is a unique homomorphism of monoids $\phi' : F \to M$ extending ϕ. By the proposition, $\mathrm{M}(A)$ is a free monoid. Show that each free monoid on A is isomorphic to $\mathrm{M}(A)$.

Exercise 2.4.2 (Cited in Proposition 2.1.5) Prove the second statement of Proposition 2.1.5. Show that each free group on A is isomorphic to $\mathrm{F}(A)$.

Exercise 2.4.3 (Cited in Remark 2.1.6) Let A be a finite set of size n. Consider the congruence relation $\sim'$ generated by $a^2 \sim' 1$ for each $a \in A$, and the congruence relation $\sim''$ generated by $\sim'$ and $ab \sim'' ba$ for each $a, b \in A$.

(a) Show that each congruence class of $\sim'$ contains a unique word without repetitions.
(b) Deduce that $\mathrm{M}(A)/\sim'$ is a group of order 2 if $n = 1$ and of infinite order if $n > 1$.
(c) Show that $\mathrm{M}(A)/\sim''$ is a group of order 2^n.

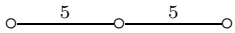
Exercise 2.4.4 Let M be a Coxeter matrix of dimension $n \geq 1$ and set $\Sigma = \{\sigma_i \mid i \in [n]\}$. Let $\mathrm{A}(M)$ be the group with presentation

$$\langle \Sigma \mid \{\underbrace{\sigma_i\sigma_j\sigma_i\cdots}_{m_{ij}} = \underbrace{\sigma_j\sigma_i\sigma_j\cdots}_{m_{ij}} \mid i, j \in [n]\}\rangle.$$

This group is called the *Artin group of type* M.

(a) Prove that there is a surjective homomorphism $\phi : \mathrm{A}(M) \to W(M)$ such that $\phi(\sigma_j) = s_j$ for $j \in [n]$.
(b) Establish that $\mathrm{A}(M)$ is an infinite group.

Exercise 2.4.5 Consider the Coxeter diagram



Show that the dihedral group Dih_{10} of order 10 is a homomorphic image of the corresponding Coxeter group.

Exercise 2.4.6 The Coxeter diagram of a Coxeter group is not uniquely determined by the abstract group. Here are two counterexamples.

(a) Show that the groups $W(\mathrm{A}_1 \dot\cup \mathrm{I}_2(3))$ and $W(\mathrm{I}_2(6))$ are both isomorphic to the dihedral group of order 12.
(b) Consider the two diagrams of Figure 2.1. Prove that the two Coxeter groups are isomorphic.
(*Hint:* Show that replacement of the reflection s_4 by $s_1s_2s_4s_2s_1$ in the left hand Coxeter group leads to the same Coxeter group, but a presentation corresponding to the diagram at the right hand side, and that replacement of s_4 by $s_2s_1s_4s_1s_2$ in the right hand Coxeter group leads to the same Coxeter group, but a presentation corresponding to the diagram at the left hand side.)

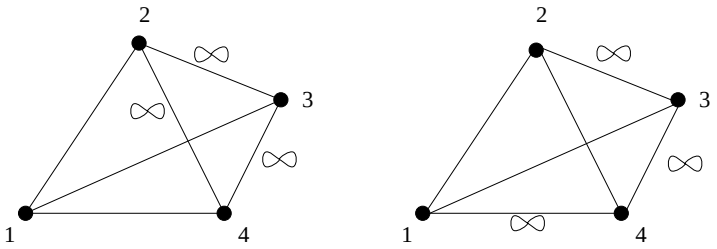


Fig. 2.1. Two Coxeter diagrams whose Coxeter groups are isomorphic.

Section 2.1

Exercise 2.4.7 (Cited in Proposition 2.2.5) Let $A = B \dot\cup C$ be the disjoint union of the alphabets B and C and let $R = S \dot\cup T \dot\cup U$ be the disjoint union of a set S of relations in $\mathrm{M}(B \dot\cup B^{-1})$, a set T of relations in $\mathrm{M}(C \dot\cup C^{-1})$, and the set $U = \{cb = bc \mid b \in B, c \in C\}$.

(a) Prove that $\langle A \mid R\rangle$ is isomorphic to the direct product $\langle B \mid S\rangle \times \langle C \mid T\rangle$.
(b) Let J be an arbitrary subset of $[n]$. Verify that the subgroup of $W(M)$ generated by $\{s_i \mid i \in J\}$ is a homomorphic image of $W(J)$. (See Definition 2.2.4.)
(c) Suppose that M is a Coxeter diagram with connected components J and K; here M is viewed as a graph as described in Notation 1.6.4. Show that $W(M)$ is isomorphic to the direct product of $W(J)$ and $W(K)$.

By use of the disjoint union symbol, we can express M as $J \dot\cup K$, so that the last result reads $W(J \dot\cup K) \cong W(J) \times W(K)$.

Exercise 2.4.8 Show that $l(w^{-1}) = l(w)$ for each w in a Coxeter group W.

Section 2.3

Exercise 2.4.9 (Cited in Proposition 2.3.3) Let $\phi : V \to \mathbb{R}$ be a nonzero linear form on the real vector space V and let $a \in V \backslash \{0\}$.

(a) Prove that the map $r_{a,\phi} : V \to V$ defined by $r_{a,\phi}v = v - \phi(v)a$ for $v \in V$ is a reflection if and only if $\phi(a) = 2$.
(b) Show that every reflection on V can be written in this way.

Exercise 2.4.10 Prove that the group $W(\mathrm{H}_3)$ is isomorphic to the direct product $\mathrm{Alt}_5 \times \mathbb{Z}/2\mathbb{Z}$ of the alternating group on five letters and the cyclic group of order 2. Conclude that $W(\mathrm{H}_3)$ is not isomorphic to $W(\mathrm{A}_4)$, as the latter is isomorphic to Sym_5.

Exercise 2.4.11 The Coxeter matrix

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

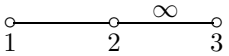
is usually denoted $\widetilde{\mathrm{A}}_2$. Set $c = \rho_1\rho_2\rho_3$ in the notation of Proposition 2.3.3. Prove that c has infinite order. (Hint: compute its minimal polynomial.) Deduce that the Coxeter group $W(\widetilde{\mathrm{A}}_2)$ has infinite order.

Exercise 2.4.12 Compute the orders of $W(\mathrm{H}_3)$ and $W(\mathrm{B}_3)$.

Exercise 2.4.13 By $\mathrm{PGL}(2,\mathbb{Z})$ we denote the quotient of the group $\mathrm{GL}(2,\mathbb{Z})$ of invertible 2×2 matrices with integer entries by the central subgroup consisting of the identity element and its negative. Take

$$\rho_1 = \pm\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \rho_2 = \pm\begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \rho_3 = \pm\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad \text{in} \quad \mathrm{PGL}(2,\mathbb{Z}).$$

(a) Prove that $\{\rho_1, \rho_2, \rho_3\}$ is a generating set for $\mathrm{PGL}(2,\mathbb{Z})$.
(b) Use the generating set in (a) to verify that $\mathrm{PGL}(2,\mathbb{Z})$ is a quotient of the Coxeter group of type



[In fact, $\mathrm{PGL}(2,\mathbb{Z})$ is isomorphic to this Coxeter group, as will become clear in Exercise 3.4.8.]
(c) Derive from the above that $W(\mathrm{A}_3)$ is isomorphic to $\mathrm{PGL}(2,\mathbb{F}_3)$ and (using Exercise 2.4.12 if needed) that $W(\mathrm{H}_3)$ is isomorphic to $\mathrm{PGL}(2,\mathbb{F}_5)$.

2.5 Notes

The name Coxeter groups refers to the fact that Coxeter studied presentations for finite linear groups generated by reflections, cf. [10, 11, 12].

Section 2.1 deals with the very beginning of combinatorial group theory. See [1] for more comprehensive lectures. The fact that $xx^{-1}x$ can be rewritten in two different ways that both lead to the same answer is a local confluence. The famous Knuth-Bendix algorithm [22] is an attempt at constructing a locally confluent rewrite system in more general circumstances, in order to exploit the fact that local confluence implies global confluence (and hence a unique reduced form) within a free monoid provided the rewrite rules decrease of words according to a well-founded (or Noetherian) ordering on the free monoid. If the Knuth Bendix process is successful, the resulting locally confluent rewrite system is called a completion. The solution of the word

problem for the free group of Proposition 2.1.5 is a very simple instance of Knuth Bendix completion.

The word problem for Coxeter groups can be solved by means of rewrite rules as in Exercise 2.4.4. This fact will be proved later.

In Section 2.3, the linear representation of Theorem 2.3.5 is faithful. This result, due to Tits, will be dealt with in the next lecture.

Exercise 2.4.6(b) is due to Mühlherr [27].

3. Coxeter groups are linear

In Definition 2.3.6, the reflection representation of a Coxeter group was introduced. In this lecture, we will show that this representation is faithful. This means that each Coxeter group is isomorphic to a group of real linear transformations; this explains the title of this lecture.

The first section gives an brief introduction into affine spaces. The second second section shows that a large class of groups generated by affine reflections are in fact Coxeter groups. The third section contains the promised result.

Suppose that (W, S) is a Coxeter system and write $n = |S|$. When $n < \infty$, it is often convenient to order S and identify the ordered set with $[n]$. By Theorem 2.3.5(ii) the subset of images of S in W is in bijective correspondence with S. Therefore, we can view S as a subset of W.

Consider the real vector space V with basis e_s for $s \in S$. Let $B : V \times V \to \mathbb{R}$ be the bilinear form on V determined by $B(e_r, e_s) = -2\cos(2\pi/m_{rs})$ for $r, s \in S$. The reflection representation $\rho : G \to \mathrm{GL}(V)$ is given by $\rho_s(v) = v - B(v, e_s)e_s$ $(v \in V, s \in S)$.

3.1 The affine space of a vector space

Affine spaces are closely related to vector spaces. Fixing a point in affine space reveals the structure of a vector space. Here we start with the latter and reconstruct an affine space from it. We state some facts without proofs because they come down to elementary linear algebra.

Definition 3.1.1 Let $\mathbb{F}$ be a field and let V be a vector space over $\mathbb{F}$. The *affine space* $\mathrm{A}(V)$ *of* V is the set V of *points* together with the collection of distinguished subsets, called *affine subspaces*, and the relation of *parallelism* on the latter, defined as follows:

- an affine subspace of $\mathrm{A}(V)$ is a coset of a linear subspace of V;
- two affine subspaces are *parallel* if they are cosets of the same linear subspace of V.

We write $X \parallel Y$ to denote that X and Y are parallel. A *real affine space* is an affine space of a real vector space. An *affine line* is a parallel of a 1-

dimensional linear subspace. An *affine hyperplane* is a parallel of an $(n-1)$-dimensional linear subspace.

Parallelism is an equivalence relation and all parallels to a given subspace partition the set of points. An *automorphism* of $\mathrm{A}(V)$ is a permutation of V preserving containment and parallelism amongst affine subspaces. So $g \in \mathrm{Sym}(V)$ belongs to the group $\mathrm{Aut}(\mathrm{A}(V))$ of all automorphisms of $\mathrm{A}(V)$ if and only if, for each pair (X, Y) of affine subspaces of $\mathrm{A}(V)$, we have $gX \subseteq gY$ if $X \subseteq Y$ and $gX \parallel gY$ if $X \parallel Y$.

Example 3.1.2 Consider the field $\mathbb{F}_3$ of order 3. The affine space of $\mathrm{A}(\mathbb{F}_3^2)$ is also called the *affine plane of order* 3. It has nine points, twelve lines, and four classes of parallel lines. See Figure 3.1.

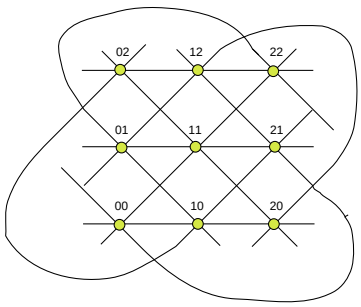


Fig. 3.1. The affine plane of order 3. Only three of the four parallel classes of lines are drawn: the three vertical lines are missing.

Definitions 3.1.3 If Y is a coset of a linear subspace of V of dimension d, then we say that Y is of *dimension* d as well. In particular, $\mathrm{A}(V)$ has *dimension* $\dim(V)$. We write $\dim(Y)$ for d. The empty set has dimension -1. An affine subspace of dimension 0 or 1, respectively, is a singleton (i.e., consists of a single point) or an affine line, respectively.

If $\{S_i\}_{i \in J}$ is a collection of affine subspaces of $\mathrm{A}(V)$, the intersection $\cap_{j \in J} S_j$ is again an affine subspace. Thus, it makes sense to introduce, for any subset X of V, the subspace $\langle X \rangle$ *generated* (or *spanned*) by X as the intersection of all affine subspaces containing X.

Any three points of $\mathrm{A}(V)$ not on a line are in a unique affine plane, and so they span an affine plane. More generally, if X is a set of $n+1$ points not lying in an $(n-1)$-dimensional affine space, then $\dim \langle X \rangle = n$.

We describe the important automorphisms of $\mathrm{A}(V)$. The group $\mathrm{T}(V)$ of all translations of V is a subgroup of $\mathrm{Aut}(\mathrm{A}(V))$. For $v \in V$, we write t_v to denote the translation by v:

$$t_v x = x + v \qquad (x \in V).$$

A non-trivial translation can be characterized as an automorphism of $\mathrm{A}(V)$ fixing each parallel class and fixing no point. Consequently, if $\dim V \geq 2$, then $\mathrm{T}(V)$ is a normal subgroup of $\mathrm{Aut}(\mathrm{A}(V))$.

Proposition 3.1.4 *Let V be a vector space. The subgroup of* $\mathrm{Aut}(\mathrm{A}(V))$ *generated by* $\mathrm{T}(V)$ *and* $\mathrm{GL}(V)$ *is a semi-direct product with normal subgroup* $\mathrm{T}(V)$.

Conjugation of an element $g \in \mathrm{GL}(V)$ by t_b is given by

$$t_b g t_{-b} = t_{v-g(v)} g.$$

Proof. As each element of $\mathrm{GL}(V)$ fixes 0 and each non-trivial element of $\mathrm{T}(V)$ does not, the intersection of $\mathrm{T}(V)$ and $\mathrm{GL}(V)$ is trivial.

Suppose $x, a \in V$. If $g \in \mathrm{GL}(V)$), then

$$g t_a g^{-1}(x) = g(g^{-1}x + a) = g(g^{-1}x) + ga = t_{ga} x, \tag{3.1}$$

whence $gTg^{-1} \subseteq T$. The first assertion follows. A similar computation shows the final assertion. □

Definitions 3.1.5 The subgroup of $\mathrm{Aut}(\mathrm{A}(V))$ generated by $\mathrm{T}(V)$ and $\mathrm{GL}(V)$, usually denoted by $\mathrm{AGL}(V)$, is called the *affine linear group* of V.

Example 3.1.6 Let $\mathbb{F}_q$ be the field of order $q = p^m$ where p is a prime number and m a non-negative integer. Then it is known that $\mathrm{Aut}(\mathbb{F}_q)$ is a cyclic group of order m, generated by the mapping $\mathbb{F}_q \to \mathbb{F}_q$, $x \mapsto x^p$ (called a Frobenius automorphism).

If $V = \mathbb{F}_q^n$, then $\mathrm{T}(V)$ has order q^n, and $\mathrm{GL}(V)$ has order $(q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-1})$; see Exercise 1.8.1. We state without proof that, if $n \geq 2$, then $\mathrm{Aut}(\mathrm{A}(V))$ has order

$$m q^n \prod_{i=0}^{n-1} (q^n - q^i).$$

In particular, the affine plane of order 3 (Example 3.1.2) has a group of automorphisms of order 432, which coincides with $\mathrm{AGL}(V)$.

Special elements of $\mathrm{AGL}(V)$ are affine reflections.

Definition 3.1.7 An *affine reflection* on a real affine space $\mathrm{A}(V)$ is an element of $\mathrm{AGL}(V)$ of order 2 fixing an affine hyperplane. The fixed affine hyperplane is also called its *mirror*.

Exercise 3.4.3 gives an explicit description of an arbitrary affine reflection.

3.2 Groups generated by affine reflections

Any group G generated by a set $\{\rho_i \mid i \in [n]\}$ of involutions is a homomorphic image of a Coxeter group W: simply take the Coxeter matrix of type $M = (m_{ij})_{i,j\in[n]}$, where m_{ij} is the order of $\rho_i\rho_j$ and apply Theorem 1.2.4. In this section it is shown that, for G a subgroup of $\mathrm{AGL}(V)$ generated by certain affine reflections, this surjective homomorphism is actually an isomorphism.

Example 3.2.1 Consider the Coxeter diagram B_3 of the cube and the Euclidean space $\mathbb{R}^3$. Let Γ be the cube whose vertices are the points all of whose coordinates are ± 1. Construct the barycentric subdivision into triangles of the surface spanned by the faces of the cube. The triangles found in this way will be called *chambers*. Each chamber determines a unique vertex, edge, and face of Γ. We fix the chamber c of Γ associated with the vertex $v_1 = (1, 1, 1)$, the edge $v_2 = \{v_1, (1, -1, 1)\}$, the face $v_3 = v_2 \cup \{(1, 1, -1), (1, -1, -1)\}$.

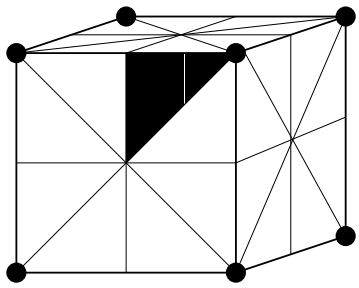


Fig. 3.2. The chambers of the Coxeter group of type B_3 drawn on the cube, with one chamber singled out.

In Figure 3.2, we have drawn the cube as the set of points $(\pm 1, \pm 1, \pm 1)$. The axes are chosen so that the positive x-axis and y-axis are horizontal, with the former pointing toward us and the latter to the right. The positive z-axis goes up. Now c corresponds to the chamber at the right hand top side of the left face. The chamber c determines three reflections ρ_1, ρ_2, ρ_3 leaving Γ invariant and generating the group G of 48 isometries of Γ. Here ρ_i is the reflection stabilizing v_{i+1} and v_{i+2} (indices mod 3). They are given by the matrices

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

The 48 transforms of the chamber c represent the 48 chambers of Γ and form a regular $W(\mathrm{B}_3)$-orbit.

For arbitrary groups generated by affine reflections, we will be looking for a set of domains similar to the above 48 chambers on which the group acts regularly.

Definition 3.2.2 If a group G acts on a set E, then a subset P of E is called a *prefundamental domain* for G if $P \neq \emptyset$ and $P \cap gP = \emptyset$ for all $g \in G \backslash \{1\}$.

Thus, the existence of a prefundamental domain for G acting on E implies that the action of G on E is faithful. Observe that a prefundamental domain need not quite be what is classically called a fundamental domain as it is not required that the domain be connected or contain a member of each G-orbit in E.

Example 3.2.3 Let $m \in \mathbb{N}$, $m \geq 2$. Consider the two vectors $\alpha_1 = (\sqrt{2}, 0)^\top$ and $\alpha_2 = \sqrt{2}(-\cos(\pi/m), \sin(\pi/m))^\top$ in Euclidean space $\mathbb{R}^2$ with standard inner product. These two vectors have squared norm 2 and make an angle of $\pi(1 - 1/m)$. The orthogonal reflections ρ_1 and ρ_2 (cf. Exercise 3.4.5) with roots α_1 and α_2, respectively, generate the dihedral group G of order $2m$. The product $\rho_1\rho_2$ is a rotation with angle $2\pi/m$. So there is an isomorphism $\gamma : W(M) \to G$ where M is the Coxeter matrix of size 2 with off-diagonal entry m, such that $\gamma(s_i) = \rho_i$ $(i = 1, 2)$. The two open half-planes A_1 and A_2, where $A_i = \{x \in \mathbb{R}^2 \mid x^\top \alpha_i > 0\}$ meet in a cone A_{12} bounded to the left by $\mathbb{R}_{\geq 0}(0, 1)^\top$ and to the right by $\mathbb{R}_{\geq 0}(\sin(\pi/m), \cos(\pi/m))^\top$. These half-lines make an angle of π/m and A_{12} is a prefundamental domain for G.

A characteristic property concerning the length $l(w)$ of an element of w of $W(M)$ with respect to $\{s_1, s_2\}$ that we will use later is the following.

$$l(s_i w) < l(w) \quad \Leftrightarrow \quad \gamma(w)A_{12} \subseteq \gamma(s_i)A_i.$$

It is readily verified in a picture like Figure 3.3 by observing that $l(w)$ is the minimal number of reflection hyperplanes separating a vector in wA_{12} from a vector in A_{12}.

Theorem 3.2.4 *Let $\{H_i \mid i \in I\}$ be a family of affine hyperplanes of the affine space $\mathrm{A}(V)$ of the real vector space V. For each $i \in I$, let A_i denote one of the two open half-spaces determined by H_i and write $A = \bigcap_{i \in I} A_i$. Assume that $A \neq \emptyset$. Furthermore, for each $i \in I$, let ρ_i be an affine reflection whose mirror in $\mathrm{A}(V)$ is H_i. Assume further that for $i \neq j$ in I, the intersection*

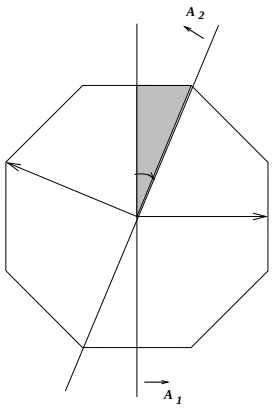


Fig. 3.3. A prefundamental domain for the dihedral Coxeter group of order 16.

$A_{ij} = A_i \cap A_j$ is a prefundamental domain for the subgroup G_{ij} of $\mathrm{AGL}(V)$ *generated by ρ_i and ρ_j. Then the following statements hold.*

(i) A is a prefundamental domain for the subgroup G of $\mathrm{AGL}(V)$ *generated by the ρ_i, $i \in I$.*

(ii) $(G, \{\rho_i \mid i \in I\})$ is a Coxeter system of type $M = (m_{ij})_{\{i,j \in I\}}$, where m_{ij} is the order of $\rho_i\rho_j$. In particular, $G \cong W(M)$.

Proof. Denote by M the Coxeter matrix $(m_{ij})_{i,j \in I}$, where m_{ij} is the order of $\rho_i\rho_j$, by (W, S) the corresponding Coxeter system, and by $\gamma : W \to G$, the homomorphism mapping $s_i \in S$ onto ρ_i of Theorem 1.2.4. Then γ establishes an action of W on $\mathrm{A}(V)$. We shall often write wX rather than $\gamma(w)X$ if $w \in W$ and $X \subseteq \mathrm{A}(V)$.

Denote by l the length function of the Coxeter system of (ii); cf. Definition 2.1.7. Here is a claim for each $q \in \mathbb{N}$.

> (P_q): For all $i \in I$ and $w \in W$ with $l(w) \leq q$, the domain wA is contained in either A_i or s_iA_i; in the latter case $l(s_iw) = l(w) - 1$.

We show that the truth of (P_q) for all q implies (i) and (ii). As for (i), assume that $w \in W$ satisfies $A \cap wA \neq \emptyset$. Then, for all i, we have $A_i \cap wA \neq \emptyset$ and so, by (P_q) for $q = l(w)$, as $A_i \cap s_iA_i = \emptyset$, we have $wA \subseteq A_i$. Hence $wA \subseteq A$. But the assumption on w also implies $w^{-1}A \cap A \neq \emptyset$, so that, similarly, $w^{-1}A \subseteq A$, and $A \subseteq wA$. Consequently $A = wA$. Moreover, $s_iwA = s_iA \subseteq s_iA_i$; by ($\mathrm{P}_q$) with $q = l(s_iw)$, this yields $l(s_i^2w) = l(s_iw) - 1$, i.e., $l(s_iw) = l(w) + 1$ for all $i \in I$. This means that w is the identity. Thus (i) holds for W (instead of G) and hence also for G. The argument also shows that the kernel of the homomorphism γ is trivial, so W is isomorphic to G and (ii) follows.

We next pursue the proof of (P_q). We proceed in four steps, and use induction on q.

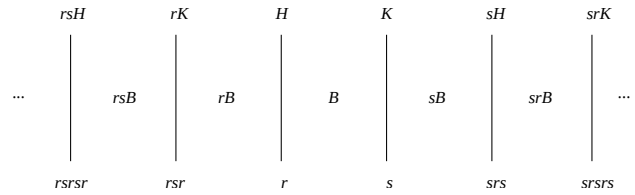


Fig. 3.4. The domains corresponding to the group generated by two affine reflections in the plane with parallel fixed lines. We have written r instead of ρ_1, s instead of ρ_2, H instead of H_1 and K instead of H_2. Observe that $\langle r, s\rangle = \mathrm{D}_\infty$.

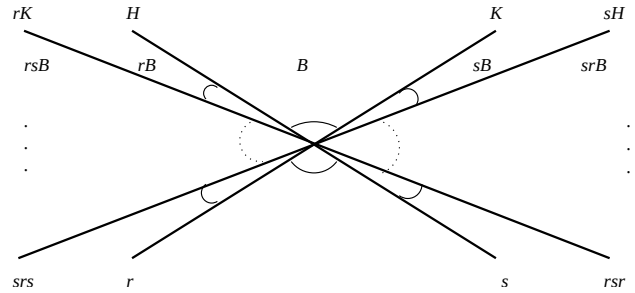


Fig. 3.5. The domains corresponding to the group generated by two affine reflections in the plane with intersecting fixed lines. We have written r instead of ρ_i, s instead of ρ_j, H instead of H_i and K instead of H_j. Observe that $\langle r, s\rangle = \mathrm{D}_{2m}$, where m is the order of rs.

STEP 1. (P_q) *holds if* $I = \{i, j\}$.

Put $r = \rho_i$ and $s = \rho_j$. For (P_q) distinguish the cases $H_i \parallel H_j$ and $H_i \nparallel H_j$. In the first case, the assumption that A_{ij} is a prefundamental domain for G_{ij} implies that A is the set of points strictly between H_i and H_j. Then $sA \subseteq A_i$, $rA \subseteq A_j$, $srA \subseteq sA_j$, etc. Now, it is clear from Figure 3.4 how to finish the proof of (P_q).

In the second case, $H_i \cap H_j$ is a subspace of codimension 2 and Figure 3.5 shows how to establish (P_q).

STEP 2. *For each pair* $i, j \in I$, *the group* G_{ij} *satisfies the hypotheses of the theorem.*

This is obvious.

Thus, in view of Step 1, we have (P_q) for every choice of G_{ij} instead of G. We proceed by induction on q. For $q = 0$, the claim (P_q) is trivial.

STEP 3. *Suppose* (P_q) *for some* $q \geq 1$. *Then, for each* $w \in W$ *with* $l(w) \leq q$ *and* $i \in I$, *we have* $l(s_i w) < l(w)$ *if and only if* $wA \subseteq s_i A_i$; *and also* $l(s_i w) > l(w)$ *if and only if* $wA \subseteq A_i$.

For, $l(s_i w) = l(w) - 1$ implies $l(s_i(s_i w)) = l(s_i w) + 1$, so ($\mathrm{P}_{q-1}$) gives $s_i wA \subseteq A_i$. The assertion now follows from (P_q).

STEP 4. (P_q) *implies* (P_{q+1}).
Let $w \in W$ with $l(w) = q+1$ and take $i \in I$. Choose $j \in I$ and $w' \in W$ such that $w = s_j w'$ and $l(w') = q$. By (P_q) and the observation at the beginning of the proof, $w'A \subseteq s_j A_j$ and $l(s_j w') = l(w') + 1$. In particular, $wA = s_j w' A \subseteq A_j$. If $j = i$, then we are done.

Suppose $j \neq i$. By Lemma 2.2.3, there exist $u \in \langle s_i, s_j \rangle$ and $v \in {}^{\{i,j\}}W$ such that $w' = uv$ and $l(w') = l_{ij}(u) + l(v) = l(u) + l(v)$. Now $v \in {}^{\{i,j\}}W$ implies $l(s_i v) > l(v)$ and $l(s_i v) > l(v)$. By Step 3, this gives $vA \subseteq A_{ij}$, so $w'A \subseteq uA_{ij}$. Then $wA = s_j w' A \subseteq s_j u A_{ij}$. Observe that $l_{ij}(s_j u) \leq l_{ij}(u) + 1 \leq l(w') + 1 = q + 1$. By Step 2, ($\mathrm{P}_{q+1}$) holds for $s_j u \in \langle s_i, s_j \rangle$, so $s_j u A_{ij}$ is contained in either A_i or $s_i A_i$, and in the latter case, $l_{ij}(s_i s_j u) = l_{ij}(s_j u) - 1$. In particular, $wA \subseteq A_i$ or $wA \subseteq s_i A_i$, which is the first statement of (P_{q+1}). If $wA \subseteq s_i A_i$, then $wA \subseteq s_j u A_{ij} \subseteq s_i A_i$, and

$$\begin{aligned} l(s_i w) &= l((s_i s_j u)(u^{-1} w')) \leq l(s_i s_j u) + l(u^{-1} w') \\ &\leq l_{ij}(s_i s_j u) + l(w') - l_{ij}(u) \quad \text{(see above)} \\ &\leq l_{ij}(s_j u) - 1 + q - l_{ij}(u) \leq q\,. \end{aligned}$$

Since $l(w) = q + 1$, we find $l(s_i w) = q = l(w) - 1$ and so (P_{q+1}) holds. □

Corollary 3.2.5 *Retain the conditions of Theorem 3.2.4 and let $\gamma : W(M) \to G$ be the isomorphism found in the theorem. Then, for all $i, j \in I$ and $w \in W$, the following assertions hold.*

(i) Either $\gamma(w)A \subseteq A_i$ and $l(s_i w) = l(w) + 1$,
or $\gamma(w)A \subseteq \gamma(s_i)A_i$ and $l(s_i w) = l(w) - 1$.
(ii) If $i \neq j$, there exists $w_{ij} \in \langle s_i, s_j \rangle$ such that $\gamma(w)A \subseteq \gamma(w_{ij})A_{ij}$ and $l(w) = l(w_{ij}^{-1} w) + l(w_{ij})$.

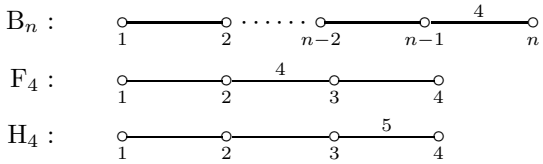
Proof. Part (i) follows from Step 3 of the proof of Theorem 3.2.4. As for (ii), by Lemma 2.2.3(ii), l_{ij} and l coincide on $\langle s_i, s_j \rangle$, so, the corollary follows directly from (i). □

Examples 3.2.6 (i). With the notation of Example 3.2.1, the group of 48 isometries of the cube is isomorphic to the Coxeter group $W(\mathrm{B}_3)$. Here A is a cone whose apex is the origin and whose radii run through the small triangle that bounds the chamber c, see Figure 3.2.

(ii). Each of the convex regular polytopes of a Euclidean space gives rise to a group of isometries that is a Coxeter group. As a result, the Coxeter groups of the types represented in Table 3.1 are finite; their orders can be computed by a count of chambers, using induction on n, in the same way as in (i). The diagrams as yet unexplained are:

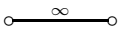
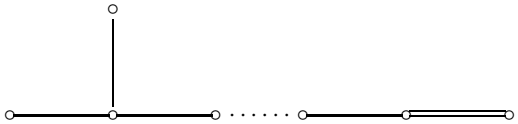
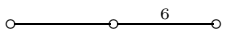
Table 3.1. Coxeter diagrams of some finite reflection groups related to polytopes

M	$\lvert W(M)\rvert$	restriction
A_n	$(n+1)!$	$n \geq 1$
$\mathrm{B}_n = \mathrm{C}_n$	$2^n(n!)$	$n \geq 2$
F_4	$24 \cdot 48 = 1152$	
H_3	120	
H_4	$120 \cdot 120 = 14400$	
$\mathrm{I}_2^{(m)}$	$2m$	$m \geq 2$



(ii). Each of the tilings of a Euclidean space by regular convex polytopes gives rise to an infinite group of isometries which is a Coxeter group. The diagrams of these infinite Coxeter groups are as in Table 3.2. We have included the tiling of $\mathbb{R}$ by unit intervals.

Table 3.2. Coxeter diagrams of some infinite reflection groups related to tilings

name	diagram	restriction
$\widetilde{\mathrm{A}}_1$		
$\widetilde{\mathrm{B}}_2 = \widetilde{\mathrm{C}}_2$		
$\widetilde{\mathrm{B}}_n$		$n \geq 3$
$\widetilde{\mathrm{C}}_n$		$n \geq 3$
$\widetilde{\mathrm{F}}_4$		
$\widetilde{\mathrm{G}}_2$		

3.3 Linear reflection representations

In this section, Theorem 3.2.4 will be applied to derive that the reflection representation is faithful. However, the prefundamental domain will be used for the contragredient representation rather than the reflection representation.

Definition 3.3.1 If $\rho : G \to \mathrm{GL}(V)$ is a linear representation on a vector space V, then the contragredient representation ρ^* is defined by

$$\rho_g^* f = (v \mapsto f(\rho_g^{-1} v))$$

for all $f \in V^*$, $g \in W$.

It is readily checked that ρ^* is also a linear representation of G.

Example 3.3.2 (The infinite dihedral group) Let (W, S) be the Coxeter system of rank $n = 2$ with Coxeter matrix determined by $m_{12} = \infty$. The linear representation ρ of W occurs in $V = \mathbb{R}^2$. On the basis $\{e_1, e_2\}$,

$$B(x, y) = 2x_1y_1 + 2x_2y_2 - 2x_1y_2 - 2x_2y_1 = 2(x_1 - x_2)(y_1 - y_2),$$

whence $\mathrm{Rad}(B) = \{x \in V \mid x_1 = x_2\}$. Moreover,

$$\rho_1 = \begin{pmatrix} -1 & 2 \\ 0 & 1 \end{pmatrix} \text{ and } \rho_2 = \begin{pmatrix} 1 & 0 \\ 2 & -1 \end{pmatrix}$$

fix all points of $\mathrm{Rad}(B)$. There is no convenient choice for A as in Theorem 3.2.4. However, ρ has a contragredient representation ρ^* on the dual vector space V^* which behaves much better. In matrix form, with respect to a dual basis $(f_i)_i$ of $(e_i)_i$ (that is, $f_i(e_j) = 1$ if $i = j$ and 0 otherwise), we have $\rho_g^* = (\rho_g)^{-\top}$ and so

$$\rho_1^* = \begin{pmatrix} -1 & 0 \\ 2 & 1 \end{pmatrix} \text{ and } \rho_2^* = \begin{pmatrix} 1 & 2 \\ 0 & -1 \end{pmatrix}.$$

Let a standard domain be represented by the set A of elements of V^* which take strictly positive values on e_1 and e_2, i.e., the set of all $(a, b)^\top \in \mathbb{R}^2$ with $a > 0$ and $b > 0$. Then the transforms $\rho_g^* \overline{A}$ of the closure $\overline{A}$ of A, cover an open half-plane of V^* bounded by the line $x_1 + x_2 = 0$ and the group acts regularly on the set of all those transforms, i.e., A is a prefundamental domain for this group; see Figure 3.6.

Example 3.3.3 (The finite dihedral groups) Let us consider once more the case $n = 2$ and $m = m_{12} < \infty$. Then B is positive definite and the matrices of ρ_1 and ρ_2 in the reflection representation with respect to e_1, e_2 are

$$\text{for } \rho_1 : \begin{pmatrix} -1 & 2\cos(\pi/m) \\ 0 & 1 \end{pmatrix}, \qquad \text{for } \rho_2 : \begin{pmatrix} 1 & 0 \\ 2\cos(\pi/m) & -1 \end{pmatrix}.$$

On the other hand, in Euclidean space $\mathbb{R}^2$ with standard inner product $(\cdot, \cdot)$ and standard orthonormal basis ε_1, ε_2, we can take the vectors $a = \varepsilon_1 =$

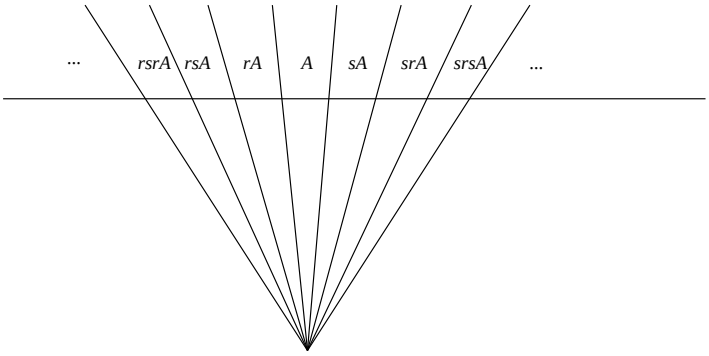


Fig. 3.6. The domain A and its transforms under $\rho^* W$.

$(1,0)^\top$ and $b = (-\cos(\pi/m), \sin(\pi/m))^\top$ of unit length which make an angle $-\cos(\pi/m)$ and consider the corresponding reflections r_a, r_b. Observe that the two pairs of reflections are actually the same up to a coordinate transformation sending the standard basis ε_1, ε_2 to $\sqrt{2}a$, $\sqrt{2}b$. In other words,

$$B = 2 \begin{pmatrix} 1 & -\cos(\pi/m) \\ 0 & \sin(\pi/m) \end{pmatrix}^\top \begin{pmatrix} 1 & -\cos(\pi/m) \\ 0 & \sin(\pi/m) \end{pmatrix}.$$

In Example 2.3.4, $\rho_i^\top = \rho_i$ for all i, whence $\rho = \rho^*$.

In general, for a Coxeter system (W, S) of type M and the corresponding reflection representation $\rho : W \to \mathrm{GL}(V)$, we will consider the contragredient representation ρ^* (see Definition 3.3.1) to prove that ρ is faithful. This is justified by the following result.

Lemma 3.3.4 $\operatorname{Ker} \rho = \operatorname{Ker} \rho^*$. *In particular, ρ is faithful if and only if ρ^* is faithful.*

Proof. This is Exercise 3.4.7. □

For $v \in V$, set $A_v = \{x \in V^* \mid x(v) > 0\}$. This is an open half-space in V^*.

Theorem 3.3.5 *Let $\rho : W \to \mathrm{GL}(V)$ be the reflection representation. Then, in V^*, the half-spaces $A_i = \{x \in V^* \mid x(e_i) > 0\}$ and the linear transformations $\rho_i^* \in \mathrm{GL}(V^*)$ satisfy the following conditions.*

(i) For each, $i \in [n]$, the transformation ρ_i^* is a reflection on V^* and A_i and $\rho_i^* A_i$ are the half-spaces separated by its mirror.

(ii) *For i, j in $[n]$ with $i \neq j$, the intersection $A_{ij} = A_i \cap A_j$ is a prefundamental domain for the subgroup G_{ij} of* $\mathrm{AGL}(V)$ *generated by ρ_i^* and ρ_j^*.*

(iii) *The intersection $\bigcap_{i\in[n]} A_i \neq \emptyset$ is a prefundamental domain for the subgroup G acting on V^*.*

(iv) *ρ is faithful.*

Proof. (i) is straightforward: for $f \in V^*$ and $i \in [n]$, put $a = B(\cdot, e_i)$ and $\phi = (h \mapsto h(e_i))$. Then

$$\rho_i^* f = f - f(e_i)B(\cdot, e_i) = r_{a,\phi} f,$$

with $\phi(a) = B(e_i, e_i) = 2$, so the assertion follows from Exercise 2.4.9.

(ii). Let $i, j \in [n]$ with $i \neq j$. Observe that G_{ij} is the image under ρ^* of $\langle s_i, s_j\rangle$. Consider $w \in \langle s_i, s_j\rangle$ with $A_{ij} \cap \rho_w^* A_{ij} \neq \emptyset$. We will show $w = 1$. Set $U = \mathbb{R}e_i + \mathbb{R}e_j$ in V. There is a canonical surjective linear map $\pi : V^* \to U^*$ obtained by restriction of each linear form f on V to U. The subgroup G_{ij} of $\mathrm{AGL}(V)$ leaves U invariant, since each ρ_k leaves invariant every linear subspace of V containing e_k, and $e_i, e_j \in U$. Let σ_w be the restriction of ρ_w to U, for $w \in \langle s_i, s_j\rangle$. Write $K_v = \{x \in U^* \mid x(v) > 0\}$ for $v \in U$. Then $K_v = \pi A_v$. Inspection of Examples 3.2.3 and 3.3.3 gives that the assertion holds if $n = 2$. Therefore, writing $K_i = K_{e_i}$ and $K_{ij} = K_i \cap K_j$, we find that $K_{ij} \cap \sigma_w^* K_{ij} \neq \emptyset$ implies $w = 1$.

Now $f \in A_{ij} \cap \rho_w^* A_{ij} \neq \emptyset$ implies that $f\,|_U \in \pi A_{ij} = K_{ij}$ and $f\,|_U \in \pi\rho_w^* A_{ij} = \sigma_w^* K_{ij}$ (see the analysis after the definition of ρ^*). Thus $f\,|_U \in K_{ij} \cap \sigma_w^* K_{ij}$ and so $w = 1$.

(iii). The intersection $\bigcap_{i\in[n]} A_i \neq \emptyset$ contains any linear form f taking the value 1 on each e_i, and so is non-empty. As we have seen before, the restriction of ρ to a subgroup $\langle s_i, s_j\rangle$ of w is faithful. In particular, $\rho_i^* \rho_j^*$ has order m_{ij}. In view of (ii), we can apply Theorem 3.2.4 to conclude that $(\rho^* W, \{\rho_i^* \mid i \in [n]\})$ is a Coxeter system of type M and that A is a prefundamental domain.

(iv). The proof of (iii) implies that ρ^* is faithful. The assertion now follows from Lemma 3.3.4. □

Corollary 3.3.6 *If (W, S) is a Coxeter system and J a subset of S, the subgroup $\langle J\rangle$ of W is a Coxeter group with Coxeter system $(\langle J\rangle, J)$.*

3.4 Exercises

Section 3.1

Exercise 3.4.1 A *semi-linear transformation* of a vector space V over a field $\mathbb{F}$ is a bijective map $g : V \to V$ for which there is an automorphism σ_g of $\mathbb{F}$ such that

$$g(v\lambda + w\mu) = (gv)\sigma_g(\lambda) + (gw)\sigma_g(\mu) \quad (\lambda, \mu \in \mathbb{F};\, v, w \in V)\,. \quad (3.2)$$

(a) Show that σ_g is uniquely determined by this equation; it is called the automorphism of $\mathbb{F}$ *induced* by g.
(b) Let $V = \mathbb{F}^n$ and let $\sigma \in \mathrm{Aut}(\mathbb{F})$. Define $g : V \to V$ by $gx = (\sigma x_i)_{i\in[n]}$. Verify that $g \in \mathrm{Aut}(\mathrm{A}(V))$.
(c) Prove that $\mathrm{Aut}(\mathrm{A}(V)) = \mathrm{Sym}(V)$ if $\dim(V) = 1$.

(It can be shown that, if $\dim(V) > 1$, the group $\mathrm{Aut}(\mathrm{A}(V))$ is generated by $\mathrm{AGL}(V)$ and all transformations as in (b)).

Exercise 3.4.2 Let $n \in \mathbb{N}$. Show that the affine group $\mathrm{AGL}(\mathbb{F}^n)$ is isomorphic to a subgroup of $\mathrm{GL}(\mathbb{F}^{n+1})$.
(*Hint:* View the affine space $\mathrm{A}(\mathbb{F}^n)$ as the affine hyperplane $\{x \in \mathbb{F}^{n+1} \mid x_{n+1} = 1\}$ of $\mathrm{A}(\mathbb{F}^{n+1})$ and extend the elements $\mathrm{AGL}(\mathbb{F}^n)$ to elements of $\mathrm{AGL}(\mathbb{F}^{n+1})$ fixing $0 \in \mathbb{F}^{n+1}$.)

Exercise 3.4.3 (Cited in Definition 3.1.7) Show that each affine reflection is of the form $t_{\lambda a} r_{a,\phi}$ for certain $a \in V$, $\phi \in V^*$, and $\lambda \in \mathbb{R}$ with $\phi(a) = 2$; see Exercise 2.4.9. Here, the mirror is $\{x \in V \mid \phi(x) = \lambda\}$.

Section 3.2

Exercise 3.4.4 Let $\rho : W(\mathrm{H}_3) \to \mathrm{GL}(V)$ be the reflection representation of $W(\mathrm{H}_3)$.

(a) Show that the symmetric bilinear form B on V associated with ρ is positive definite. Conclude that the image of $W(\mathrm{H}_3)$ under ρ is a group of isometries, that is, linear transformations preserving Euclidean distance.
(b) Find a $W(\mathrm{H}_3)$-orbit X of 12 vectors in V.
(c) Show that X is the set of vertices of a regular icosahedron in the Euclidean space determined by V and B.

Exercise 3.4.5 (Cited in Example 3.2.3 and Remark 4.1.4) Let V be a real vector space equipped with a symmetric bilinear form $\kappa : V \times V \to \mathbb{R}$. A reflection $r \in \mathrm{GL}(V)$ is called an *orthogonal reflection* (with respect to κ) if it preserves κ (in the sense that $\kappa(rx, ry) = \kappa(x, y)$ for all $x, y \in V$). Prove that, for $r_{a,\phi}$ as in Exercise 2.4.9 to be an orthogonal reflection, it is necessary and sufficient that either $\kappa(a, a) = 0$ and $a \in \mathrm{rad}(\kappa)$ or $\kappa(a, a) \neq 0$ and $\phi = (x \mapsto 2\kappa(a, a)^{-1}\kappa(x, a))$. In particular, if $\kappa(a, a) \neq 0$, there is a unique orthogonal reflection with root a.

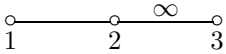
Exercise 3.4.6 Let $W = W(\mathrm{F}_4)$.

(a) Prove that the order of W is equal to 1152. Hint: study the permutation representation on roots of reflections with norm 1 (this will be the subject of the next lecture).
(b) Derive that W is a finite solvable group.
(*Hint:* Use the natural homomorphism $W \to W(\mathrm{A}_2 \,\dot\cup\, \mathrm{A}_2)$.)

Section 3.3

Exercise 3.4.7 (Cited in Lemma 3.3.4) Prove Lemma 3.3.4.

Exercise 3.4.8 We continue Exercise 2.4.13, retaining the notation ρ_i for $i = 1, 2, 3$ and writing M for the Coxeter diagram



There it was shown that the map $\{s_1, s_2, s_3\} \to \{\rho_1, \rho_2, \rho_3\}$ extends to a surjective group homomorphism $\psi : W(M) \to \mathrm{PGL}(2, \mathbb{Z})$. Set $V = \mathbb{R}^2$.

(a) By $V \otimes V$ we denote the tensor product of V with itself. Prove that there is a unique linear transformation $\sigma \in \mathrm{GL}(V \otimes V)$ of order 2 with $\sigma(x \otimes y) = y \otimes x$ for all $x, y \in V$.
(b) Let V^{2+} be the subspace of $V \otimes V$ linearly spanned by $f_1 = e_1 \otimes e_1$, $f_2 = \frac{1}{2}(e_1 \otimes e_2 + e_2 \otimes e_1)$, and $f_3 = e_2 \otimes e_2$ for a fixed basis e_1, e_2 of V. Prove that V^{2+} coincides with the subspace of $V \otimes V$ consisting of the fixed vectors of σ.
(c) Prove that there is a unique group homomorphism

$$\phi : \mathrm{GL}(V) \to \mathrm{GL}(V \otimes V)$$

determined by $\phi(g)(x \otimes y) = (gx) \otimes (gy)$ for $x, y \in V$.
(d) Show that for $g \in \mathrm{GL}(V)$, the map $\phi(g)$ leaves invariant V^{2+} and satisfies

$$B(\phi(g)x, \phi(g)y) = \det(g)^2 B(x, y) \qquad (x, y \in V^{2+}),$$

where B is the symmetric bilinear form on V^{2+} given by the matrix

$$\begin{pmatrix} 0 & 0 & 2 \\ 0 & -1 & 0 \\ 2 & 0 & 0 \end{pmatrix}$$

on the basis f_1, f_2, f_3.
(e) Verify that the respective images of ρ_1, ρ_2, ρ_3 under ϕ are

$$\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \qquad \begin{pmatrix} 1 & -1 & 1 \\ 0 & -1 & 2 \\ 0 & 0 & 1 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

and that these transformations are orthogonal reflections with respect to B (see Exercise 3.4.5) on V^{2+} with respective roots $(1, 0, -1)^\top$, $(1, 2, 0)^\top$, and $(0, 1, 0)^\top$.

(f) Prove that $\phi(\langle \rho_1, \rho_2, \rho_3 \rangle)$ is a Coxeter group of type M and deduce that $\phi \circ \psi$ is an isomorphism. Deduce that $\mathrm{PGL}(2, \mathbb{Z})$ is isomorphic to $W(M)$.

3.5 Notes

Section 3.1. For a synthetic approach to affine space, see [6, Chapter 5].

Section 3.2. Theorem 3.2.4 is due to Coxeter, who was the first to state results of this kind, and Tits, who proved the theorem in its full generality.

Section 3.3. For explorations of polytopes, see Coxeter's book [12].

4. The root system

In this chapter, we study Coxeter groups as permutation groups and derive some consequences regarding special subgroups and the defining presentation by generators and relations. Throughout, we let M be a Coxeter matrix of size n.

Let (W, S) be a Coxeter system of type M with $S = \{s_1, \ldots, s_n\}$. We think of S as a totally ordered set (by $s_i < s_j$ if and only if $i < j$) and frequently identify it with $[n]$.

Our starting point is the reflection representation $\rho : W \to \mathrm{GL}(V)$, which was proved faithful in Theorem 3.3.5. Here, the standard basis $e_1, \ldots, e_n$ of $V = \mathbb{R}^n$ consists of roots of the generating reflections $\rho(s_i) = \rho_i$ described in (2.3). Moreover the image of ρ lies in $\mathrm{O}(V, B)$, the stabilizer in $\mathrm{GL}(V)$ of the symmetric bilinear form B determined by (2.2). As a result we can view W as a group of real invertible $n \times n$ matrices generated by n orthogonal reflections with respect to B (cf. Exercise 3.4.5).

In Section 4.2 we use the root system to derive a characterization of Coxeter groups in terms of a property of minimal expressions of group elements with respect to a generating set of involutions, called the exchange condition.

Finally, Section 4.3 uses the exchange condition to provide a solution to the word problem for Coxeter groups. This solution is not efficient but quite practical in hand computations.

4.1 Root systems

Throughout this section, (W, S) is a Coxeter system of type M. Much like Proposition 1.5.3 (but without the finiteness restriction), we will single out a union of orbits of vectors in the reflection representation space V on which W acts faithfully, namely the set Φ below.

Definition 4.1.1 The subset $\Phi = \cup_{s \in S} \rho(W) e_s$ of V is the called the *root system* of W. The subsets

$$\Phi^+ = \Phi \cap (\mathbb{R}_{\geq 0} e_1 + \cdots + \mathbb{R}_{\geq 0} e_n) \qquad \text{and} \qquad \Phi^- = \Phi \cap (\mathbb{R}_{\leq 0} e_1 + \cdots + \mathbb{R}_{\leq 0} e_n)$$

are called the set of *positive roots* and the set of *negative roots* of W, respectively.

For the action of $w \in W$ on $v \in V$, we often write wv rather than $\rho(w)v$. Part (ii) of the following lemma justifies the name root system; recall Definition 2.3.1.

Proposition 4.1.2 *The root system of a Coxeter group W satisfies the following properties.*

(i) *W acts faithfully on Φ.*
(ii) *For $w \in W$ and $s \in S$ the vector $we_s \in \Phi$ is a root of the orthogonal reflection $\rho(wsw^{-1})$ with respect to B.*
(iii) *$\Phi = \Phi^+ \dot\cup \Phi^-$ and $\Phi^- = -\Phi^+$.*
(iv) *For $w \in W$ and $s \in S$ we have $we_s \in \Phi^-$ if and only if $l(ws) < l(w)$.*
(v) *If $\lambda \in \mathbb{R}$ and $\alpha \in \Phi$ satisfy $\lambda\alpha \in \Phi$, then $\lambda = \pm 1$.*

Proof. (i). As Φ contains the basis $(e_s)_{s\in S}$ of V, this is immediate from the fact (see Theorem 3.3.5) that ρ is faithful.

(ii). Since $\rho(wsw^{-1})$ is a conjugate of $\rho(s)$, it is an orthogonal reflection with respect to B. Moreover $wsw^{-1}(we_s) = wse_s = -we_s$, so we_s is a root of wsw^{-1}.

(iii). Let A_i and A be as in Theorem 3.3.5. Then $\Phi^+ = \{x \in \Phi \mid \forall_{f\in A} f(x) \geq 0\}$ and $\Phi^- = \{x \in \Phi \mid \forall_{f\in A} f(x) \leq 0\}$.

Let $w \in W$ and $s \in S$, so $we_s \in \Phi$. Since $f(we_s) = (w^{-1}f)e_s$ for $f \in V^*$, we have $we_s \in \Phi^+$ if and only if $f \in A_s$ for each $f \in w^{-1}A$, which is of course equivalent to $w^{-1}A \subseteq A_s$. Similarly, $we_s \in \Phi^-$ if and only if $w^{-1}A \subseteq sA_s$. By Theorem 3.3.5 and Corollary 3.2.5, either $w^{-1}A \subseteq A_s$ and $l(sw^{-1}) = l(w^{-1}) + 1$ or $w^{-1}A \subseteq sA_s$ and $l(sw^{-1}) = l(w^{-1}) - 1$. Therefore Φ is the union of Φ^+ and Φ^-. As $0 \notin \Phi$ this union is disjoint.

Finally, if $we_s \in \Phi^+$, then $-we_s = wse_s \in \Phi^-$, so $-\Phi^+ \subseteq \Phi^-$. Similarly $-\Phi^- \subseteq \Phi^+$, so $\Phi^- \subseteq -\Phi^+$. Therefore $\Phi^- = -\Phi^+$. This establishes (iii).

(iv). By what we have seen in the proof of (iii), $we_s \in \Phi^-$ if and only if $l(sw^{-1}) = l(w^{-1}) - 1$, which is equivalent to $l(ws) = l(w) - 1$; see Exercise 4.4.1. This proves (iv).

(v). Writing $\alpha = we_s$ we find $2 = B(e_s, e_s) = B(we_s, we_s)$, so $B(\alpha, \alpha) = 2$ for each $\alpha \in \Phi$. Consequently, $\alpha, \lambda\alpha \in \Phi$ gives $\lambda^2 2 = B(\lambda\alpha, \lambda\alpha) = 2$, and so $\lambda = \pm 1$. □

Definition 4.1.3 In view of Proposition 4.1.2(ii), the members of the set $R = \{wsw^{-1} \mid w \in W, s \in S\}$ are called *reflections* of W or, to be more precise, of (W, S).

Remark 4.1.4 By Proposition 4.1.2(iii), (v), each reflection of a Coxeter group W has a unique positive root. Conversely, by Exercise 3.4.5, each member of Φ^+ is the positive root of a unique orthogonal reflection with respect to B. In other words, if $r, s \in S$ and $v, w \in W$ satisfy $we_s = ve_r$, then $wsw^{-1} = vrv^{-1}$.

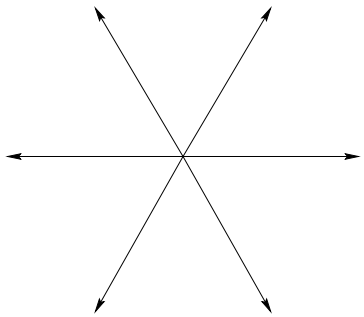


Fig. 4.1. The root system of the Coxeter group of type A_2

For $w \in W$ and Φ the root system of W, we set

$$\Phi_w := \{\alpha \in \Phi^+ \mid w\alpha \in \Phi^-\}. \tag{4.1}$$

Corollary 4.1.5 *Let $w \in W$ with $q = l(w)$ and let Φ be the root system of W. If $r_1 \cdots r_q$ is a minimal expression for w, then*

$$\Phi_w = \{r_q \cdots r_{i+1}\alpha_i \mid i \in [q]\},$$

where α_i is the root of r_i in Φ^+. In particular,

$$l(w) = |\Phi_w|.$$

Proof. Observe that the α_i are in $\{e_1, \ldots, e_n\}$, as each $r_i \in S$. Fix a minimal expression $r_1 \cdots r_q$ of w. As $l((r_q \cdots r_{i+1})r_i) < l(r_q \cdots r_{i+1})$, Proposition 4.1.2(iv) gives $r_q \cdots r_{i+1}\alpha_i \in \Phi^+$. Also, as $l((r_1 \cdots r_{i-1}r_i)r_i) < l(r_1 \cdots r_{i-1}r_i)$, Proposition 4.1.2(iv) gives $w(r_q \cdots r_{i+1}\alpha_i) = (r_1 \cdots r_{i-1}r_i)\alpha_i \in \Phi^-$. This establishes $\{r_q \cdots r_{i+1}\alpha_i \mid i \in [q]\} \subseteq \Phi_w$.

Let $\gamma \in \Phi_w$. It remains to show that γ belongs to $\{r_q \cdots r_{i+1}\alpha_i \mid i \in [q]\}$. If $q = 0$, then $\Phi_w = \emptyset$ and the corollary is trivially true.

Suppose $q = 1$, so $w = r_1 = s \in S$. Write $\gamma = \sum_{t\in S} \lambda_t e_t$ with $\lambda_t \geq 0$. If $\gamma \neq \alpha_1$, there must be $u \in S$ distinct from s with $\lambda_u > 0$; cf. Proposition 4.1.2(v). But then $s\gamma = \sum_{t\in S} \lambda_t se_t = \mu_s e_s + \sum_{t\in S\setminus\{s\}} \lambda_t e_t$ for some $\mu_s \in \mathbb{R}$. The coefficient of e_u in $s\gamma$ is again $\lambda_u > 0$, so $s\gamma \in \Phi^+$ by Proposition 4.1.2(iii). This means $\gamma \notin \Phi_{r_1}$ and so $\Phi_{r_1} = \{\alpha_1\}$, as required.

We proceed by induction on q. Assume $q > 1$ and $\gamma \in \Phi_w$. Since $w\gamma \in \Phi^-$ and $\gamma \in \Phi^+$, there is a maximal $i \leq q$ such that $\gamma, r_q\gamma, \ldots, r_{i+1} \cdots r_q\gamma \in \Phi^+$ and $r_i \cdots r_q\gamma \in \Phi^-$. But then $r_{i+1} \cdots r_q\gamma$ lies in Φ_{r_i}, which we have seen coincides with $\{\alpha_i\}$ in the previous paragraph. Thus, $r_{i+1} \cdots r_q\gamma = \alpha_i$ and $\gamma = r_q \cdots r_{i+1}\alpha_i$. This proves that the two sets Φ_w and $\{r_q \cdots r_{i+1}\alpha_i \mid i \in [q]\}$ coincide.

As a consequence $|\Phi_w| \leq q$. To prove equality, assume, that for certain i, j with $i < j$ we have $r_q \cdots r_{i+1}\alpha_i = r_q \cdots r_{j+1}\alpha_j$. Then $\alpha_i = r_{i+1} \cdots r_j\alpha_j$.

As $r_{i+1}\cdots r_j$ is a minimal expression, Proposition 4.1.2(iv) shows that the right hand side is in Φ^-, a contradiction with $\alpha_i \in \Phi^+$. Therefore, all elements of Φ_w are distinct, so $|\Phi_w| = q$. Hence the corollary. □

Example 4.1.6 Let $M = \mathrm{A}_{n-1}$. Then $B(e_i, e_j) = -1$ if $|i-j| = 1$ and $B(e_i, e_j) = 0$ if $|i-j| > 1$. Let $\varepsilon_1, \ldots, \varepsilon_n$ be the standard basis of $\mathbb{R}^n$ and $(\cdot,\cdot)$ the standard inner product that makes the standard basis orthonormal. A convenient realization of the reflection representation is furnished by the vectors $e_i = \varepsilon_i - \varepsilon_{i+1}$ $(i \in [n-1])$. These span the subspace $V = \mathbb{R}^n \cap \{\varepsilon_1 + \cdots + \varepsilon_n\}^\perp$ of $\mathbb{R}^n$ and B can be identified with the restriction of $(\cdot,\cdot)$ to V. The root system Φ for $W = W(\mathrm{A}_{n-1})$ can be partitioned into

$$\Phi^+ = \{\varepsilon_i - \varepsilon_j \mid 1 \le i < j \le n\} \text{ and}$$
$$\Phi^- = \{\varepsilon_i - \varepsilon_j \mid 1 \le j < i \le n\}.$$

Each element in Φ^+ is of the form $\varepsilon_i - \varepsilon_j = e_i + \cdots + e_j$ for certain $1 \le i < j \le n$. Corollary 4.1.5 gives that the length of $w \in \mathrm{Sym}_n$ is equal to the number of pairs (i,j) in $[n] \times [n]$ with $i < j$ and $w\,i > w\,j$.

4.2 The exchange condition

We first derive an abstract property of Coxeter groups that is very powerful. Next we explain its power by showing that it is a characterizing property for Coxeter groups.

Definition 4.2.1 Let (W, S) be a pair consisting of a group W and a generating set S for W. The *exchange condition* for (W, S) is the following property.

> If $s, r_1, \ldots, r_q \in S$ satisfy $w = r_1 \cdots r_q$ and $q = l(w) \ge l(sw)$, then there is $j \in [q]$ such that $sr_1 \cdots r_{j-1} = r_1 \cdots r_j$.

Theorem 4.2.2 *If (W, S) is a Coxeter system, then it satisfies the exchange condition.*

Proof. As the parities of $l(sw)$ and $l(w)$ differ (cf. Exercise 1.8.14), $l(sw) \le l(w)$ implies $l(sw) = l(w) - 1$. By Corollary 4.1.5 and $|\Phi_{sw}| = l(sw) = q - 1 < q = |\Phi_w|$, there is $\beta \in \Phi_w$ such that $sw\beta \in \Phi^+$. Moreover, if $r_1 \cdots r_q$ is a minimal expression for w, then $\Phi_w = \{r_q \cdots r_{i+1}\alpha_i \mid i \in [q]\}$, where α_i is the root of r_i in Φ^+. Thus, for β, there is $j \in [q]$ with $\beta = r_q \cdots r_{j+1}\alpha_j$. Now $-w\beta \in \Phi^+$ and $sw\beta \in \Phi^-$, so $-w\beta \in \Phi_s = \{\alpha_s\}$, so

$$\alpha_s = -w\beta = -(r_1 \cdots r_q)(r_q \cdots r_{j+1})\alpha_j = -r_1 \cdots r_j\alpha_j = r_1 \cdots r_{j-1}\alpha_j,$$

which implies $s = (r_1 \cdots r_{j-1})r_j(r_{j-1} \cdots r_1)$ by Remark 4.1.4, and establishes $sr_1 \cdots r_{j-1} = r_1 \cdots r_{j-1}r_j$, as required. □

In order to prove the converse, we need the following useful lemma.

Lemma 4.2.3 *Suppose that (W, S) is a pair consisting of a group W and a set S of involutions generating W that satisfies the exchange condition. Let M be the matrix over S (assuming some total ordering on S) whose r, s-entry m_{rs} is the order of rs. Suppose that F is a monoid affording a map $\sigma : S \to F$ such that for any two distinct $r, s \in S$ we have*

$$\underbrace{\sigma(r)\sigma(s)\sigma(r)\cdots}_{m_{rs}\text{ factors}} = \underbrace{\sigma(s)\sigma(r)\sigma(s)\cdots}_{m_{rs}\text{ factors}} \quad \text{if} \quad m_{rs} < \infty.$$

Then σ can be extended to a map $W \to F$, also called σ, such that $\sigma(w) = \sigma(r_1)\cdots\sigma(r_q)$ whenever $r_1 \cdots r_q$ is a minimal expression for w.

Proof. Recall from Definition 2.1.1 that $\mathrm{M}(S)$ denotes the free monoid on S. Clearly, σ can be extended to a homomorphism of monoids $\mathrm{M}(S) \to F$. Thus, for $\underline{r} = r_1 \cdots r_q \in \mathrm{M}(S)$, we have $\sigma(\underline{r}) = \sigma(r_1)\cdots\sigma(r_q)$.

For $w \in W$, let D_w be the set of all minimal expressions for w in $\mathrm{M}(S)$. We want to show that $\sigma(\underline{r}) = \sigma(\underline{r}')$ for all $\underline{r}, \underline{r}' \in D_w$. We proceed by induction on $l(w)$. If $l(w) = 1$, the exchange condition yields that $|D_w| = 1$, so this case is trivial.

Assume $q = l(w) > 1$, and let $\underline{r} = r_1 \cdots r_q$ and $\underline{r}' = r'_1 \cdots r'_q$ be two minimal expressions in $\mathrm{M}(S)$ for w. Put $r = r'_1$. We have $l(rw) < q$, so the exchange condition gives $rr_1 \cdots r_{j-1} = r_1 \cdots r_j$ for some $j \leq q$. We obtain $\underline{r}'' := rr_1 \cdots r_{j-1} r_{j+1} \cdots r_q \in D_w$. Comparing the first terms of $\underline{r}'$ and $\underline{r}''$ and applying the induction hypothesis to rw, we find $\sigma(\underline{r}') = \sigma(\underline{r}'')$. If $j < q$, then, comparing the last terms of $\underline{r}''$ and $\underline{r}$ and applying the induction hypothesis to wr_q, we find $\sigma(\underline{r}) = \sigma(\underline{r}'')$, and we are done.

It remains to consider the case where $j = q$. Then, replacing the pair $\underline{r}, \underline{r}'$ by $\underline{r}'', \underline{r}$, and using the same arguments, we obtain $\underline{r}''' = r_1 r r_1 \cdots r_{q-2} \in D_w$ with $\sigma(\underline{r}''') = \sigma(\underline{r})$. Repeating this process, we arrive at $\underline{u} = r_1 r r_1 \cdots$ and $\underline{v} = r r_1 r \cdots \in D_w$, each word involving only r, r_1 alternately, with $\sigma(\underline{u}) = \sigma(\underline{r})$ and $\sigma(\underline{v}) = \sigma(\underline{r}')$, while $w = rr_1 r \cdots = r_1 r r_1 \cdots$ (q terms). Now, by hypothesis, $\sigma(\underline{u}) = \sigma(\underline{v})$, and so $\sigma(\underline{r}) = \sigma(\underline{r}')$. In particular, the mapping σ is constant on D_w for each $w \in W$, and hence well defined on W. □

Theorem 4.2.4 *Suppose that W is a group generated by a subset S of involutions.*

(i) The pair (W, S) is a Coxeter system if and only if it satisfies the exchange condition.

(ii) If (W, S) is a Coxeter system, then for each $w \in W$, there is a unique subset S_w of S such that $S_w = \{r_1, \ldots, r_q\}$ for every minimal expression $r_1 \cdots r_q$ for w.

Proof. (i). By Theorem 4.2.2, a Coxeter system satisfies the exchange condition. Suppose that (W,S) satisfies the exchange condition. Let M be the matrix over S as given in Lemma 4.2.3. Denote by $(\overline{W},\overline{S})$ the Coxeter system of type M. We shall apply the lemma to the canonical mapping $r \mapsto \overline{r}$ from S to $\overline{S}$, taking F to be the monoid underlying the group $\overline{W}$. By definition of $(\overline{W},\overline{S})$, this mapping satisfies the conditions of the lemma. Hence we obtain a mapping $w \mapsto \overline{w}$ from W to $\overline{W}$ such that $\overline{w} = \overline{r}_1 \cdots \overline{r}_q$ whenever $w = r_1 \cdots r_q$ and $q = l(w)$. We claim that $w \mapsto \overline{w}$ is a homomorphism.

First, we show that $\overline{sw} = \overline{s}\,\overline{w}$ for all $s \in S$, $w \in W$. If $l(sw) = q+1$, we have $\overline{sw} = \overline{s}\,\overline{r}_1 \cdots \overline{r}_q = \overline{s}\,\overline{w}$. If $l(sw) \leq q$, the exchange condition gives some $j \in [q]$ with $sr_1 \cdots r_{j-1} = r_1 \cdots r_j$, so $sw = r_1 \cdots r_{j-1} r_{j+1} \cdots r_q$, and $l(sw) = q-1$. As $\overline{r}_j^2 = 1$, we find

$$\begin{aligned}\overline{sw} &= \overline{r}_1 \cdots \overline{r}_{j-1}\overline{r}_{j+1} \cdots \overline{r}_q = \overline{r}_1 \cdots \overline{r}_{j-1}\overline{r}_j^2\overline{r}_{j+1} \cdots \overline{r}_q \\ &= \overline{r_1 \cdots r_j}\,\overline{r}_j\overline{r}_{j+1} \cdots \overline{r}_q = \overline{sr_1 \cdots r_{j-1}}\,\overline{r}_j\overline{r}_{j+1} \cdots \overline{r}_q \\ &= \overline{s}\,\overline{r}_1 \cdots \overline{r}_{j-1}\,\overline{r}_j\overline{r}_{j+1} \cdots \overline{r}_q = \overline{s}\,\overline{r_1 \cdots r_q} \\ &= \overline{s}\,\overline{w}.\end{aligned}$$

Next, we derive $\overline{u\,v} = \overline{u}\;\overline{v}$ for all $u, v \in W$ by induction on $l(u)$. The case $l(u) = 1$ has just been treated. Assume $l(u) > 1$. Then $u = s\,u'$ for some $s \in S, u' \in W$ with $l(u') < l(u)$, so

$$\overline{u\,v} = \overline{s(u'v)} = \overline{s}\,\overline{u'v} = \overline{s}(\overline{u'}\,\overline{v}) = (\overline{s}\,\overline{u'})\overline{v} = \overline{su'}\,\overline{v} = \overline{u}\,\overline{v},$$

proving that $w \mapsto \overline{w}$ is a homomorphism indeed. Finally the homomorphism is clearly surjective, and, since $\overline{W}$ is freely generated by the relations $(\overline{r}\,\overline{s})^{m_{rs}} = 1$ $(r, s \in S)$, it must be an isomorphism.

(ii). We now apply the lemma to the map $r \mapsto \{r\}$ from S to the monoid 2^S of all subsets of S in which multiplication is given by set theoretic union (the empty set is the unit). Since $\{r\} \cup \{s\} \cup \{r\} \cup \cdots = \{r, s\}$, the equality of Lemma 4.2.3 is satisfied. Therefore, the map can be extended to a map $w \mapsto S_w$ such that $S_w = \{r_1, \ldots, r_q\}$ for every minimal expression $r_1 \cdots r_q$ of w. □

Notation 4.2.5 For a subset T of S, the subgroup $\langle T \rangle$ of W generated by T is often denoted by W_T. Thus, $W_\emptyset = \{1\}$ and $W_S = W$.

Corollary 4.2.6 *Let (W,S) be a Coxeter system. Suppose that J and K are subsets of S.*

(i) If $w \in W_J$, then $S_w \subseteq J$. In particular, $S \cap W_J = J$.
(ii) $W_J \cap W_K = W_{J \cap K}$.
(iii) $J \subseteq K \iff W_J \subseteq W_K$.

Proof. (i). If $r_1 \cdots r_q$ is a minimal expression for w, then $r_q \cdots r_1$ is a minimal expression for w^{-1}, so, by (ii) of the theorem, $S_w = S_{w^{-1}}$. Furthermore, by

the exchange condition, $S_{rw} \subseteq \{r\} \cup S_w$ for any $r \in S$, so $S_{vw} \subseteq S_v \cup S_w$ for all $v, w \in W$. Hence $\{w \in W \mid S_w \subseteq J\}$ is a subgroup of W_J containing J. Consequently, $W_J = \{w \in W \mid S_w \subseteq J\}$. Statement (i) follows directly.

(ii). If $w \in W_J \cap W_K$, then by (i) the set S_w is contained in $J \cap K$. Hence $w \in W_{J\cap K}$, and $W_J \cap W_K \subseteq W_{J\cap K}$. The converse inclusion is obvious.

(iii). This is a direct consequence of (ii). □

Recall the notions left-reduced and right-reduced from Definition 2.2.2.

Definition 4.2.7 Let $J, K \subseteq S$. Then ${}^JW^K := {}^JW \cap W^K$ is called the set of (J, K)-*reduced* elements.

Proposition 4.2.8 *Let (W, S) be a Coxeter system and let J, K, L be subsets of S. Then the following assertions hold.*

(i) *If $w \in W_K W_L$ then there are $x \in W_K$ and $y \in W_L$ such that $w = xy$ and $l(w) = l(x) + l(y)$.*
(ii) *$W_J \cap W_K W_L = (W_J \cap W_K)(W_J \cap W_L)$.*
(iii) *For each $w \in W$ there is a unique $d \in {}^JW^K$ of minimal length. The set ${}^JW^K$ consists of all such d for $w \in W$.*
(iv) *For $w \in W$ and $d \in {}^JW^K \cap W_J w W_K$, each $u \in W_J w W_K$ can be written as $u = xdy$ with $x \in W_J$, $y \in W_K$ and $l(u) = l(x) + l(d) + l(y)$.*

Proof. (i). Suppose $w = xy$ for certain $x \in W_K$ and $y \in W_L$. Obviously, $l(x) + l(y) \geq l(w)$. Let $r_1 \cdots r_t$ and $r_{t+1} \cdots r_q$ be minimal expressions for x and y, respectively, so $q = l(x) + l(y)$. If $q = l(w)$, we are done. Otherwise, take the largest $j \leq t$ such that $r_j \cdots r_q$ is not a minimal expression. Then, by Theorem 4.2.2 there is $k \in \{j+1, \ldots, q\}$ such that $r_j \cdots r_q = r_{j+1} \cdots r_{k-1} r_{k+1} \cdots r_q$. If $k \leq t$, then $x = r_1 \cdots r_{j-1} r_{j+1} \cdots r_{k-1} r_{k+1} \cdots r_t$, contradicting $l(w) = t$. Therefore $k > t$. Take $x_1 = r_1 \cdots r_{j-1} r_{j+1} \cdots r_t$ and $y_1 = r_{t+1} \cdots r_{k-1} r_{k+1} \cdots r_q$. Then $l(x_1) + l(y_1) = q - 2$, $x_1 \in W_K$, $y_1 \in W_L$ whereas $w = xy = x_1 y_1$, and we finish by induction on $l(x) + l(y)$.

(ii). Clearly, $(W_J \cap W_K)(W_J \cap W_L) \subseteq W_J \cap W_K W_L$. As for the converse, let $w \in W_J \cap W_K W_L$. Then, by (i), there are $x \in W_K$, $y \in W_L$ with $w = xy$ and $l(x) + l(y) = l(w)$, so if $r_1 \cdots r_t$ and $r_{t+1} \cdots r_q$ are minimal expressions for x and y, respectively, then $r_1 \cdots r_q$ is a minimal expression for w. As $w \in W_J$, Corollary 4.2.6(i) gives $r_i \in J$ for $1 \leq i \leq q$ so $x = r_1 \cdots r_t \in W_J$ and similarly for y. This establishes $w \in (W_J \cap W_K)(W_J \cap W_L)$.

(iii). Let d be an element of minimal length in $W_J w W_K$. Then, clearly, $W_J w W_K = W_J d W_K$. Suppose $u \in W_J d W_K$. Then by the same kind of reasoning as in (i), we obtain that $u = xdy$ with $x \in W_J$ and $y \in W_K$ such that $l(u) = l(x) + l(d) + l(y)$. It follows that if $l(u) = l(d)$, then $u = d$. This settles uniqueness of d. Also, by minimality of $l(d)$, we have $d \in {}^JW^K$. Conversely, assume $v \in {}^JW^K$. Let d be the element of minimal length in $W_J v W_K$. Then

$v = xdy$ for certain $w \in W_J$, $y \in W_K$ with $l(v) = l(x) + l(d) + l(y)$. If $l(x) > 0$, then there is $r \in J$ such that $l(rx) < l(x)$. But then $l(rv) < l(v)$ contradicting $v \in {}^JW^K$. Hence $l(x) = 0$. Similarly, $l(y) = 0$. Consequently $v = d$, proving that ${}^JW^K$ is the set of all elements of minimal length in the double coset they represent.

(iv). Follows from the proof of (iii). □

Notation 4.2.9 For $r, s \in S$ with $m_{rs} < \infty$, write

$$\underline{w}_{ts} = \underbrace{rsr\cdots}_{m_{rs} \text{ factors}} \in \mathrm{M}(S),$$

and, using $\delta : \mathrm{M}(S) \to W(M)$ of Remark 2.1.6, put

$$w_{rs} = \delta(\underline{w}_{rs}).$$

Lemma 4.2.10 *If $l(sw) = l(tw) < l(w)$, then $m_{st} < \infty$ and there is $v \in {}^{\{s,t\}}W$ with $w = w_{st}v$ and $l(w) = m_{st} + l(v)$.*

Proof. By Lemma 2.2.3 there exists $u \in \langle s, t\rangle$ and $v \in {}^{\{s,t\}}W$ with $w = uv$ and $l(w) = l(u) + l(v)$. It remains to show $m_{st} < \infty$ and $u = w_{st}$. Let $r_1 \cdots r_k$ be a minimal expression for u and $r_{k+1} \cdots r_q$ a minimal expression for v, so $r_1 \cdots r_q$ is a minimal expression for w. As $l(sw) < l(w)$, Theorem 4.2.2 shows the existence of $j \in [q]$ with $sr_1 \cdots r_j = r_1 \cdots r_{j+1}$. If $j > k$, then $v' = r_{k+1} \cdots r_j r_{j+2} \cdots r_q$ satisfies $l(v') < l(v)$ and $sw = uv'$, so $\langle s, t\rangle v = \langle s, t\rangle v'$, contradicting $v \in {}^{\{s,t\}}W$. Therefore, $j \leq k$ and so $l(su) \leq l(u)$. Similarly $l(tu) \leq l(u)$. By inspection of the dihedral group $\langle s, t\rangle$, it is readily verified that $m_{st} < \infty$ and $u = w_{st}$, as required. □

4.3 Solution of the word problem

As another application of Lemma 4.2.3 we show how the word problem for a Coxeter group can be solved. It is no longer a surprise that the word problem for Coxeter groups can be solved as the faithful matrix representation provides an easy solution. Nevertheless a solution within the framework of words is still very useful.

Let (W, S) be a Coxeter system of type M, so $W = W(M)$. Recall the homomorphism of monoids $\delta : \mathrm{M}(S) \to W$ of Remark 2.1.6. For two words $a, b \in \mathrm{M}(S)$, we shall write $a \rightsquigarrow b$ for the rewrite rule that allows us to replace any occurrence of a in a word of $\mathrm{M}(S)$ by b. Recall Notation 4.2.9.

Theorem 4.3.1 *Consider the following rewrite rules for words in* $\mathrm{M}(S)$.

$$\underline{w}_{rs} \rightsquigarrow \underline{w}_{sr} \quad \text{if} \quad m_{rs} < \infty$$
$$ss \rightsquigarrow \varepsilon$$

Clearly, δ maps both sides of each rule to the same element of $W(M)$. By means of these rules,

(i) each word can be rewritten to a minimal expression;
(ii) every two minimal expressions of the same element of $W(M)$ can be transformed into each other.

Proof. (ii). Since the rules of the first kind are symmetric, they can be used in both directions, and the relation $\sim$ on $\mathrm{M}(S)$ defined by $\underline{r} \sim \underline{t}$ if $\underline{r}$ can be obtained from $\underline{t}$ by a series of rewrites of the first kind, is a congruence relation on the monoid $\mathrm{M}(S)$; cf. Definitions 2.1.3.

Suppose $r_1 \cdots r_q$ and $t_1 \cdots t_q$ are two minimal expressions in $\mathrm{M}(S)$ of $w \in W$. We wish to show that they are equivalent under $\sim$. If $q = 0$, this is trivial. We proceed by induction on q and assume $q > 0$. If $r_1 = t_1$, we apply the induction hypothesis to the two minimal expressions $r_2 \cdots r_q$ and $t_2 \cdots t_q$ of $r_1 w$, and we are done. Therefore, we may assume $r_1 \neq t_1$. Similarly, $r_q \neq t_q$.

Put $r = r_1$ and $t = t_1$. As $l(rw) = l(tw) < l(w)$, Lemma 4.2.10 implies the existence of a minimal expression of the form $\underline{w}_{rt}\underline{v}$ of w. As $\underline{w}_{rt}$ starts with r, the previous paragraph gives $\underline{r} \sim \underline{w}_{rt}\underline{v}$. Similarly, $\underline{t} \sim \underline{w}_{tr}\underline{v}$, and we are done, as obviously $\underline{w}_{rt} \sim \underline{w}_{tr}$.

(i). Suppose $\underline{r} = r_1 \cdots r_q$ is an expression in $\mathrm{M}(S)$ for w that is not minimal. We show that $\underline{r}$ is congruent to an expression containing a subword ss for some $s \in S$. This is trivially true if $q \leq 1$. We proceed by induction and assume $q \geq 2$. In view of the induction hypothesis, we may assume that $r_2 \cdots r_q$ is a minimal expression. Now Theorem 4.2.2 gives $j \in \{2, \ldots, q\}$ such that $r_2 \cdots r_j$ and $r_1 \cdots r_{j-1}$ are two minimal expressions for the same element of W. By (ii), $r_2 \cdots r_j \sim r_1 \cdots r_{j-1}$, and so $(r_2 \cdots r_{j-1}) r_j r_j (r_{j+1} \cdots r_q) = (r_2 \cdots r_j)(r_j \cdots r_q) \sim \underline{r}$. □

Remark 4.3.2 Theorem 4.3.1 suggests the following solution of the word problem:

I. Given a word $\underline{s}$, compute the set $H(\underline{s})$ of all its homogeneous rewrites (those obtained by applying rule (i)). If one of these contains an occurrence ss for some $s \in S$, remove this occurrence and replace $\underline{s}$ by the resulting element and recur. In this way we obtain a set $H(\underline{r})$ of all homegeneous rewrites of a minimal expression $\underline{r}$.

II. Given two words $\underline{s}$ and $\underline{r}$, apply I. to each so as to obtain two sets $H(\underline{r}_1)$ and $H(\underline{t}_1)$ where $\underline{r}_1$ and $\underline{t}_1$ are minimal expressions of $\delta(\underline{r})$ and $\delta(\underline{t})$, respectively. Now $\underline{r}$ and $\underline{s}$ represent the same element of $W(M)$ if and only if $H(\underline{r}_1) = H(\underline{t}_1)$.

The complexity of this procedure is governed by the size of $H(\underline{r})$. If $M = \mathrm{A}_{n-1}$ and $\underline{r}$ is a minimal expression of a particular (in fact, the longest) element of $W(M)$, then

$$|H(\underline{r})| = \frac{\binom{n}{2}!}{1^{n-1}3^{n-2}5^{n-3}\cdots(2n-1)^0}.$$

(We do not prove this.) So the complexity grows faster than exponentially.

On the other hand, the algorithm is practical for hand computations. For example: $123123123123 \in \mathrm{M}([3])$ represents the identity in $W(\mathrm{A}_3)$, as

$$\begin{aligned} 12\underline{31}23123123 &\rightsquigarrow 121\underline{323}123123 \rightsquigarrow 1\underline{212}32123123 \rightsquigarrow \\ &\underline{11}2132123123 \rightsquigarrow 213\underline{212}3123 \rightsquigarrow 21\underline{31}213123 \rightsquigarrow \\ &2\underline{11}3213123 \rightsquigarrow 232\underline{13}123 \rightsquigarrow 2323\underline{11}23 \rightsquigarrow \\ &\underline{232}323 \rightsquigarrow 32\underline{33}23 \rightsquigarrow 3\underline{22}3 \rightsquigarrow \underline{33} \rightsquigarrow \varepsilon. \end{aligned}$$

Here the underlining indicates the subword that is being rewritten in the next step.

Example 4.3.3 If (W, S) is the Coxeter system of type A_n, then W is doubly transitive on W/W_J, where $S = \{s_1, \ldots, s_n\}$ and $J = \{s_2, \ldots, s_n\}$. To see this, we use the fact that W is doubly transitive on W/W_J if and only if W consists of two double cosets with respect to W_J. Now W_J is a single double coset and does not contain s_1, so $W_J s_1 W_J$ is another. Therefore, double transitivity of W on W/W_J is equivalent to $W = W_J \cup W_J s_1 W_J$. In view of Proposition 4.2.8(iii), this amounts to ${}^J W^J = \{1, s_1\}$, so we need to show that 1 and s_1 are the only elements of ${}^J W^J$. If $n = 1$, then $J = \emptyset$ and ${}^J W^J = W = \{1, s_1\}$, so we are done.

Suppose $n \geq 2$ and use induction on n. It suffices to show $s_1 W_J s_1 \subseteq W_J s_1 W_J \cup W_J$. For, if this holds, then $W_J s_1 W_J \cup W_J$ is a subgroup of W and so coincides with $\langle W_J, s_1 \rangle = W$. Suppose, therefore, $w \in s_1 W_J s_1$. Then there is $v \in W_J$ such that $w = s_1 v s_1$. By the induction hypothesis applied to v we find $a, b \in W_{J\setminus\{s_2\}}$ and $v_1 \in {}^{J\setminus\{s_2\}}W_J^{J\setminus\{s_2\}} = \{1, s_2\}$ such that $v = a v_1 b$. Now either $v_1 = s_1$ and $w = s_1 a b s_1 = a s_1^2 b = ab \in W_J$ or $v_1 = s_2$ and $w = s_1 a s_2 b s_1 = a s_1 s_2 s_1 b = a s_2 s_1 s_2 b \in W_J s_1 W_J$, a contradiction.

4.4 Exercises

Section 4.1

Exercise 4.4.1 (Cited in proof of Proposition 4.1.2) Prove the following extension to Exercise 2.4.8: $l(w^{-1}) = l(w)$ and $\Phi_{w^{-1}} = -w\Phi_w$ for each w in a Coxeter group W.

Exercise 4.4.2 Let v and w be elements of the Coxeter group W. Prove that $l(vw) = l(v) + l(w)$ holds if and only if $\Phi_w \subseteq \Phi_{vw}$.

Exercise 4.4.3 Let (W, S) be a Coxeter system of type M and rank n. For $j \in [n]$, define p_j to be the number of elements $w \in W$ such that $\{s \in S \mid we_s \in \Phi^+\}$ has size j.

(a) Prove that, for $M = \mathrm{A}_n$ (so $W \cong \mathrm{Sym}_{n+1}$), the number p_j is equal to the *Eulerian number* $\langle n+1; k\rangle$, giving the number of permutations on $n+1$ letters having exactly k permutation ascents. Here, an *ascent* of a permutation w on $n+1$ letters is a number $i \in [n]$ such that $wi < w(i+1)$.
(b) For $J \subseteq S$, define p_J to be the number of elements $w \in W$ such that $\{s \in S \mid we_s \in \Phi^+\} = J$. Prove that $p_J = \sum_{K \supseteq J} (-1)^{|K|+|J|} |W/W_K|$ for each $J \subseteq S$.
(*Hint:* Establish first $|\{w \in W \mid \{s \in S \mid we_s \in \Phi^+\} \supseteq J\}| = |W/W_J|$.)
(c) Show that

$$\sum_{j=0}^{n} p_j t^j = \sum_{K \subseteq S} \frac{|W|(t-1)^{|K|}}{|W_K|}.$$

Exercise 4.4.4 For a set X, denote by $\mathcal{P}(X)$, the *power set* of X, that is, the set of all subsets of X.

(a) Prove that the map $\phi : W \to \mathcal{P}(\Phi^+)$ given by $\phi(w) = \Phi_w$ for $w \in W$ is injective.
(b) Show that each Φ_w is closed in the sense that $\alpha, \beta \in \Phi_w$ implies $(\mathbb{R}_{\geq 0}\alpha + \mathbb{R}_{\geq 0}\beta) \cap \Phi \subseteq \Phi_w$.

Section 4.2

Exercise 4.4.5 Let v and w be elements of the Coxeter group W such that $l(vw) = l(v) + l(w)$. Prove

$$\Phi_{vw} = \Phi_w \cup w^{-1}\Phi_v.$$

Exercise 4.4.6 Let (W, S) be a Coxeter system and let J, K, L be subsets of S. Show that ${}^J W^K \cap W_J W_L W_K \subseteq W_L$.

Exercise 4.4.7 Let (W, S) be a Coxeter system and $J, K \subseteq S$.

(a) Prove that there is a bijection from ${}^J W^K$ onto the set of orbits of W_J on W/W_K.
(b) Prove that there is a bijection between the set of orbits of W_J on W/W_K and the set of orbits of W_K on W/W_J.

Exercise 4.4.8 Prove Corollary 3.3.6 by use of the exchange condition.

Exercise 4.4.9 Let (W, S) be a Coxeter system of type M, and suppose that J and K partition S. Prove that the following three statements are equivalent.

(a) $W = W_J W_K$.
(b) For all $s \in J$ and $t \in K$ we have $m_{s\,t} = 2$.
(c) $W = W_J \times W_K$.

SECTION 4.3

Exercise 4.4.10 Let $n \geq 3$. Let (W, S) be the Coxeter system of type A_n and set $J = [n]\backslash\{1, n\}$. Prove that ${}^J W^J$ has size 7 and give minimal expressions for its elements.

Exercise 4.4.11 Generalize the results of Example 4.3.3 as follows. Let (W, S) be the Coxeter system of type A_n and set $J = [n]\backslash\{k\}$ for some $k \in [n]$ with $k \leq n/2$.

(a) Prove that ${}^J W^J$ has size $k + 1$ and give minimal expressions for its elements.
(b) Derive that W_J has $k + 1$ orbits on W/W_J.

Exercise 4.4.12 Let $n \geq 2$ and let (W, S) be the Coxeter system of type B_n (defined in Example 3.2.6(i)). Set $J = S\backslash\{1\}$. Show that ${}^J W^J$ has size 3 and give minimal expressions for its elements.

Exercise 4.4.13 We consider once more the Coxeter diagram $\widetilde{\mathrm{A}}_2$ that is a triangle; it was introduced in Exercise 2.4.11. Prove that, for each $k \in \mathbb{N}$, the word $(123)^k \in \mathrm{M}([3])$ is a minimal expression for the corresponding Coxeter group element in $W(\widetilde{\mathrm{A}}_2)$. Conclude that $W(\widetilde{\mathrm{A}}_2)$ has infinite order.

Exercise 4.4.14 Let (W, S) be a Coxeter system of type M. By H we denote the algebra over the ring $\mathbb{Q}[t, t^{-1}]$ generated by elements T_w subject to the following relations, where $r, s \in S$.

$$T_s^2 = (t-1)T_s + t$$
$$\underbrace{T_r T_s T_r \cdots}_{m_{rs} \text{ factors}} = \underbrace{T_s T_r T_s \cdots}_{m_{rs} \text{ factors}}$$

This algebra is known as the *Hecke algebra* of type M. Prove the following four assertions.

(a) For each $w \in W$, there is an element $T_w \in H$ such that $T_w = T_{r_1} \cdots T_{r_q}$ for each minimal expression $r_1 \cdots r_q$ of w.
(b) The elements T_w $(w \in W)$ span H linearly.
(c) Specialising t to 1 gives a surjective homomorphism of rings from H to the group algebra $\mathbb{Q}[W]$ (cf. Exercise 1.8.11).
(d) H is a free $\mathbb{Q}[t, t^{-1}]$-module with basis T_w $(w \in W)$.

4.5 Notes

Section 4.1. The usual definition of root system is given in [2]. It differs from the one used in this section in that it has an integrality and a finiteness condition. In a later chapter, we will discuss these issues. The approach using the root system to prove properties of minimal expressions was known and probably introduced by Deodhar and Howlett, see [13].

Papi [29] has given a characterization of subsets of Φ^+ of the form Φ_w for some $w \in W$ as the subsets that are closed and whose complements in Φ^+ is also closed. He also shows that the element w is uniquely determined by Φ_w.

Section 4.2. The exchange condition can be found in [2]. In [14], a strong exchange condition appears.

Section 4.3. The Tits rewrite rules appearing in Theorem 4.3.1, originate from [37] and [25]. The number of minimal expressions for the longest word in $W(\mathrm{A}_{n-1}) = \mathrm{Sym}_n$ in Remark 4.3.2 is due to [36].

5. Finite Coxeter groups

This chapter is devoted to the classification of finite Coxeter groups. In Section 5.2 we first link finiteness of Φ and an upper bound on the word length to finiteness of W. In Section 5.3 we state and prove the classification. We begin, however, by showing that every finite reflection group is a Coxeter group.

5.1 Finite reflection groups

The purpose of this section is to establish that every finite linear group generated by reflections is a Coxeter group. The approach is to find in such a group a set S of reflections such that (G, S) is a Coxeter system.

Let V be a real vector space. We first recall some elementary facts on finite subgroups of $\mathrm{GL}(V)$.

Definition 5.1.1 A linear representation of a group G on a real vector space V is called *absolutely irreducible* if it is irreducible and, after extension of scalars to the complex numbers, the representation is still irreducible.

A symmetric bilinear form κ on a real vector space V is called *positive definite* if its corresponding quadratic form is positive definite, that is, $\kappa(x, x) \geq 0$ for all $x \in V$ with equality only if $x = 0$.

Lemma 5.1.2 *Let $\rho : G \to \mathrm{GL}(V)$ be a linear representation of a finite group G on a finite-dimensional real vector space V. Then there is a positive-definite symmetric bilinear form κ on V that is invariant under G. If, moreover, ρ is absolutely irreducible, then*

(i) each linear map $V \to V$ commuting with G is multiplication by a scalar;
(ii) the form κ is the unique G-invariant bilinear form on V up to scalar multiples.

Proof. As before, for the action of an element $g \in G$ on a vector $v \in V$, we will often suppress ρ and write gv rather than $\rho(g)v$. Take any positive-definite symmetric bilinear form κ_1 on V and consider the sum κ over all of its transforms by elements of G:

$$\kappa(x,y) := \sum_{g\in G} \kappa_1(gx, gy).$$

Then κ is a positive definite symmetric bilinear form on V that is invariant under G.

(i) Suppose that A is a linear map $V \to V$ commuting with G, and take an eigenvalue $\lambda \in \mathbb{C}$ of A. Then, after extension of the scalars to $\mathbb{C}$, we obtain the G-invariant subspace $\mathrm{Ker}\,(A - \lambda 1)$ of V. As A has an eigenvector with respect to λ, this subspace is nontrivial. Since G is absolutely irreducible, the subspace must be all of V, whence $A = \lambda 1$. This establishes (i).

(ii) Suppose that κ_2 is yet another G-invariant bilinear form. Since V is finite dimensional and κ_1 is nondegenerate, any element of V^* is of the form $y \mapsto \kappa_1(z, y)$ for a unique $z \in V$. In particular, for each $x \in V$, there is a unique vector $u(x)$ in V such that $\kappa_2(x, y) = \kappa_1(u(x), y)$ for each $y \in V$. It is readily seen that $u : V \to V$ is a linear map. Since κ_2 and κ_1 are invariant under G, the transformation u commutes with each member of G. Indeed,

$$\begin{aligned}\kappa_1(u(gx), y) &= \kappa_2(gx, y) = \kappa_2(x, g^{-1}y)\\ &= \kappa_1(ux, g^{-1}y) = \kappa_1(g(ux), y)\end{aligned}$$

for all x, $y \in V$. Since κ_1 is nondegenerate, $ug(x) = gu(x)$ for all $x \in V$. By (i), u is multiplication by a scalar, say $u = \alpha \cdot 1$, with $\alpha \in \mathbb{R}$. Then $\kappa_2 = \alpha\kappa_1$, as required. □

The following lemma covers part of the 2-dimensional case of the general result stated in Theorem 5.1.4.

Lemma 5.1.3 *Let V be a real 2-dimensional vector space supplied with a positive-definite symmetric bilinear form κ and let G a finite subgroup of $\mathrm{O}(V, \kappa)$ generated by two reflections with distinct mirrors. Write Φ for the set of roots of reflections in G having norm 2 with respect to κ. Suppose that $h \in V$ is a vector such that $\kappa(h, \alpha) \neq 0$ for all roots $\alpha \in \Phi$. Then there is a unique pair $\alpha, \beta \in \Phi$ such that $\kappa(h, \alpha) > 0$, $\kappa(h, \beta) > 0$ and each root $\gamma \in \Phi$ with $\kappa(h, \gamma) \geq 0$ is a linear combination with non-negative coefficients of α and β. Moreover $\kappa(\alpha, \beta) = -2\cos(\pi/m)$ for some $m \in \mathbb{N}$.*

Proof. Let r_α and r_β be two generating reflections of G. Then G is isomorphic to Dih_{2m}, where m is the order of $r_\alpha r_\beta$ and we recover the setting of Example 3.2.3. The result now follows from a comparison of $G\alpha \cup G\beta$ with the 2-dimensional root system of Dih_{2m}. □

Theorem 5.1.4 *Let V be a real vector space of dimension $n < \infty$ and G a finite subgroup of $\mathrm{GL}(V)$ generated by reflections.*

(i) *There is a set Δ of linearly independent roots of reflections in G such that each reflection in G has a root that is a linear combination with nonnegative coefficients of roots from Δ.*
(ii) *There is a set S of $|\Delta|$ reflections in G, each having a root from Δ as in (i), such that (G, S) is a Coxeter system.*

Proof. By Lemma 5.1.2 there is a positive definite symmetric bilinear form κ such that G is a subgroup of $\mathrm{O}(V, \kappa)$. In particular, each reflection of G is an orthogonal reflection with respect to κ. Let Φ be the set of roots of these reflections of norm 2. Then Φ is finite as G is finite. Consequently, the union of all mirrors of reflections in G does not cover V; in other words, there is a vector h in V not contained in any mirror of G. Let Φ^+ be the intersection of Φ with the half-space $\{x \in V \mid \kappa(h, x) \geq 0\}$.

Take Δ to be the set of roots in Φ^+ that cannot be written as a linear combination with positive coefficients of at least two elements of Φ^+. Let $\alpha, \beta \in \Delta$. By Lemma 5.1.3 we find $\kappa(\alpha, \beta) = -2\cos(\pi/m_{\alpha,\beta})$ for some $m_{\alpha,\beta} \in \mathbb{N}$. Consequently, the conditions of Theorem 3.2.4 are satisfied for the subgroup W of G generated by $S = \{r_\alpha \mid \alpha \in \Delta\}$, with $A_s = \{x \in V \mid \kappa(h, x) \geq 0\}$ for each $s \in S$. This proves (ii) provided we show $W = G$.

(i). We prove that the roots in Δ are linearly independent. Suppose that $\sum_{\alpha\in\Delta} \lambda_\alpha \alpha = 0$ for certain $\lambda_\alpha \in \mathbb{R}$. Put $\Sigma = \{\alpha \in \Delta \mid \lambda_\alpha > 0\}$ and $\Pi = \{\beta \in \Delta \mid \lambda_\beta < 0\}$. Then $v := \sum_{\alpha\in\Sigma} \lambda_\alpha \alpha = \sum_{\beta\in\Pi}(-\lambda_\beta)\beta$ satisfies $0 \leq \kappa(v, v) = -\sum_{\alpha\in\Sigma,\beta\in\Pi} \lambda_\alpha\lambda_\beta\kappa(\alpha, \beta) \leq 0$, so $\kappa(v, v) = 0$, and hence $v = 0$. Now $0 = \kappa(h, v) = \sum_{\alpha\in\Sigma} \lambda_a\kappa(h, \alpha) \geq 0$, so $\Sigma = \emptyset$, and similarly $\Pi = \emptyset$. Therefore, $\lambda_\alpha = 0$ for $\alpha \in \Delta$, which establishes that the roots in Δ are linearly independent. This completes the proof of (i).

(ii). By construction, $W \subseteq G$. Let $\gamma \in \Phi^+$. In order to establish $G \subseteq W$, it suffices to show $\gamma = w\alpha$ for some $\alpha \in \Delta$ and $w \in W$, for then $r_\gamma = wr_\alpha w^{-1} \in W$ and we are done as G is generated by reflections r_γ for $\gamma \in \Phi^+$. Suppose the contrary, and let γ be such that $\kappa(h, \gamma)$ is minimal for all choices of γ in $\Phi^+ \setminus \bigcup_{\alpha\in\Delta} W\alpha$. Write $\gamma = \sum_{\alpha\in\Delta} c_\alpha\alpha$ with $c_\alpha \geq 0$. As $\sum_{\alpha\in\Delta} c_\alpha\kappa(\gamma, \alpha) = \kappa(\gamma, \gamma) > 0$, there exists $\alpha \in \Delta$ with $\kappa(\gamma, \alpha) > 0$. Now $r_\alpha\gamma = \sum_{\beta\in\Delta\setminus\{\alpha\}} c_\beta\beta + (c_\alpha - \kappa(\gamma, \alpha))\alpha$ with $c_\beta > 0$ for some $\beta \in \Delta\setminus\{\alpha\}$ and so $r_\alpha\gamma \in \Phi^+$. Moreover, $\kappa(r_\alpha\gamma, h) = \kappa(\gamma, r_\alpha h) = \kappa(\gamma, h) - \kappa(\gamma, \alpha)\kappa(h, \alpha) < \kappa(\gamma, h)$, a contradiction with the minimality of $\kappa(h, \gamma)$. This gives $\gamma \in \bigcup_{\alpha\in\Delta} W\alpha$, as required. □

The intersection of all mirrors of reflections of G coincides with the intersection of all mirrors of reflections having roots in Δ. Hence, it is an $(n-|\Delta|)$-dimensional subspace of V each of whose vectors is fixed by G. Besides, it is orthogonal to the $|\Delta|$-dimensional subspace spanned by Δ. Therefore, we can restrict our attention to the latter subspace and, by the theorem, identify it with the reflection representation space of the corresponding Coxeter group.

In view of Theorem 5.1.4, a full determination of finite reflection groups hinges on the classification of finite Coxeter groups.

Example 5.1.5 Consider the cube as drawn in Figure 3.2 of Example 3.2.1. There are 9 reflections leaving the cube invariant. Let G be the group they generate. Any choice of a vector h in the black part of the front face of the figure leads to the choice of S as the set of reflections whose mirrors bound the black part. More precisely, set $\alpha_1 = (1, 0, -1)$, $\alpha_2 = (0, -1, 1)$, and $\alpha_3 = \sqrt{2}(0, 1, 0)$; then the black area coincides with the part of the cube surface consisting of all vectors x with $(x, \alpha_i) \geq 0$ for $i \in [3]$. The theorem gives that (G, S) is a Coxeter system, where S consists of the reflections with mirrors α_1, α_2, and α_3. Now $(\alpha_1, \alpha_3) = 0 = -2\cos(\pi/2)$, $(\alpha_1, \alpha_2) = -1 = -2\cos(\pi/3)$, and $(\alpha_2, \alpha_3) = -\sqrt{2} = -2\cos(\pi/4)$, and the Coxeter diagram B_3 emerges.

The orthogonal group $\mathrm{O}(n, \mathbb{R})$ shows that a group generated by reflections and leaving invariant a positive-definite symmetric bilinear form, need not be finite; see Exercise 5.4.1. The following result shows that, still, in the reflection representation of a Coxeter group W on the vector space V, two reflections generate a finite subgroup of W provided their roots span a positive-definite subspace of V. This result will be of use in Chapter 7, notably Theorem 7.2.9.

Lemma 5.1.6 *Suppose (W, S) is a Coxeter system, $\rho : W \to \mathrm{O}(V, B)$ is its reflection representation, and Φ is the corresponding root system Φ. If $\alpha, \beta \in \Phi$ span a positive-definite subspace of V with respect to B, then $\langle r_\alpha, r_\beta \rangle$ is a finite subgroup of W.*

Proof. If $w \in W$, then $\langle r_{w\alpha}, r_{w\beta} \rangle = w\langle r_\alpha, r_\beta \rangle w^{-1}$, so it suffices to prove the statement for a representative pair from each W-orbit of pairs of roots. By definition of Φ, we can choose the representative pair (α, β) in such a way that $\alpha = e_s$ for some $s \in S$. Also, as $r_\beta = r_{-\beta}$, we may assume $\beta \in \Phi^+$.

Write $\beta = \sum_{t \in S} \mu_t e_t$ and put $v = \beta - \mu_s e_s$. Now $\mu_t \geq 0$ for all t. If β and α are linearly dependent, then $\langle r_\alpha, r_\beta \rangle$ is of order 2 and there is nothing to prove. So suppose they are not. Then $v \neq 0$ and so $\mu_t > 0$ for at least one $t \in S \backslash \{s\}$.

Each root of a reflection in $\langle r_\alpha, r_\beta \rangle$ will be of the form $\lambda e_s + \mu v = (\lambda - \mu\mu_s)e_s + \sum_{t \in S\backslash\{s\}} \mu\mu_t e_t$, with λ and μ of the same sign. For, it suffices to prove the statement when the root is positive, in which case $\mu\mu_t \geq 0$ for all $t \in S\backslash\{s\}$, so $\mu \geq 0$, and $\lambda \geq \mu\mu_s \geq 0$.

Suppose now that $\langle r_\alpha, r_\beta \rangle$ is not finite. Then $r_\alpha r_\beta$ is a rotation of $\mathbb{R}e_s + \mathbb{R}v$ of infinite order and so, with respect to the positive-definite form induced by B, it is a rotation over an angle πa with a irrational. Now certain high powers of $r_\alpha r_\beta$ will be rotations over arbitrary small degrees. As a consequence, the image of e_s under a suitable power of $r_\alpha r_\beta$ will be of the form $\lambda e_s + \mu v$ with $\lambda > 0$ and $\mu < 0$, contradicting that the signs of λ and μ are equal for roots. □

5.2 Finiteness criteria

Recall from Definition 4.1.3 that the set of reflections of a Coxeter system (W, S) is the set $R = \bigcup_{w \in W} wSw^{-1}$. For $t \in R$, denote by α_t the unique positive root of t in Φ; cf. Remark 4.1.4.

Proposition 5.2.1 *Let (W, S) be a Coxeter system with set of reflections R. For $t \in R$ and $w \in W$, the following three statements are equivalent.*

(i) $l(tw) \leq l(w)$.
(ii) $\alpha_t \in \Phi_{w^{-1}}$.
(iii) If $r_1 \cdots r_q$ is an expression for w (not necessarily minimal), then there is $i \in [q]$ such that $tr_1 \cdots r_i = r_1 \cdots r_{i-1}$.

Proof.
(ii)⇒(iii). Suppose that $w = r_1 \cdots r_q$ with $r_i \in S$. Let $\alpha_t \in \Phi_{w^{-1}}$, that is, $\alpha_t \in \Phi^+$ and $w^{-1}\alpha_t \in \Phi^-$. Then there is $i \in [q]$ with $r_{i-1} \cdots r_1 \alpha_t \in \Phi^+$ and $r_i \cdots r_1 \alpha_t \in \Phi^-$. By Corollary 4.1.5, $r_{i-1} \cdots r_1 \alpha_t \in \Phi_{r_i} = \{\alpha_i\}$, where $\alpha_i = \alpha_{r_i}$, so, by Remark 4.1.4, $r_{i-1} \cdots r_1 t r_1 \cdots r_{i-1} = r_i$, whence $tr_1 \cdots r_{i-1} = r_1 \cdots r_{i-1} r_i$, proving (iii).
(iii)⇒(i). Take $q = l(w)$ in (iii), so tw has expression $r_1 \cdots r_{i-1} r_{i+1} \cdots r_q$ for some $i \in [q]$. The length of this expression is $q - 1$.
(i)⇒(ii). The two implications just proved show that each $w \in W$ and $t \in R$ with $w^{-1}\alpha_t \in \Phi^-$ satisfy $l(tw) \leq l(w)$. Suppose now that (ii) does not hold; then $w^{-1}\alpha_t \in \Phi^+$. As $t^2 = 1$, we then have $(tw)^{-1}\alpha_t \in \Phi^-$, so, replacing w by tw in the conclusion of the first sentence of this paragraph, we find $l(t(tw)) \leq l(tw)$, proving $l(tw) \geq l(w)$, which means that (i) does not hold (equality does not occur in view of the difference in parity between $l(w)$ and $l(tw)$). This establishes the required implication. □

Corollary 5.2.2 *Let (W, S) be a Coxeter system with set of reflections R. If $t \in R$ and $v, w \in W$ satisfy $l(tw) \leq l(w)$ and $l(tv) \leq l(v)$, then $l(v^{-1}w) < l(v^{-1}tw)$.*

Proof. By Proposition 5.2.1, for t, v, and w as in the hypotheses, we have $\alpha_t \in \Phi_{w^{-1}} \cap \Phi_{v^{-1}}$. Consequently, $-v^{-1}\alpha_t$ is the positive root of the reflection $v^{-1}tv$, so $-v^{-1}\alpha_t = \alpha_{v^{-1}tv}$, and

$$(w^{-1}v)\alpha_{v^{-1}tv} = -(w^{-1}v)v^{-1}\alpha_t = -w^{-1}\alpha_t \in \Phi^+.$$

Proposition 5.2.1 gives $l((v^{-1}tv)(w^{-1}v)^{-1}) \geq l((w^{-1}v)^{-1})$, which is equivalent to $l(v^{-1}tw) \geq l(v^{-1}w)$. □

Remark 5.2.3 Let (W, S) be a pair consisting of a group W and a generating set S for W. The *strong exchange condition* for (W, S) is the following property.

If $t \in R$ and $r_1, \ldots, r_q \in S$ satisfy $w = r_1 \cdots r_q$ and $l(tw) \leq l(w)$, then there is $j \in [q]$ such that $tr_1 \cdots r_{j-1} = r_1 \cdots r_j$.

By Proposition 5.2.1 this condition is satisfied in a Coxeter system. But the condition is stronger than the exchange condition of Definition 4.2.1 as q is no longer required to be the length of w and t varies over all reflections of (W, S) (cf. Definition 4.1.3) rather than S. Hence, in view of Theorem 4.2.4, the strong exchange condition also characterizes Coxeter groups.

The above details regarding the root system lead to several finiteness criteria for Coxeter groups.

Theorem 5.2.4 *The following statements regarding a Coxeter system (W, S) with S finite and R the set of all reflections of W are equivalent.*

(i) The group W is finite.
(ii) The root system Φ of W is finite.
(iii) There is a longest element in W (with respect to l).
(iv) There is a unique element $w \in W$ with $l(tw) < l(w)$ for all $t \in R$.
(v) There is a unique longest element in W (with respect to l).

Moreover, the elements of (iii) and (iv) coincide and have length $|\Phi^+|$.

Proof.

(i)⇒(ii). A look at Definition 4.1.1 shows that the root system Φ is the union of at most n orbits of W, so, if W is finite, then so is Φ.

(ii)⇒(iii). If Φ is finite, then, by Corollary 4.1.5, there is an upper bound to the values of the length function on W, so there is an element in W of greatest length.

(iii)⇒(iv). By (iii), there is a longest element w_0 of W. Then, by definition, $l(tw_0) < l(w_0)$ for all $t \in R$. Suppose that w_1 is an element of W with $l(tw_1) < l(w_1)$ for all $t \in R$. Then, by Corollary 5.2.2, for any $t \in R$, we have $l(w_0^{-1}w_1) < l(w_0^{-1}tw_1)$. Applying this inequality with the reflection $w_0tw_0^{-1} \in R$ instead of t, we find $l(w_0^{-1}w_1) < l(t(w_0^{-1}w_1))$ for all $t \in R$. This implies $w_0^{-1}w_1 = 1$, and so $w_0 = w_1$.

(iv)⇒(i). Let w be as in (iv). By Proposition 5.2.1 each positive root belongs to $\Phi_{w^{-1}}$, so, by Corollary 4.1.5, $|\Phi^+| = l(w^{-1})$ is finite. In view of Proposition 4.1.2(iii), $|\Phi| = 2|\Phi^+|$ is finite as well. According to Proposition 4.1.2(i), W acts faithfully on Φ and so W is finite.

(iv)⇔(v) follows directly from the fact that any $w \in W$ is a longest element if and only if $l(tw) < l(w)$ for all $t \in R$.

The final statement is a consequence of the proofs of (iv)⇒(i) and (iv)⇔(v). □

Corollary 5.2.5 *The longest element of W is the unique element of W with $l(sw) < l(w)$ for all $s \in S$.*

Proof. Let $w \in W$ satisfy $l(sw) < l(w)$ for each $s \in S$ and let $t \in R$. Then $\alpha_t \in \Phi^+$, so there are $\lambda_s \in \mathbb{R}_{\geq 0}$ such that $\alpha_t = \sum_{s\in S} \lambda_s e_s$. By Proposition 4.1.2(iv), $w^{-1}\alpha_t = \sum_{s\in S} \lambda_s w^{-1} e_s$ with $w^{-1}e_s \in \Phi^-$. Hence $w^{-1}\alpha_t \in \sum_{s\in S} \mathbb{R}_{\leq 0} e_s$, so $w^{-1}\alpha_t \in \Phi^-$ and, by Proposition 5.2.1, $l(tw) < l(w)$. In particular w satisfies the condition of Theorem 5.2.4(iii), hence also (iv), which states that w is the unique longest element of W. □

Definition 5.2.6 If $W(M)$ is finite, then we say that M is *spherical*. If $T \subseteq S$ is spherical, we denote by w_T the unique longest element of W_T.

The following result gives more information on the coset decomposition than its predecessor Lemma 2.2.3.

Corollary 5.2.7 *Suppose $w \in W$ and $T \subset S$ satisfy $l(tw) \leq l(w)$ for each $t \in T$. Then W_T is finite and there is $v \in {}^T W$ such that $w = w_T v$ with $l(w) = l(w_T) + l(v)$.*

Proof. By Lemma 2.2.3 there are $u \in W_T$ and $v \in {}^T W$ with $w = uv$ and $l(w) = l(u) + l(v)$. As $l(su) \leq l(u)$ for all $s \in T$, Corollary 5.2.5 implies $u = w_T$. □

Corollary 5.2.8 *If W is finite and $S \neq \emptyset$, then its longest element w_S satisfies the following properties.*

(i) $l(w_S) = |\Phi^+|$.
(ii) w_S *is an involution.*
(iii) For each $w \in W$, we have $l(ww_S) = l(w_S) - l(w) = l(w_S w)$.
(iv) The map $x \mapsto w_S x w_S$ $(x \in W)$ is an automorphism of W leaving invariant the subset S.

Proof.

(i) is already stated in Theorem 5.2.4.

(ii). According to Exercise 4.4.1, $l(w_S^{-1}) = l(w_S)$, so it follows from Theorem 5.2.4 that $w_S^{-1} = w_S$, that is, $w_S^2 = 1$. Clearly, $w_S \neq 1$ as $S \neq \emptyset$.

(iii). Fix $w \in W$. We apply Exercise 4.4.2 with $v = w_S w^{-1}$. As $\Phi_w \subseteq \Phi^+ = \Phi_{w_S}$, we find $l(w_S) = l(w_S w^{-1}) + l(w) = l(ww_S) + l(w)$, proving the first equality. As w_S is an involution (see (ii)), the second equality follows by inverting the arguments and replacing w by its inverse.

(iv). By (ii), w_S is an involution, so the map is conjugation by w_S. Let $s \in S$. Then $l(w_S s w_S) = l(w_S) - l(sw_S) = l(w_S) - l(w_S) + l(s) = 1$ by a double application of (iii). This implies $w_S s w_S \in S$. □

Remark 5.2.9 The fact that w_S preserves S under conjugation implies that it induces an automorphism on M. This automorphism is called the *opposition* on M. It is the identity if and only if w_S is in the center of the group W.

5.3 The classification

We have already given several examples of finite irreducible Coxeter groups. We shall now classify all of them.

There is no harm in restricting ourselves to irreducible groups; cf. Definition 2.2.4.

Lemma 5.3.1 *Let (W, S) be a Coxeter system of type M. Then W is finite if and only if W_J is finite for each connected component $J \subseteq S$ of the labelled graph M.*

Proof. This is immediate from Proposition 2.2.5. □

The quadratic form Q_M associated with the reflection representation of a Coxeter group was introduced in Definition 2.3.2.

Proposition 5.3.2 *For any Coxeter system (W, S) of type $M = (m_{ij})_{s,t\in S}$ such that W is irreducible, the following properties are equivalent.*

(i) W is finite.
(ii) The reflection representation $\rho : W \to \mathrm{GL}(V)$ is irreducible.
(iii) The quadratic form Q_M associated with M is positive definite.

Proof.

(i)⇒(ii). Since W is finite, S is finite and the vector space $V = \bigoplus_{s\in S} \mathbb{R}e_s$ is finite dimensional. By Lemma 5.1.2 there is a positive-definite bilinear form κ invariant under ρW. Suppose that E is a proper nontrivial invariant subspace of V. Then so is its perpendicular $D = \{x \in V \mid \kappa(x, E) = 0\}$ with respect to κ. By Proposition 2.3.7, both D and E are in the radical of B. As $V = D \oplus E$ (use that κ is positive definite), this leads to $B = 0$, a contradiction with $B(e_1, e_1) = 2$. We have shown that ρ is irreducible.

(ii) ⇒ (iii). In view of Lemma 5.1.2(ii), the symmetric bilinear form B is a nonzero scalar multiple of a positive-definite form. As $B(e_1, e_1) > 0$, this scalar must be positive, and so B is positive definite as well.

(iii) ⇒ (i). The linear map sending $y \in V$ to $Dy \in V^*$ defined by $(Dy)x = B(y, x)$ is an isomorphism of W-modules. For, it clearly is an isomorphism of vector spaces and $(D(wy))x = B(wy, x) = B(y, w^{-1}x) = (Dy)(w^{-1}x) = (w(Dy))x$ for all $x, y \in V$, so $Dw = wD$ for all $w \in W$. Recall from

Theorem 3.3.5(ii) that $A = \bigcap_{s\in S} A_s$, where $A_s = \{h \in V^* \mid h(e_s) \geq 0\}$, is a prefundamental domain for W in V^*. As D is an isomorphism of W-modules, $D^{-1}A$ is a prefundamental domain for W in V, so all wA, for $w \in W$, are distinct. Now $D^{-1}A$ is non-empty and coincides with the intersection of the half-spaces $\{x \in V \mid B(x, e_s) \geq 0\}$. In particular, its intersection with the unit ball $\{x \in V \mid Q_M(x) \leq 1\}$ has positive volume, say μ. Now $\bigcup_{w\in W} wD^{-1}A$ has volume $\mu|W|$ and lies in the unit ball, so $\mu|W|$ is bounded from above by the volume of the unit ball, which proves that $|W|$ is finite. □

Theorem 5.3.3 *An irreducible Coxeter group is finite if and only if its Coxeter diagram occurs in Table 5.1.*

Proof. We proceed in thirteen steps.

Step 1. *If M occurs in Table 5.1, then W is finite.* This can be derived directly from Proposition 5.3.2 by checking that B_M is positive definite.

From now on, let W be a finite irreducible Coxeter group of type M.

Step 2. *Any subdiagram of M is the Coxeter diagram of a finite Coxeter group.* This follows from Corollary 3.3.6.

Step 3. 5.4.10 for a proof. Here is another proof. Suppose (after suitably relabeling the indices) that M has a circuit on $[k]$. Then $e = \sum_{i=1}^{k} e_i$ satisfies $Q_M(e) = k - 2\sum_{i<j} \cos(\pi/m_{ij})$ and since there are k pairs $\{i, j\}$ with $\cos(\pi/m_{i,j}) \geq \frac{1}{2}$ while the other pairs provide a contribution greater than or equal to zero. So $Q_M(e) \leq 0$, a contradiction as Q_M is positive definite.

Step 4. *The diagram M cannot have a subdiagram of the form $\widetilde{\mathrm{A}}_1$, $\widetilde{\mathrm{B}}_n$ $(n \geq 2)$, $\widetilde{\mathrm{C}}_n$ $(n \geq 2)$, $\widetilde{\mathrm{F}}_4$, or $\widetilde{\mathrm{G}}_2$.* By Examples 3.2.6(iii), these diagrams have infinite groups.

Step 5. *For each $i \in [n]$, we have $\sum_{j\neq i} B(e_i, e_j)^2 < 4$.* Indeed, let J be the set of $j \in [n]$ such that $m_{ij} \geq 3$. By Step 3, $m_{j\,k} = 2$ for all $j, k \in J$, and so $\{e_j \mid j \in J\}$ is an orthogonal set. Now

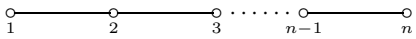
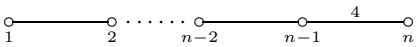
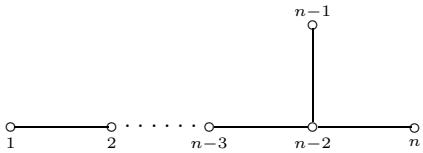
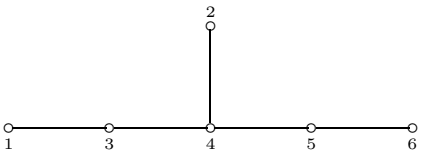
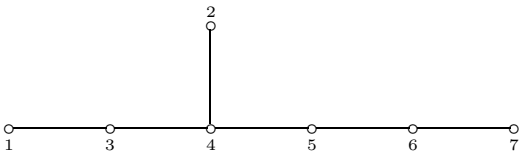
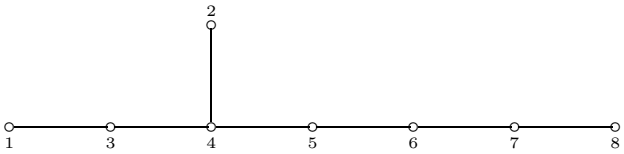
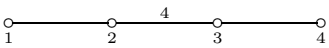
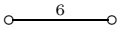
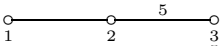
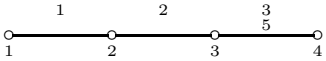
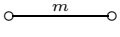
$$Q_M(e_i - \frac{1}{2}\sum_{k\in J} B(e_i, e_k)e_k) = 1 + \frac{1}{4}\sum_{k\in J} B(e_i, e_k)^2 - \frac{1}{2}B(e_i, e_k)^2$$
$$= 1 - \frac{1}{4}\sum_{k\neq i} B(e_i, e_k)^2,$$

so the statement states that this value must be positive.

Step 6. *An element $i \in [n]$ cannot be on more than three edges of M.* If $\{i, j\}$ is an edge of M, then $B(e_i, e_j)^2 = 4\cos^2(\pi/m_{ij}) \geq 1$ and so it suffices to apply Step 5.

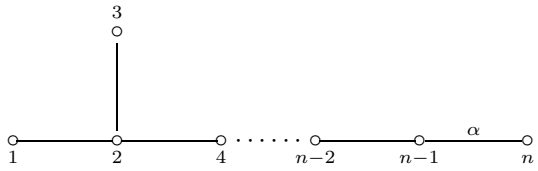
Step 7. *If an element $i \in [n]$ is on three edges of M then all these edges have label $m_{ij} = 3$.* Obvious by Step 5.

Table 5.1. Diagrams of irreducible finite Coxeter systems. The diagrams G_2 and $I_2^{(6)}$ are the same. The diagrams H_2 and B_2 might be defined as $I_2^{(5)}$ and $I_2^{(4)}$, respectively. The diagram A_2 coincides with $I_2^{(3)}$.

name	diagram
A_n $(n \geq 1)$	
$B_n = C_n$ $(n \geq 3)$	
D_n $(n \geq 4)$	
E_6	
E_7	
E_8	
F_4	
G_2	
H_3	
H_4	
$I_2^{(m)}$ $(m \geq 3)$	

STEP 8. *If $m_{ij} \geq 6$, then $n = 2$.* If $n \geq 3$, then, as M is connected, there is a node in $\{i, j\}$, say i, with another node, say k, adjacent to it. Now Step 5 gives $4 = 1 + 3 \leq B(e_i, e_k)^2 + B(e_i, e_j)^2 < 4$, a contradiction.

STEP 9. *If $i \in [n]$ is on three edges of M then all edges of M are of multiplicity $m_{ij} = 3$.* Otherwise, by Steps 8 and 7, there exists a subdiagram

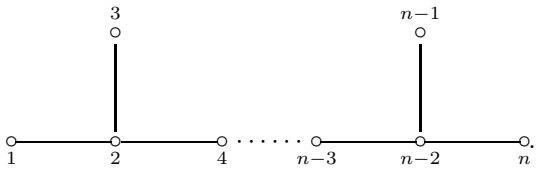


with $\alpha = 4$ or 5. Then

$$Q_M(e_1 + e_2 + 2(e_3 + e_4 + \cdots + e_{n-1}) + \sqrt{2}e_n) \leq 0.$$

STEP 10. *If $m_{ij} = 5$ then i is on at most one more edge and, if so, this edge, say $\{i, k\}$, has label $m_{ik} = 3$.* This is due to Step 5 as $\cos^2 \pi/5 = (6 + 2\sqrt{5})/16 \approx 0.65$.

STEP 11. *There is at most one $i \in [n]$ which is on three edges of M.* For otherwise, by Steps 6, 7, and 9, there is a subdiagram

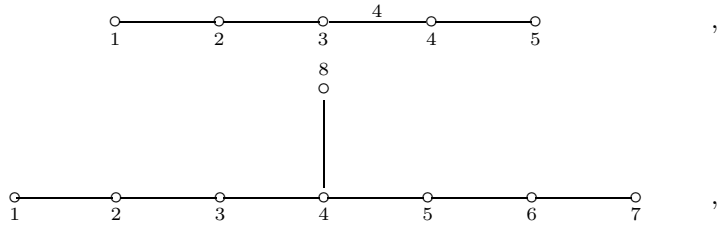


Now, the quadratic form Q_M vanishes on

$$e_1 + e_2 + 2(e_3 + e_4 + \cdots + e_{n-2}) + e_{n-1} + e_n,$$

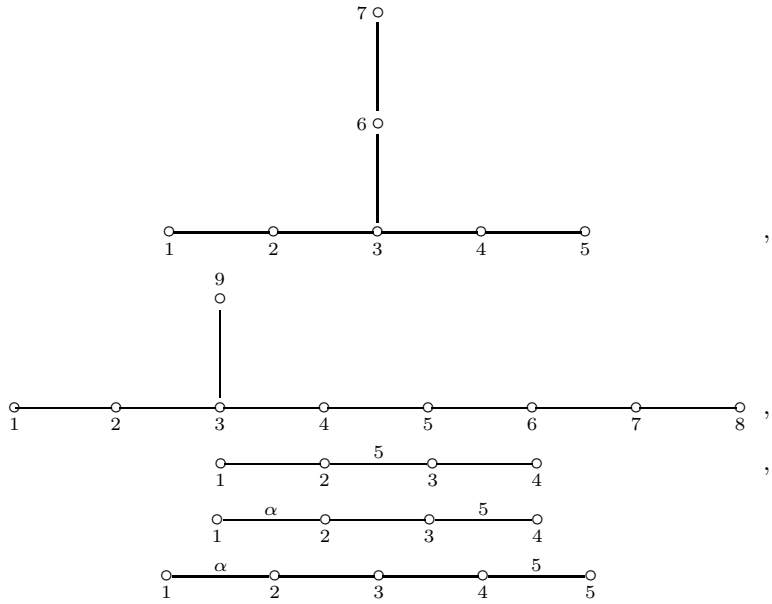
which contradicts that it be positive definite.

STEP 12. *M cannot have a subdiagram of the form*



,

,



,

,

,

$(\alpha \geq 4)$,

$(\alpha \geq 3)$.

Consider the vector x given by, in the respective cases,

$$x = e_1 + 2e_2 + 3e_3 + 2\sqrt{2}e_4 + \sqrt{2}e_5,$$
$$x = e_1 + 2e_2 + 3e_3 + 4e_4 + 3e_5 + 2e_6 + e_7 + 2e_8,$$
$$x = e_1 + 2e_2 + 3e_3 + 2e_4 + e_5 + 2e_6 + e_7,$$
$$x = 2e_1 + 4e_2 + 6e_3 + 5e_4 + 4e_5 + 3e_6 + 2e_7 + e_6 + 3e_9,$$
$$x = e_1 + 2e_2 + 2e_3 + e_4,$$
$$x = e_1 + 2e_2 + 2e_3 + e_4,$$
$$x = e_1 + 2e_2 + 3e_3 + 4e_4 + \frac{5}{2}(\sqrt{5} - 1)e_5.$$

A straightforward calculation gives that $Q_M(x) \leq 0$ in each of these cases.

STEP 13. *The only connected diagrams satisfying the conditions of Steps 3–12 are those in the list of the theorem.* This is easily verified. □

Remark 5.3.4 By analysis of the root system and the corresponding Coxeter group action it can be shown that the orders of the Coxeter groups of type E_n $(n = 6, 7, 8)$ and their root systems are
The corresponding numbers for D_n are in Exercise 5.4.2 and the orders for most other irreducible spherical types are in Table 3.1.

type	group order	root system size
E_6	51,840	72
E_7	2,903,040	126
E_8	696,729,600	240

5.4 Exercises

Section 5.1

Exercise 5.4.1 Prove that $O(n, \mathbb{R})$, the orthogonal group on $\mathbb{R}^n$ with respect to the standard inner product, is generated by reflections. Verify that, for $n > 1$, this group is not a Coxeter group.

Exercise 5.4.2 (Cited in Theorem 5.3.3) Let $n \geq 4$ and consider the following set of $2n(n-1)$ vectors in $\mathbb{R}^n$ with standard basis $\varepsilon_1, \ldots, \varepsilon_n$.

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

Here, the two $\pm$ signs stand for independent variations, so one expression indicates four distinct elements. Let $(\cdot, \cdot)$ be the standard inner product on $\mathbb{R}^n$.

(a) Prove that each orthogonal reflection r_α (cf. Exercise 3.4.5) with root $\alpha \in \Phi$ leaves Φ invariant. Denote by W the group generated by all r_α for $\alpha \in \Phi$.

(b) Prove that

$$\Delta = \{\varepsilon_1 - \varepsilon_2, \varepsilon_2 - \varepsilon_3, \ldots, \varepsilon_{n-1} - \varepsilon_n, \varepsilon_{n-1} + \varepsilon_n\}$$

is a subset of Φ with the property that each element of Φ is a linear combination of members of Δ all of whose nonzero coefficients have the same sign.

(c) Derive that W is a finite Coxeter group of type D_n (see Table 5.1 for the diagram).

(d) Prove that $|W| = 2^{n-1}n!$
(*Hint:* Interpreting the roots of Φ modulo 2, one obtains a surjective homomorphism $W \to W(A_{n-1})$; determine the order of the kernel and use the first isomorphism theorem.)

Section 5.2

Exercise 5.4.3 Which permutation in Sym_{n+1} corresponds to the longest element in $W(A_n)$ under the isomorphism between the two groups?

Exercise 5.4.4 Consider the real vector space $V = \mathbb{R}^8$, its standard basis $\varepsilon_1, \ldots, \varepsilon_8$, and the standard inner product $(\cdot, \cdot)$. Let Φ be the subset of V consisting of

- all $\pm\varepsilon_i \pm \varepsilon_j$, $i < j$ (with the same convention for the two $\pm$ signs as in Exercise 5.4.2), and
- all $\frac{1}{2}\sum_i (-1)^{k_i}\varepsilon_i$ with $\sum_i k_i$ even.

(a) Verify that $|\Phi| = 240$.
(b) Prove that Φ is invariant under each orthogonal reflection r_α with respect to $(\cdot,\cdot)$ having a root α in Φ; cf. Exercise 3.4.5.
(c) Consider the following elements of Φ.

$$\begin{aligned}
\alpha_1 &= \frac{1}{2}(\varepsilon_1 - \varepsilon_2 - \varepsilon_3 - \varepsilon_4 - \varepsilon_5 - \varepsilon_6 - \varepsilon_7 + \varepsilon_8),\\
\alpha_2 &= \varepsilon_1 + \varepsilon_2, \quad \alpha_3 = \varepsilon_2 - \varepsilon_1, \quad \alpha_4 = \varepsilon_3 - \varepsilon_2\\
\alpha_5 &= \varepsilon_4 - \varepsilon_3, \quad \alpha_6 = \varepsilon_5 - \varepsilon_4, \quad \alpha_7 = \varepsilon_6 - \varepsilon_5,\\
\alpha_8 &= \varepsilon_7 - \varepsilon_6.
\end{aligned}$$

Verify that the *Gram matrix* of $\alpha_1, \ldots, \alpha_8$, that is, the matrix of inner products (α_i, α_j) for $i, j \in [8]$, is equal to the Gram matrix of the basis $e_1, \ldots, e_8$ of the reflection representation of the Coxeter group of type E_8 with respect to the symmetric bilinear form B_{E_8} (see Table 5.1 for the diagram). Conclude that $(\langle S\rangle, S)$, where $S = \{r_{\alpha_i} \mid i \in [8]\}$, is a Coxeter system of type E_8.
(d) Prove that the subgroup $\langle S\rangle$ of (c) coincides with $\langle r_\alpha \mid \alpha \in \Phi\rangle$ and that $W(\mathrm{E}_8)$ is finite.

Exercise 5.4.5 Let Ψ be the set of roots from Φ of Exercise 5.4.4 inside the linear span of $\alpha_1, \ldots, \alpha_6$.

(a) Prove that Ψ has size 72 and that Ψ is invariant under $s_i = r_{\alpha_i}$ for each $i \in [6]$.
(b) Set $S = \{s_1, \ldots, s_6\}$ and $W = \langle S\rangle$. Show that (W, S) is a Coxeter system of type E_6 (see Table 5.1 for the diagram).
(c) Show that $(s_1 s_2 \cdots s_6)^6 (s_1 s_3 s_1 s_5 s_6 s_5)$ is the longest element w_0 of W.
(d) What is the action of w_0 on the Coxeter diagram E_6?
(e) Prove that each element of the subgroup $F = \langle s_1 s_6, s_3 s_5, s_4, s_2\rangle$ is fixed under conjugation by w_0.
(f) Show that F is a homomorphic image of the Coxeter group of type F_4. (Later, we will prove that this homomorphism is in fact an isomorphism.)

Exercise 5.4.6 Consider $w_0 = (s_1 s_2 s_3 s_4)^{15}$ in $W(\mathrm{H}_4)$ (see Table 5.1 for the diagram).

(a) Show that the image $\rho(w_0)$ of w_0 in the reflection representation ρ of $W(\mathrm{H}_4)$ is equal to scalar multiplication by -1.
(b) Determine the root system of H_4 and show that it has size 120.
(c) Show that w_0 is the longest element of $W(\mathrm{H}_4)$.

Exercise 5.4.7 Let $n \in \mathbb{N}$, $n \geq 3$, and consider the Coxeter system (W, S) of type B_n with $S = \{s_1, \ldots, s_n\}$.

(a) Take $\varepsilon_1, \ldots, \varepsilon_n$ to be the standard orthonormal basis of $\mathbb{R}^n$ with respect to the standard inner product $(\cdot, \cdot)$. Prove that, up to a coordinate transformation,
$$\{\varepsilon_i \pm \varepsilon_j, \sqrt{2}\varepsilon_k \mid i, j, k \in [n], i < j\}$$
is the set of positive roots of the root system for W in its reflection representation.
(b) Show that the subgroup D of W generated by $s_1, \ldots, s_{n-1}, s_n s_{n-1} s_n$ is a homomorphic image of the Coxeter group of type D_n.
(c) Derive from the results of Exercise 5.4.2 that D is isomorphic to $W(\mathrm{D}_n)$.
(d) Prove that D has index 2 in W and conclude that $|W| = 2^n n!$

Exercise 5.4.8 Let (W, S) be a finite irreducible Coxeter system of type M. Prove that the following statements are equivalent.

(a) The action of the opposition on S is trivial.
(b) There is an element in W that maps to scalar multiplication by -1 under the reflection representation.
(c) The longest element of W maps to scalar multiplication by -1 under the reflection representation.

Exercise 5.4.9 Let (W, S) be a finite irreducible Coxeter system of type M. Prove that the opposition on M is trivial if and only if M is one of A_1, B_n $(n \geq 3)$, D_n (n even), E_7, E_8, F_4, $\mathrm{I}_2^{(m)}$ (m even), H_n $(n \in \{3, 4\})$.

Section 5.3

Exercise 5.4.10 (Cited in Theorem 5.3.3) Let (W, S) be a Coxeter system of type M and let $k \geq 3$. Suppose that $1, 2, \ldots, k$ is a circuit in M (so $m_{1,k} \geq 3$ and $m_{i,i+1} \geq 3$ for $i \in [k-1]$). Show that the word $(12 \cdots k)^i$ is a minimal expression in $\mathrm{M}(S)$ for each $i \in \mathbb{N}$. Conclude that W is an infinite group. (*Hint:* Use Theorem 4.3.1.)

Exercise 5.4.11 By means of an example it will become clear in this exercise that finite complex linear groups generated by reflections need not be Coxeter groups. Put $\sigma = (1 + \sqrt{-7})/2$ and consider the following set of vectors in $\mathbb{C}^3$ with standard basis ε_1, ε_2, ε_3.
$$\Phi = \pm \left\{ \varepsilon_i, \frac{\overline{\sigma}}{2}(\varepsilon_i \pm \varepsilon_j), \frac{1}{2}(\varepsilon_i \pm \varepsilon_j \pm \sigma\varepsilon_k) \,\middle|\, \{i, j, k\} = [3] \right\}$$
Supply $\mathbb{C}^3$ with the standard hermitian inner product $(x, y) = \sum_i x_i \overline{y_i}$. For $\alpha \in \Phi$, let r_α be the *unitary reflection* with respect to $(\cdot, \cdot)$ having root α, that is,
$$r_\alpha x = x - 2(x, \alpha)(\alpha, \alpha)^{-1}\alpha \qquad (x \in \mathbb{C}^3).$$

(a) The size of Φ is equal to 42.
(b) For each $\alpha \in \Phi$, the reflection r_α leaves Φ invariant.
(c) The group $W = \langle r_\alpha \mid \alpha \in \Phi \rangle$ is generated by $S := \{r_{\alpha_1}, r_{\alpha_2}, r_{\alpha_3}\}$, where

$$\alpha_1 = \varepsilon_2, \qquad \alpha_2 = \frac{\overline{\sigma}}{2}(\varepsilon_2 + \varepsilon_3), \qquad \alpha_3 = \frac{1}{2}(\varepsilon_1 + \varepsilon_2 - \sigma\varepsilon_3).$$

(d) W is a homomorphic image of the Coxeter group with Coxeter matrix

$$\begin{pmatrix} 1 & 3 & 3 \\ 3 & 1 & 4 \\ 3 & 4 & 1 \end{pmatrix}.$$

(e) The order of W is equal to 336.
(f) The pair (W, S) is not a Coxeter system.
(g) The center of W has order 2.
(h) The group W is not isomorphic to any finite Coxeter group.

5.5 Notes

Sections 5.1 and 5.2. Most finiteness characterizations are in [2]. There are interesting combinatorial properties of Φ that we will not go into in this course. For instance, for each finite Coxeter group of rank n, there exist positive integers $d_1, \ldots, d_n$ with $d_1 \leq d_2 \leq \cdots \leq d_n$ such that Φ has precisely $d_1 + \cdots + d_n - n$ elements, $d_1 d_2 \cdots d_n = |W|$, and the sum $d_i + d_{n+1-i}$ is constant for $i \leq \lfloor n/2 \rfloor$. If $M = \mathrm{A}_n$, then these integers are $2, 3, \ldots, n+1$.

Lemma 5.1.6 is taken from [3], where it is credited to Dyer.

Section 5.3. Most of this material is dealt with in [2]. There, and in [20], you can also find classifications of Coxeter diagrams M for which Q_M is hyperbolic.

The proof of Proposition 5.3.2 did not need the precise value of the volume of the n-dimensional unit ball, which is well known to be $\pi^{\frac{n}{2}} \Gamma(\frac{n}{2} + 1)$.

6. Weyl groups and parabolic subgroups of Coxeter groups

In this chapter we will determine the finite Coxeter groups leaving invariant a lattice in the reflection representation. Such groups are called Weyl groups. They play a major role in the classification of finite-dimensional simple complex Lie algebras and in Chevalley groups, the finite samples of which are prominent in the classification of finite simple groups; see Theorem 1.7.1.

Our first goal is to introduce the bare essentials on lattices; this takes place in Section 6.1. In the next section, we classify Weyl groups. The last section is devoted to finite subgroups of Coxeter groups; these turn out to be contained in parabolic subgroups, that is, conjugates of finite subgroups generated by a subset of the standard generating set.

6.1 Lattices

Consider the n-dimensional vector space $\mathbb{R}^n$ with the standard inner product, which we denote by $(\cdot, \cdot)$. The Euclidean length of norm of a vector $v \in \mathbb{R}^n$ is equal to $\sqrt{(v,v)}$. By the square norm of a vector v we mean (v,v). For $i \in [n]$, we usually denote by ε_i the i-th standard basis vector.

A lattice can be defined as a discrete additive subgroup of $\mathbb{R}^n$, but Definition 6.1.1 below is another approach. According to Lemma 6.1.2 the two definitions are equivalent. Given any two lattices L and L' in $\mathbb{R}^n$, it is easy to find a linear transformation mapping L onto L'. But this transformation need not respect the structure of $\mathbb{R}^n$ as a Euclidean space. The orthogonal group

$$\mathrm{O}(n,\mathbb{R}) = \{g \in \mathrm{GL}(n,\mathbb{R}) \mid (gx, gy) = (x,y) \text{ for all } x, y \in \mathbb{R}^n\} \qquad (6.1)$$

does. Elements of this group are called *orthogonal transformations*.

Definition 6.1.1 A *lattice* in $\mathbb{R}^n$ is an additive subgroup of $\mathbb{R}^n$ generated by a basis of $\mathbb{R}^n$. Such a basis will also be called a *basis* of L. We call two lattices *similar* whenever one can be transformed into the other by means of an orthogonal transformation.

An orthogonal transformation preserving L is called an *automorphism* of L. The set of all automorphisms of L, denoted $\mathrm{Aut}(L)$, is a group, called the *automorphism group* of L.

Being similar, also referred to as *similarity*, is an equivalence relation. We cannot find an orthogonal linear transformation (a member of $\mathrm{O}(n,\mathbb{R})$) mapping the lattice $\mathbb{Z}^n$ to $2\mathbb{Z}^n$ (see Remark 6.1.7 below). In other words, there is more than one similarity class of lattices in $\mathbb{R}^n$.

Lemma 6.1.2 *Let L be an additive subgroup of $\mathbb{R}^n$. Then L is discrete in $\mathbb{R}^n$ if and only if L contains linearly independent vectors $v_1,\dots,v_r$ such that $L=\mathbb{Z}v_1+\cdots+\mathbb{Z}v_r$.*

Proof. Suppose $L=\mathbb{Z}v_1+\cdots+\mathbb{Z}v_r$ with $v_1,\dots,v_r$ linearly independent over $\mathbb{R}$. Let μ be the minimum of $(\lambda_1v_1+\cdots+\lambda_rv_r,\lambda_1v_1+\cdots+\lambda_rv_r)$ as $\lambda_1,\dots,\lambda_r$ run over all real numbers such that $\lambda_1^2+\cdots+\lambda_r^2=1$. Since the v_i are independent, this minimum is nonzero. Moreover, for any $\lambda_1,\dots,\lambda_r\in\mathbb{R}$,

$$(\lambda_1v_1+\cdots+\lambda_rv_r,\lambda_1v_1+\cdots+\lambda_rv_r)\geq\mu(\lambda_1^2+\cdots+\lambda_r^2).$$

Hence, for any nonzero $v\in L$, we obtain $(v,v)\geq\mu$. Consequently, L is discrete.

Suppose, conversely, that L is discrete. Let r be the dimension of the $\mathbb{R}$-linear span of L and choose r linearly independent elements $w_1,\dots,w_r$ of L. Consider the set

$$F=\{x\in L\mid x=\mu_1w_1+\cdots+\mu_rw_r,\ \forall i:0\leq\mu_i\leq 1\}.$$

Since L is discrete, the set F is finite. For $i=1,\dots,r$ we choose $v_i\in F$ such that $v_i\in\mu_iw_i+\mathbb{R}w_{i+1}+\cdots+\mathbb{R}w_r$ with $\mu_i>0$ and minimal. Since $w_i\in F$, such an element always exists. Clearly the v_i are also linearly independent. Let $v\in L$ and write $v=\sum_{i=1}^r\lambda_iv_i$. For each i, let ν_i be equal to λ_i minus its largest integral part. Then $v':=\sum_{i=1}^r\nu_iv_i$ is also an element of L. We assert that $\nu_i=0$ for all i. Suppose not, then choose $j\in[r]$ minimal such that $\nu_j>0$. Then $v'\in\nu_j\mu_jw_j+\mathbb{R}w_{j+1}+\cdots+\mathbb{R}w_r$, contradicting the minimality of μ_j in our choice of v_j. □

Corollary 6.1.3 *The automorphism group of each lattice of $\mathbb{R}^n$ is finite.*

Proof. The argument is similar to the one for Proposition 5.3.2: Let $b_1,\dots,b_n$ be a basis of a lattice L of $\mathbb{R}^n$. As L is a discrete subset of $\mathbb{R}^n$, the set N of all vectors in L whose square norm is equal to (b_i,b_i) for some $i\in[n]$ is finite and invariant under $\mathrm{Aut}(L)$. But N contains the basis b_i ($i\in[n]$) of $\mathbb{R}^n$, so the restriction of $\mathrm{Aut}(L)$ to N is faithful (cf. the proof of Proposition 1.5.3). Consequently, $\mathrm{Aut}(L)$ embeds in the finite group $\mathrm{Sym}(N)$, and so is finite. □

Notation 6.1.4 A basis $b_1,\dots,b_n$ of $\mathbb{R}^n$ determines the lattice

$$L=\mathbb{Z}b_1\oplus\mathbb{Z}b_2\oplus\cdots\oplus\mathbb{Z}b_n.$$

We collect the vectors b_i as columns in a matrix B and write $L(B)$ for L.

The matrix B can also be used to describe L as the image of the map

$$\mathbb{Z}^n \to \mathbb{R}^n, \quad x \mapsto Bx.$$

In general, a lattice can be given by many different bases.

Lemma 6.1.5 *If B is a matrix whose columns are a basis for the lattice L in $\mathbb{R}^n$, then*

$$d(L) := |\det(B)|$$

does not depend on the chosen basis.

Proof. If $b'_1, \ldots, b'_n$ is a second basis of L, with corresponding matrix B', then there are integers x_{ij} and y_{ij} $(1 \leq i, j \leq n)$ such that $b'_i = \sum_{j=1}^n x_{ij} b_j$ and $b_i = \sum_{j=1}^n y_{ij} b'_j$. In terms of matrices: $B' = BX$ and $B = B'Y$. Now $\det(B) = \det(B')\det(Y) = \det(B)\det(X)\det(Y)$, so $\det(X)\det(Y) = 1$. As both factors are integers, it follows that $\det(X) = \det(Y) = \pm 1$ and so $|\det(B)| = |\det(B')|$. □

Definition 6.1.6 We call a property of L an *invariant* when it holds for all lattices in the similarity class of L.

Remark 6.1.7 The number $d(L)$ is an invariant because, for $g \in \mathrm{O}(n, \mathbb{R})$, we have $\det(g) = \pm 1$, so $d(gL) = |\det(gB)| = |\pm \det(B)| = d(L)$. The number $d(L)$ is often called the *determinant* of L. The *discriminant* of L is the square of $d(L)$. The determinant of L measures the n-dimensional volume of $\{\lambda_1 b_1 + \cdots + \lambda_n b_n \mid 0 \leq \lambda_1, \ldots, \lambda_n \leq 1\}$ in the Euclidean space on $\mathbb{R}^n$. Clearly, $d(\mathbb{Z}^n) = 1$ and $d(2\mathbb{Z}^n) = 2^n$, so the lattices $\mathbb{Z}^n$ and $2\mathbb{Z}^n$ are not similar.

The isomorphism type of $\mathrm{Aut}(L)$ is another example of an invariant of L.

Example 6.1.8 The lattice

$$L = \{(x_1, \ldots, x_n) \in \mathbb{Z}^n \mid x_1 + x_2 + \cdots + x_n \text{ is even}\}$$

of $\mathbb{R}^n$ has $d(L) = 2$. This follows directly from the choice of basis $\varepsilon_1 - \varepsilon_2, \ldots, \varepsilon_{n-1} - \varepsilon_n, 2\varepsilon_n$ for L: the matrix whose columns are these basis elements has determinant 2. This lattice is usually denoted $L(\mathrm{D}_n)$ (for $n \geq 3$). Later, in Example 6.2.4, we will see why. The automorphism group of L has order $2^n n!$ and is in fact isomorphic to $W(\mathrm{B}_n)$; cf. Exercise 6.4.9.

In practice, we often work with a slight extension of the definition of a lattice: we take the additive subgroup L of $\mathbb{R}^n$ generated by a linearly independent set of vectors in $\mathbb{R}^n$. The result L need not be a lattice of $\mathbb{R}^n$ but can be seen as a lattice of a subspace of $\mathbb{R}^n$. If the subspace has dimension

m (that is, the size of an independent set of generating vectors of L is equal to m), then we say that L has *rank* m.

Computing the discriminant of a lattice in $\mathbb{R}^n$ of rank m can be done without a change of basis: put the vectors $b_1, \ldots, b_m$ generating a lattice L inside $\mathbb{R}^n$ again into a matrix B. Now $d(L)$, for L viewed as a lattice of $\mathbb{R}^m$, is the number

$$d(L) = \sqrt{|\det((b_i, b_j))_{1 \le i,j \le m}|} = \sqrt{|\det(B^\top B)|}.$$

It measures the m-dimensional volume of the subset $[0,1]b_1 + \cdots + [0,1]b_m$. To make this plausible we add basis vectors $a_1, \ldots, a_{n-m}$ from $\{b_1, \ldots, b_m\}^\perp$ of length 1 and mutually orthogonal. Then compute $B'^\top B'$ for the matrix B' containing the b's and the a's. Then $|\det(B')| = |\det(B)|$.

Example 6.1.9 Let $\varepsilon_1, \ldots, \varepsilon_{n+1}$ be the standard basis of $\mathbb{R}^{n+1}$. Consider

$$\begin{aligned} L &= \mathbb{Z}(\varepsilon_1 - \varepsilon_2) + \cdots + \mathbb{Z}(\varepsilon_n - \varepsilon_{n+1}) \\ &= \{(x_1, \ldots, x_{n+1}) \in \mathbb{Z}^{n+1} \mid x_1 + \cdots + x_{n+1} = 0\}. \end{aligned}$$

These are the vectors in $\mathbb{Z}^{n+1}$ that are perpendicular to the all-one-vector. This lattice is usually denoted by $L(\mathrm{A}_n)$. It is of rank n. The set $\{\varepsilon_1 - \varepsilon_2, \ldots, \varepsilon_n - \varepsilon_{n+1}\}$ is a basis of this lattice and, if B is the matrix whose columns are these factors, then $\det(B^\top B) = n+1$, so $d(L(\mathrm{A}_n)) = \sqrt{n+1}$.

The linear transformation interchanging the i and the $(i+1)$-st coordinate is an automorphism of L. Exercise 6.4.2 shows that, together with scalar multiplication by -1, these automorphisms generate all of $\mathrm{Aut}(L)$, which is a group isomorphic to $\mathrm{Sym}_{n+1} \times \mathbb{Z}/2\mathbb{Z}$.

Definition 6.1.10 Let L be a lattice on which $(\cdot,\cdot)$ takes integer values only. Then L is called *even* if (x,x) is even for all x; otherwise it is called *odd*. L is called *unimodular* if $d(L) = 1$.

It is easy to see that evenness need only be checked on a set of basis vectors. Examples of even lattices of rank n are $L(\mathrm{D}_n)$ and $L(\mathrm{A}_n)$ of Examples 6.1.8 and 6.1.9, respectively.

The lattice $\mathbb{Z}^n$ is unimodular, but the lattices $L(\mathrm{A}_n)$ of Example 6.1.9 and $L(\mathrm{D}_n)$ of Example 6.1.8 are not.

Proposition 6.1.11 *Let L and M be lattices of $\mathbb{R}^n$ with $L \subseteq M$. Then the index $[M : L]$ of L in M is equal to $|d(L)/d(M)|$.*

Proof. If X is an invertible linear transformation of $\mathbb{R}^n$ then $d(XL)/d(XM) = d(L)/d(M)$ and $[XM : XL] = [M : L]$, so it suffices to prove the proposition for the case where $M = \mathbb{Z}^n$. Now $L = L(B)$ for an $n \times n$ matrix B with integer

entries. It is well known (and easy to prove by means of elementary matrices and permutations matrices) that there are X, $Y \in \mathrm{SL}(n,\mathbb{Z})$ such that XBY has diagonal form. Now $L(XBY) = XL$ and $L(XY) = X\mathbb{Z}^n = \mathbb{Z}^n$, so we may assume that B has diagonal form. But then $|d(B)|$ is the number of vectors of the form $(v_1, \ldots, v_n)$ with $v_i \in \mathbb{Z}$ and $0 \le v_i < |B_{ii}|$, which is equal to $[\mathbb{Z}^n : L(B)]$. This establishes the proposition.

Here is another proof, which uses the classification of finite abelian groups. The quotient group L/M is a finite abelian group and is therefore isomorphic to some $\mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_n}$. So there is a matrix B whose columns $b_1, \ldots, b_n$ are a basis of L such that $d_1 b_1, \ldots, d_n b_n$ is a basis of M. As $[L : M] = |L/M| = d_1 \cdots d_n$, it follows that $d(M) = d_1 \cdots d_n \det(B) = [L : M]\, d(L)$. □

Example 6.1.12 We present four construction methods for lattices.

(i). **Direct sum.** An obvious way to construct lattices out of two given ones is to take the direct sum: $L \oplus M$ inside $\mathbb{R}^n \oplus \mathbb{R}^m = \mathbb{R}^{n+m}$ whenever L is a lattice of $\mathbb{R}^n$ and M a lattice of $\mathbb{R}^m$. Then $d(L \oplus M) = d(L)\, d(M)$.

(ii). **Construction using linear binary codes.** Let $\mu\colon \mathbb{Z}^n \to \mathbb{F}_2^n$ be coordinatewise reduction mod 2 and let $C \subset \mathbb{F}_2^n$ be a linear binary $[n,k,d]$-code. This means that C is a linear subspace of $\mathbb{F}_2^n$ of dimension k such that each vector in C has at least d nonzero entries. The number of nonzero entries of a vector is called its *weight*. Then μ is a surjective homomorphism of additive groups. By the First Isomorphism Theorem for groups, $\mu^{-1}(0)$ is a subgroup of $\mathbb{Z}^n$ of index $|\mathbb{F}_2^n| = 2^n$, and so $\mu^{-1}(C)$ is a subgroup of $\mathbb{Z}^n$ of index $2^n/|C| = 2^{n-k}$. Therefore, $\mu^{-1}(C)$ is a Euclidean lattice of $\mathbb{R}^n$, with index 2^{n-k} in $\mathbb{Z}^n$. We normalize the lattice by dividing by $\sqrt{2}$:

$$L(C) = \frac{1}{\sqrt{2}}\mu^{-1}(C).$$

This lattice takes integer values if and only if $C \subseteq C^\perp$, where $\perp$ is taken with respect to the standard inner product on $\mathbb{F}_2^n$. It is even if, in addition, all the weights are divisible by 4. Finally, $d(L(C)) = 2^{\frac{n}{2}-k}$, so $L(C)$ is unimodular if and only if $C = C^\perp$. This property of C is referred to as self-duality in Coding Theory.

(iii). **A variation on this theme.** Consider

$$g\colon \mathbb{Z}^n \to \mathbb{F}_2, \quad g(x) = \sum_i x_i \pmod 2.$$

Then $g^{-1}(0) \subset \mathbb{Z}^n$ is the lattice $L(\mathrm{D}_n)$ we constructed earlier. For n divisible by 4 add vectors: $L(\mathrm{D}_n) + \frac{1}{2}\mathbb{Z}e$, with e the all-one vector. For n divisible by 8 this is an even unimodular lattice. For $n = 8$ it is called $L(\mathrm{E}_8)$. See Exercise 6.4.10.

(iv). **Sublattices**. Any subgroup of a lattice is again a lattice, possibly of lower rank. For example, intersect the lattice with the space perpendicular to some vectors. This is how we obtained $L(\mathrm{A}_n)$ from the lattice $\mathbb{Z}^{n+1}$ of $\mathbb{R}^n$.

For $L(\mathrm{E}_8)$, defined in (iii), take $\alpha^\perp$ for some $\alpha \in L(\mathrm{E}_8)$ satisfying $(\alpha,\alpha) = 2$. It does not matter which one as $\mathrm{Aut}(L)$ is transitive on the set of vectors of L with square norm 2 (see Exercise 6.4.10) and so the resulting lattice is determined up to similarity. This lattice is called $L(\mathrm{E}_7)$.

Take the space $\{\alpha,\beta\}^\perp$ in $L(\mathrm{E}_8)$, where $(\alpha,\alpha) = (\beta,\beta) = 2$, $(\alpha,\beta) = 1$. Such pairs α,β exist and the choice is again irrelevant; see Exercise 6.4.10. The resulting lattice is called $L(\mathrm{E}_6)$.

Definition 6.1.13 If L is a lattice of $\mathbb{R}^n$, then its *dual lattice* is the lattice

$$L^\circ := \{z \in \mathbb{R}^n \mid \forall_{v\in L}\ (v,z) \in \mathbb{Z}\}.$$

The dual L° is also a lattice of $\mathbb{R}^n$, but the standard inner product may assume non-integral values as will be clear from the example $L = 2\mathbb{Z}$ in $\mathbb{R}^1$.

Proposition 6.1.14 *Let L be a lattice in $\mathbb{R}^n$.*

(i) $d(L^\circ) = 1/d(L)$.
(ii) *L is integer-valued if and only if $L \subset L^\circ$.*
(iii) *If L is integer-valued, then $L = L^\circ$ if and only if L is unimodular.*

Proof. Let B be a matrix whose columns are a basis of L, so $L = L(B)$. Let B° be the matrix whose columns form the dual basis of B. Then $B^\top B^\circ = I$ and $L^\circ = L(B^\circ)$.

(i). Now $d(L^\circ) = |\det(B^\circ)| = |\det(B^\top)|^{-1} = 1/d(L)$.

(ii). The 'only if' part follows directly from the definition of L°.

If $L \subseteq L^\circ$, then there is an $n \times n$-matrix Y with integer entries such that $B = B^\circ Y$. It follows that $B^\top B = Y$, so L is integer-valued. This proves the 'if' part of (ii).

(iii). Suppose that L is integer-valued. Then $L \subseteq L^\circ$ by (ii) and $d(L) = d(L^\circ)\,[L^\circ : L]$ by Proposition 6.1.11, so, by (i), $d(L) = \sqrt{[L^\circ : L]}$. In particular, L is unimodular if and only if $[L^\circ : L] = 1$, which is equivalent to $L^\circ = L$. □

6.2 Weyl groups

Suppose that L is a lattice in $\mathbb{R}^n$, supplied with the standard inner product $(\cdot,\cdot)$. By Exercise 6.4.1, for nonzero $v \in L$, the orthogonal reflection r_v with respect to $(\cdot,\cdot)$ on $\mathbb{R}^n$ (defined in Exercise 3.4.5) belongs to $\mathrm{Aut}(L)$ if $(v,v) \in \{1,2\}$. More generally, if $2(w,v)/(v,v) \in \mathbb{Z}$ for all $w \in L$, then $r_v(z)$ is an integral linear combination of elements of L for each $z \in L$, so r_v preserves the lattice L and $r_v \in \mathrm{Aut}(L)$. Since the automorphism group of a lattice of

$\mathbb{R}^n$ is finite (cf. Corollary 6.1.3), such r_v generate a finite reflection group. The set of all roots $v \in L$ such that $2(w,v)/(v,v) \in \mathbb{Z}$ for all $w \in L$, comes close to satisfying the following properties.

Definition 6.2.1 Let V be a real vector space of finite dimension, supplied with a positive-definite symmetric bilinear form $(\cdot,\cdot)$. An *integral root system* in V is a finite spanning subset Φ of V with $\alpha \neq 0$ for each $\alpha \in \Phi$ such that the following two conditions hold.

(i) For each $\alpha \in \Phi$, the orthogonal reflection r_α preserves Φ.
(ii) For all $\alpha, \beta \in \Phi$, the number $2(\beta,\alpha)/(\alpha,\alpha)$ is an integer.

If in addition, for all $\lambda \in \mathbb{R}$ and $\alpha \in \Phi$,

$$\lambda\alpha \in \Phi \text{ if and only if } \lambda = \pm 1,$$

then Φ is called *restricted*. The lattice $\mathbb{Z}\Phi$ spanned by Φ is called the *root lattice* of Φ. The group generated by all reflections of the form r_α for $\alpha \in \Phi$ is called the *reflection group* of Φ and denoted by $W(\Phi)$. The *rank* of the integral root system is the rank of $\mathbb{Z}\Phi$.

By Theorem 5.1.4, $W(\Phi)$ is a Coxeter group. Its Coxeter type is called the *type* of Φ.

Two integral root systems Φ and Φ' in V, respectively V', are *isomorphic* if there is an invertible linear transformation $g : V \to V'$ respecting inner products such that $g\Phi = \Phi'$.

Comparing the above with Definition 4.1.1 of a root system, we see that scaling the roots occurring in an integral root system Φ so as to make the square norm of each root equal to 2 gives a root system. However, in a root system, Condition (ii) of an integral root system need not be satisfied. Indeed, a root system need not be an integral root system. If it is, then the integral root system is even a restricted integral root system.

Remark 6.2.2 Suppose that Φ is an integral root sytem. If $\lambda \in \mathbb{R}$ and $\alpha \in \Phi$ satisfy $\lambda\alpha \in \Phi$, then $2/\lambda = 2(\alpha,\lambda\alpha))/(\lambda\alpha,\lambda\alpha)$ is an integer, so $\lambda = \pm 1, \pm 2$. Therefore, the only positive scalars that may lead to roots in Φ after multiplication with a root already in Φ are $\frac{1}{2}$, 1, and 2.

Figure 6.1 depicts an integral root system of rank 2 that is not restricted; its type is known as BC_2. Its reflection group is the Coxeter group of type B_2. This is typical of the general picture in that no new Coxeter groups arise when non-restricted integral root systems are taken into account.

As $W(\Phi)$, for Φ an integral root system, is a finite group generated by reflections, it is a Coxeter group by Theorem 5.1.4. We investigate which Coxeter systems give rise to integral root systems. First we deal with *simply*

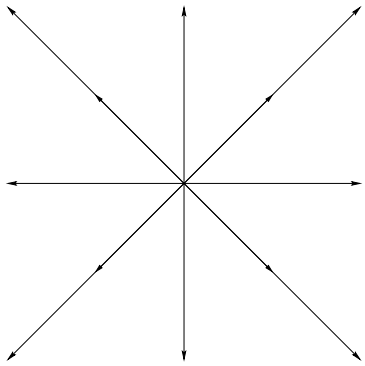


Fig. 6.1. The integral root system of type BC_2.

laced types, that is, Coxeter diagrams in which each edge $\{i, j\}$ has label $m_{ij} = 3$.

Recall that, if W is finite of rank n, Proposition 5.3.2 gives that the image of W under the reflection representation $\rho : W \to \mathrm{GL}(\mathbb{R}^n)$ leaves invariant the positive-definite symmetric bilinear form B on $\mathbb{R}^n$. Therefore, in this case, after a suitable coordinate transformation, we can view ρ as a map $W \to \mathrm{O}(n, \mathbb{R})$. Recall the definition of root system in Definition 4.1.1; it made use of the reflection representation ρ.

Lemma 6.2.3 *Let (W, S) be a finite Coxeter system of simply laced type M. Let $\rho : W \to \mathrm{O}(n, \mathbb{R})$ be its reflection representation. Then the root system Φ in $\mathbb{R}^n$ corresponding to ρ is a restricted integral root system in V, and so $\mathbb{Z}\Phi$ is a W-invariant lattice of $\mathbb{R}^n$.*

Proof. Each root e_i for $i \in [n]$ belongs to Φ and, by construction, Φ is a W-invariant set of roots in $\mathbb{R}^n$. Clearly, $B(\alpha, \alpha) = 2$ for each $\alpha \in \Phi$ and Φ spans V.

We verify the conditions (i) and (ii) of Definition 6.2.1. Condition (i) is obvious from the construction of Φ. As an arbitrary root in Φ can be mapped by an element of W to a root e_i for some $i \in [n]$, for the proof of Condition (ii), it suffices to verify that $B(we_i, e_j) \in \mathbb{Z}$ for all $i, j \in [n]$ and $w \in W$. We prove this by induction on $l(w)$. For $l(w) = 0$, we have $w = 1$ and $B(e_i, e_j) = -2\cos(\pi/m_{ij}) \in \{0, -1, 2\}$ as $m_{ij} \in \{1, 2, 3\}$.

Assume therefore $l(w) > 1$ and write $w = su$ with $s \in S$ and $l(w) = 1 + l(u)$. Then, by the induction hypothesis, $B(ue_i, e_p) \in \mathbb{Z}$ for each $p \in [n]$ and so $B(sue_i, e_j) = B(ue_i, se_j) = B(ue_i, e_j) - B(ue_i, e_s)B(e_s, e_j) \in \mathbb{Z}$, proving (ii). The conclusion is that Φ is indeed an integral root system.

It remains to show that Φ is restricted. By restriction to components of M, cf. Proposition 2.2.5, it suffices to show this in the case where M is irreducible. Then $\Phi = We_1$ as $e_j = s_i s_j e_i$ if $\{i, j\}$ is an edge of M. Suppose that, for some $\lambda \in \mathbb{R}$ and $\alpha \in \Phi$, we have $\lambda\alpha \in \Phi$. Then there are $w_1, w_2 \in W$

such that $\alpha = w_1 e_1$, and $\lambda\alpha = w_2 e_1$, so $w = w_2 w_1^{-1}$ satisfies $w\alpha = \lambda\alpha$, whence

$$2\lambda^2 = B(\lambda\alpha, \lambda\alpha) = B(w\alpha, w\alpha) = B(\alpha, \alpha) = 2,$$

proving $\lambda = \pm 1$. Hence Φ is restricted. □

Example 6.2.4 We discuss the three series of simply laced diagrams of finite Coxeter groups; (cf. Theorem 5.3.3).

D_n (for $n \geq 4$). After a suitable change of basis, which transforms B to the standard inner product, the integral root system of the Coxeter group of type D_n in $\mathbb{R}^n$ becomes

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

Clearly, $(x, x) = 2$ for all $x \in \Phi$, so Φ is a restricted integral root system indeed. The root lattice is the lattice $L(\mathrm{D}_n)$ introduced in Example 6.1.8. It is generated by the roots

$$\varepsilon_1 - \varepsilon_2, \varepsilon_2 - \varepsilon_3, \ldots, \varepsilon_{n-1} - \varepsilon_n, \varepsilon_{n-1} + \varepsilon_n.$$

The automorphism group of $L(\mathrm{D}_n)$ is the group generated by the elements which induce sign changes and by elements which permute the coordinates; see Exercise 6.4.9. It is a group of order $2^n \cdot n!$ The reflections r_v with $v \in \Phi$ generate a subgroup of order $2^{n-1} \cdot n!$ It is the Coxeter group of type D_n with which we started and has index 2 in $\mathrm{Aut}(L(\mathrm{D}_n))$.

A_n ($n \geq 1$). Here the integral root system is

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

There are exactly $(n+1)n$ roots in Φ. Its root lattice is $L(\mathrm{A}_n)$ as introduced in Example 6.1.9. The automorphism group $\mathrm{Aut}(L(\mathrm{A}_n))$ is the direct product of the Coxeter group $W(\mathrm{A}_n) \cong \mathrm{Sym}_{n+1}$ (acting by permutations of the coordinates) and the group of order two generated by the scalar multiplication by -1; see Exercise 6.4.2. The case $n = 2$ is depicted in Figure 4.1.

E_n ($n = 6, 7, 8$). First consider $n = 8$ and take Φ to be the root system described in Exercise 5.4.4, that is,

$$\Phi = \{\pm\varepsilon_i \pm \varepsilon_j \mid 1 \leq i < j \leq 8\} \cup \left\{ \frac{1}{2}\sum_i (-1)^{m_i}\varepsilon_i \,\middle|\, \sum_i m_i \equiv 0 \pmod 2 \right\}.$$

Then Φ is again a restricted integral root system and so the Coxeter group $W(\mathrm{E}_8)$ leaves invariant the root lattice $\mathbb{Z}\Phi = L(\mathrm{E}_8)$.

Likewise, the roots for E_7 and E_6 in Φ lead to integral root systems for $W(\mathrm{E}_7)$ and $W(\mathrm{E}_6)$, respectively, and to corresponding lattices. These coincide with the lattices $L(\mathrm{E}_8)$, $L(\mathrm{E}_7)$, $L(\mathrm{E}_6)$ found in Example 6.1.12.

By Exercise 6.4.11, $d(L(\mathrm{E}_8)) = 1$, $d(L(\mathrm{E}_7)) = \sqrt{2}$, $d(L(\mathrm{E}_6)) = \sqrt{3}$.

The construction of an integral root system from the reflection representation of a Coxeter group in the above example can also be carried out in certain cases where the Coxeter matrix has entries greater than 3. In order to determine exactly which irreducible Coxeter groups have integral root systems, we start with the analysis of the 2-dimensional case.

Example 6.2.5 Let W be a finite Coxeter group of type $M = (m_{ij})_{1\leq i,j\leq 2}$ of rank 2 with $m = m_{12} \in \{2, 3, 4, 6\}$. In these cases, B is positive definite by Proposition 5.3.2. Starting from the root system corresponding to the reflection representation, cf. Definition 4.1.1, we produce an integral root system in each case. Recall that the root system is of the form $We_1 \cup We_2$ with $B(e_1, e_1) = B(e_2, e_2) = 2$ and $B(e_1, e_2) = -2\cos(\pi/m)$.

For $m = 2$, we have $M = \mathrm{A}_1 \times \mathrm{A}_1$. The set

$$\Phi(\mathrm{A}_1 \times \mathrm{A}_1) = \{\pm e_1, \pm e_2\}$$

is easily seen to be an integral root system.

For $m = 3$, we have $M = \mathrm{A}_2$, which has been dealt with in Example 6.2.4.

For $m = 4$, we have $M = \mathrm{B}_2$ and $B(e_1, e_2) = -\sqrt{2}$. The set

$$\Phi(\mathrm{B}_2) = \{\pm e_1, \pm\sqrt{2}e_2, \pm(e_1 + \sqrt{2}e_2), \pm(2e_1 + \sqrt{2}e_2)\}$$

is an integral root system. See Figure 6.2.

For $m = 6$, we have $M = \mathrm{G}_2$ and $B(e_1, e_2) = -\sqrt{3}$. The set

$$\begin{aligned}\Phi(\mathrm{G}_2) = \{&\pm e_1, \pm\sqrt{3}e_2, \pm(e_1 + \sqrt{3}e_2),\\ &\pm(2e_1 + \sqrt{3}e_2), \pm(3e_1 + \sqrt{3}e_2), \pm(3e_1 + 2\sqrt{3}e_2)\}\end{aligned}$$

is an integral root system. See Figure 6.3.

It is not true that the reflection representation of every finite Coxeter group gives an integral root system. For example H_2 does not, see Exercise 6.4.12. The key condition is that there be a W-invariant lattice in the reflection representation space.

Definition 6.2.6 Let (W, S) be a finite Coxeter system of rank n and let $\rho : W \to \mathrm{O}(n, \mathbb{R})$ be its reflection representation (the image is in $\mathrm{O}(n, \mathbb{R})$ by Proposition 5.3.2). Then W is called a *Weyl group* if there is an $\rho(W)$-invariant lattice in $\mathbb{R}^n$.

Lemma 6.2.7 *Let (W, S) be a Coxeter system of rank $n = 2$ whose Coxeter matrix M has off-diagonal entry $m = m_{12}$ with $1 < m < \infty$. Let ρ be the reflection representation of W in $\mathbb{R}^2$. Then the following statements are equivalent.*

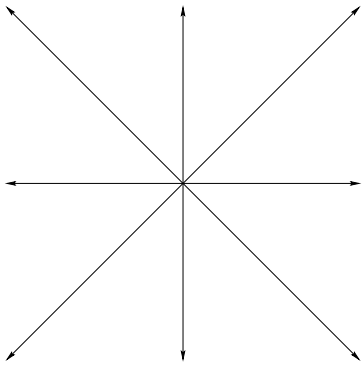


Fig. 6.2. The integral root system of type B_2.

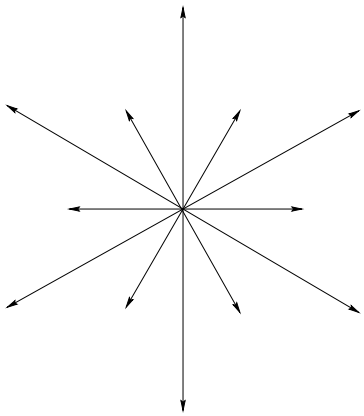


Fig. 6.3. The integral root system of type G_2.

(i) The group W is a Weyl group.
(ii) There is an integral root system Φ in $\mathbb{R}^2$ whose corresponding group $W(\Phi)$ coincides with $\rho(W)$.
(iii) $m = 2$, 3, 4, or 6.

Proof. Let $S = \{s_1, s_2\}$. The group $\rho(W)$ is generated by the two orthogonal reflections $\rho_1 = \rho(s_1)$ and $\rho_2 = \rho(s_2)$, with respect to the symmetric bilinear form B defined in (2.2) and with roots e_1, e_2, respectively, such that $B(e_1, e_1) = B(e_2, e_2) = 2$ and $B(e_1, e_2) = -2\cos(\pi/m)$. By Proposition 5.3.2, B is positive definite and so can be identified with the standard inner product after a coordinate transformation.

(i)⇒(iii). Let L be a $\rho(W)$-invariant lattice of $\mathbb{R}^2$. Let $i = 1, 2$. Since B is positive definite, it is nondegenerate, so there is $v \in L$ such that $B(v, e_i) \neq 0$. Therefore $B(v, e_i)e_i = (1 - \rho_i)v \in L$. This shows that a nonzero scalar multiple $\mu_i e_i$ of e_i belongs to L. Since $v \in L$ implies $-v \in L$, we may

suppose, without loss of generality, that $\mu_i > 0$. Moreover, L is a discrete subgroup of $\mathbb{R}^2$, so we can take μ_i minimal in $\mathbb{R}_{>0}$ such that $\mu_i e_i \in L$.

Taking $i = 2$ and $v = \mu_1 e_1 \in L$ in the above argument, we see that $(1 - \rho_2)\mu_1 e_1 = -2\mu_1 \cos(\pi/m)e_2$ also belongs to L. In particular, by minimality of μ_2, we have $2\mu_1 \cos(\pi/m)/\mu_2 \in \mathbb{Z}_{>0}$. Similarly, for $i = 1$, we find $2\mu_2 \cos(\pi/m)/\mu_1 \in \mathbb{Z}_{>0}$.

Multiplying the two scalars and putting $\mu = \mu_1/\mu_2$, we find a non-negative integer d with

$$2\cos(\pi/m) = \sqrt{d} \quad \text{and } \sqrt{d}/\mu,\ \mu\sqrt{d} \in \mathbb{Z}. \tag{6.2}$$

But, as $m \in [2, \infty)$, the quantity $2\cos(\pi/m)$ is less than 2, so $d = 0, 1, 2, 3$, and $m = 2, 3, 4, 6$ in the respective cases. This proves (iii).

(iii)⇒(ii). The existence of an integral root system in these cases is established in Example 6.2.5.

(ii)⇒(i). The lattice $\mathbb{Z}\Phi$ suffices for the proof of this implication. □

The above result does not yet precisely determine the integral root systems. For the case $m = 2$, or type $\mathrm{A}_1 \times \mathrm{A}_1$, the roots e_1 and e_2 can be replaced by any scalar multiple, but the other cases are (irreducible and) more rigid.

Corollary 6.2.8 *Suppose that (W, S) is a finite irreducible Coxeter system of rank 2 such that W is a Weyl group. Then the type M of (W, S) is one of A_2, B_2, or G_2 and, up to an interchange of e_1 and e_2, the integral root systems afforded by the reflection representation ρ of W in $\mathbb{R}^2$ are as described in Example 6.2.5. In particular, the following lattices are $\rho(W)$-invariant.*

$$\begin{cases} L(\mathrm{A}_2) = \mathbb{Z}e_1 + \mathbb{Z}e_2 & \text{in case of } \mathrm{A}_2, \\ L(\mathrm{B}_2) = \mathbb{Z}\sqrt{2}e_1 + \mathbb{Z}e_2 & \text{in case of } \mathrm{B}_2, \\ L(\mathrm{G}_2) = \mathbb{Z}e_1 + \mathbb{Z}\sqrt{3}e_2 & \text{in case of } \mathrm{G}_2. \end{cases}$$

The interchange of e_1 and e_2 would lead to isomorphic integral root system, and so there is no loss of generality in allowing it.

Proof. The type $\mathrm{A}_1 \times \mathrm{A}_1$ is ruled out by the irreducibility condition.

Let Φ be an integral root system for $\rho(W)$. As we have seen in the proof of Lemma 6.2.7, this implies, for $d = 1, 2, 3$ and $\mu = \mu_1/\mu_2$ as before, that (6.2) must hold. As $\sqrt{d}/\mu, \mu\sqrt{d} \in \mathbb{Z}$, there is an integer divisor g of d such that $\mu = \sqrt{d}/g$. But then $g = d$ or $g = 1$, which leads to the following five possibilities.

$$(d, \mu, m) = (1, 1, 3), \quad (2, \sqrt{2}^{\pm 1}, 4), \quad (3, \sqrt{3}^{\pm 1}, 6).$$

Now, for fixed $m = 4, 6$, the two distinct possibilities differ from each other by an interchange of e_1 and e_2. Hence the integral root systems must be as claimed. □

The classification of Weyl groups of higher rank follows directly from the lemma.

Theorem 6.2.9 *The following properties for a finite Coxeter system (W, S) of type M with reflection representation $\rho : W \to \mathrm{O}(n, \mathbb{R})$ are equivalent.*

(i) W is a Weyl group.
(ii) There is a restricted integral root system Φ such that $W(\Phi) = \rho(W)$.
(iii) The Coxeter matrix $M = (m_{ij})_{ij}$ satisfies $m_{ij} \in \{2, 3, 4, 6\}$ for all $1 \leq i < j \leq n$.

Moreover, the reflection representation of each irreducible Weyl group of rank $n > 2$ has a single integral root system in the space $\mathbb{R}^n$, with the exception of B_n, in which case there are two integral root systems, viz.,

$$\mathrm{B}_n : \Phi = \{\pm\varepsilon_i \pm \varepsilon_j \mid 1 \leq i, j \leq n\} \cup \{\pm\varepsilon_i \mid 1 \leq i \leq n\},$$
$$\mathrm{C}_n : \Phi = \{\pm\varepsilon_i \pm \varepsilon_j \mid 1 \leq i, j \leq n\} \cup \{\pm 2\varepsilon_i \mid 1 \leq i \leq n\},$$

where $\varepsilon_1, \ldots, \varepsilon_n$ is the standard orthonormal basis of $\mathbb{R}^n$.

In other words, the irreducible Coxeter groups that are Weyl groups have type A_n ($n \geq 1$), B_n ($n \geq 2$) with two non-isomorphic integral root systems for $n \geq 3$ (one of type B_n and the other of type C_n), D_n ($n \geq 4$), E_6, E_7, E_8, F_4, G_2.

Proof. If W has rank 1, there is nothing to prove. So we may assume that W has rank $n \geq 2$. Moreover, a reducible Coxeter group is easily seen to have any of the three properties if and only if the properties hold for each of its irreducible components. Thus, we may also assume that W is irreducible.

(i)⇒(iii). Suppose that (i) holds. Then there is a W-invariant lattice L containing a scalar multiple of each root. The restriction of $\langle s_i, s_j \rangle$ to $\mathbb{R}e_i + \mathbb{R}e_j$ satisfies Condition (ii) of Lemma 6.2.7, so $m_{ij} \in \{2, 3, 4, 6\}$, whence (iii).

(ii)⇒(i). This follows directly from the definition of Weyl group as $\mathbb{Z}\Phi$ is a $\rho(W)$-invariant lattice.

(iii)⇒(ii). Assume that (iii) holds. If all $m_{ij} \in [3]$, then M is simply laced and we can apply Lemma 6.2.3. Assume therefore, that there are $i, j \in [n]$ with $m_{ij} > 3$. So $m_{ij} \in \{4, 6\}$. If $n = 2$, assertion (ii) follows from Lemma 6.2.7. So, we may assume $n > 2$. By inspection of the list of all finite irreducible Coxeter groups, we find that $m_{ij} = 4$ and $We_i \cup We_j$ is a root system for W. As usual, we write $S = \{s_1, \ldots, s_n\}$. Corollary 6.2.8 shows that, up to an interchange of i and j, for some $\mu \in \mathbb{R}$ the lattice $\mathbb{Z}e_i + \mathbb{Z}\mu e_j$ of $U = \mathbb{R}e_i + \mathbb{R}e_j$ is invariant under the restriction of $W_{ij} = \langle s_i, s_j \rangle$ to U and contains the integral root system $W_{ij}e_i \cup \mu W_{ij}e_j$ in U with reflection group W_{ij}. We show that

$$\Phi = We_i \cup \mu We_j$$

is a restricted integral root system in $\mathbb{R}^n$ with $W(\Phi) = \rho(W)$. In fact, the only hard part is to establish Condition (ii) of Definition 6.2.1. This condition is a consequence of the claim that

$$\frac{2B(w(\mu_p e_p), \mu_q e_q)}{B(\mu_q e_q, \mu_q e_q)} = \mu_p/\mu_q B(we_p, e_q) \in \mathbb{Z}$$

for all $p, q \in \mathbb{N}$ and $w \in W$, where $\mu_k = \mu_j$ if $e_k \in We_j$ and $\mu_k = 1$ otherwise (that is, $e_k \in We_i$). The assertion in turn can be shown to hold by induction on $l(w)$, similarly to the proof of Lemma 6.2.3. For $w = 1$, it follows from Corollary 6.2.8. For $l(w) > 1$, take $k \in [n]$ and $u \in W$ such that $w = s_k u$ with $l(w) = 1 + l(u)$. Then

$$\begin{aligned}&\mu_p/\mu_q B(\rho(s_k u)e_p, e_q) = \mu_p/\mu_q B(\rho(u)e_p, \rho_k e_q)\\ &= \mu_p/\mu_q B(ue_p, e_q) - (\mu_k/\mu_q B(e_k, e_q))\,(\mu_p/\mu_k B(ue_p, e_k))\end{aligned}$$

is an integer in view of the induction hypothesis. Hence (ii).

In order to establish the final assertion of the theorem about integral root systems, observe that, if $n > 2$, we have $m_{ij} = 4$ as in the proof of the last implication, so the only case where ambiguity in a 2-dimensional subsystem may arise is B_2. Indeed, here it matters whether we take $\sqrt{2}e_{n-1}, e_n \in \Phi$ or $e_{n-1}, \sqrt{2}e_n \in \Phi$ for our choice of integral root system Φ. For the Coxeter diagram B_n, the first possibility leads to B_n, the second to C_n. For the Coxeter diagram F_4, the distinction is irrelevant as there is a diagram symmetry interchanging the roles of i and j in the proof of the last implication. □

If $n \geq 3$, the root lattices for B_n and C_n are not similar to each other, as the number of roots closest to the origin in $L(\mathbb{Z}\Phi)$ is $2n(n-1)$ for B_n and $2n$ for C_n.

6.3 Finite subgroups

Let (W, S) be a Coxeter system of type M and finite rank n. In this section we show that, up to conjugacy, the maximal finite subgroups of W are of the form W_J for $J \subseteq S$ (cf. Notation 4.2.5). In view of the classification of finite Coxeter groups, Theorem 5.3.3, this fully determines the finite subgroups of W.

Recall from Definition 2.3.6 the reflection representation $\rho : W \to \mathrm{GL}(V)$ and from Definition 3.3.1 the contragredient representation $\rho^* : W \to \mathrm{GL}(V^*)$ on the dual of V. For each $s \in S$, we put $A_s = \{f \in V^* \mid f(e_s) > 0\}$ and we set $A = \bigcap_{s \in S} A_s$. Furthermore, we take $\overline{A}$ to be the topological closure of A, that is, $\overline{A} = \{f \in V^* \mid \forall_{s \in S}\ f(e_s) \geq 0\}$. For $f \in V^*$, we denote by W_f the stabilizer in W of f, that is, the subgroup $\{w \in W \mid wf = f\}$ of W, where wf is short for $\rho^*(w)f$. It can be characterized as follows.

Proposition 6.3.1 *For each $f \in \overline{A}$ and $J = \{s \in S \mid f(e_s) = 0\}$, we have*

$$W_J = W_f = \{w \in W \mid wf \in \overline{A}\}.$$

Proof. $W_J \subseteq W_f$. Let $s \in J$. Then, by definition, $f(e_s) = 0$, so, for $x \in V$, we have $sf(x) = f(sx) = f(x) - B(x, e_s)f(e_s) = f(x)$, which shows $s \in W_f$, and hence $W_J = \langle J \rangle \subseteq W_f$.

$W_f \subseteq \{w \in W \mid wf \in \overline{A}\}$. This is immediate as $f \in \overline{A}$ and $w \in W_f$ means $wf = f$.

$\{w \in W \mid wf \in \overline{A}\} \subseteq W_J$. Let $w \in W$ and $g \in \overline{A}$ be such that $g = wf$. If $w = 1$, then clearly $w \in W_J$ and we are done. We proceed by induction on $l(w)$ and assume $l(w) > 0$. Then there is $s \in S$ with $l(ws) < l(w)$. By Proposition 4.1.2, $we_s \in \Phi^-$, so, as $g \in \overline{A}$,

$$0 \leq f(e_s) = w^{-1}g(e_s) = g(we_s) \leq 0.$$

Therefore, $f(e_s) = 0$, which gives $s \in J$. As $W_J \subseteq W_f$ (see above), we also have $sf = f$. Consequently, $(ws)f = wf = g \in \overline{A}$. By induction, $ws \in W_J$, and so $w = (ws)s \in W_J$, as required. □

For $f \in V^*$, write $\Phi_f = \{\alpha \in \Phi^+ \mid f(\alpha) < 0\}$. Notice that

$$\overline{A} = \{f \in V^* \mid \forall_{s \in S}\ \alpha_s \notin \Phi_f\} = \{f \in V^* \mid \Phi_f = \emptyset\}.$$

Proposition 6.3.2 *The union of $\overline{A}$ and its images under W satisfies*

$$\bigcup_{w \in W} w\overline{A} = \{f \in V^* \mid |\Phi_f| < \infty\}.$$

Proof. $\subseteq$. Let $w \in W$ and $f \in \overline{A}$. Recall Φ_w from (4.1). If $\alpha \in \Phi^+$ and $w^{-1}\alpha \in \Phi^+$, then $(wf)\alpha = f(w^{-1}\alpha) \geq 0$ and so

$$\Phi_{wf} = \{\alpha \in \Phi^+ \mid f(w^{-1}\alpha) < 0\} \subseteq \{\alpha \in \Phi^+ \mid w^{-1}\alpha \in \Phi^-\} = \Phi_{w^{-1}}.$$

By Corollary 4.1.5, the right hand side is finite, and so Φ_{wf} is finite. This proves $\bigcup_{w \in W} w\overline{A} \subseteq \{f \in V^* \mid |\Phi_f| < \infty\}$.

$\supseteq$. Suppose $f \in V^*$ satisfies $|\Phi_f| < \infty$. We will show that $f \in w\overline{A}$ for some $w \in W$. If $|\Phi_f| = 0$, then, by the observation preceeding the proposition, $f \in \overline{A}$, and we are done with $w = 1$. We proceed by induction on $|\Phi_f|$. Assume $|\Phi_f| > 0$, so there is $s \in S$ with $f(e_s) < 0$. Now $e_s \notin \Phi_{sf}$ as $sf(e_s) = f(se_s) = -f(e_s) > 0$. But s preserves $\Phi^+\backslash\{e_s\}$ by Corollary 4.1.5, and, for $\beta \in \Phi^+\backslash\{e_s\}$, we have $\beta \in \Phi_{sf}$ if and only if $f(s\beta) < 0$, which is equivalent to $s\beta \in \Phi_f$. Therefore, $\Phi_{sf} = s(\Phi_f\backslash\{e_s\})$, which has cardinality $|\Phi_f| - 1$. By the induction hypothesis applied to sf, we find $sf = u\overline{A}$ for some $u \in W$, and so $f \in su\overline{A}$, as required. This proves the proposition. □

Definition 6.3.3 Let (W, S) be a Coxeter system. A *parabolic* subgroup of W is a subgroup that is conjugate in W to a subgroup of the form W_J for some $J \subseteq S$.

Theorem 6.3.4 *Let (W, S) be a Coxeter system of finite rank. If H is a finite subgroup of W, then H is contained in a finite parabolic subgroup of W.*

Proof. If W is finite, then the choice $J = S$ and $w = 1$ suffice, so assume W is of infinite order. Then, by Theorem 5.2.4, Φ is infinite as well. It follows that $|S| > 1$. We proceed by induction on $|S|$.

Let $f \in A$ and take $g = \sum_{h \in H} hf$. Then, for each $h \in H$,

$$hg = \sum_{k \in H} hkf = \sum_{k \in H} kf = g,$$

so $H \subseteq W_g$. By Proposition 6.3.2, Φ_{hf} is a finite set for each $h \in H$, so $\bigcup_{h \in H} h\Phi_f$ is a finite subset of the infinite set Φ^+. Consequently, there is $\alpha \in \Phi^+ \setminus \bigcup_{h \in H} h\Phi_f$. Now, for each $h \in H$, we have $h^{-1}\alpha \notin \Phi_f$, so $hf(\alpha) \geq 0$, and hence $g(\alpha) \geq 0$, that is, $\alpha \notin \Phi_g$. Therefore, Φ_g is contained in the finite set $\bigcup_{h \in H} h\Phi_f$, and so is finite. By Proposition 6.3.2 this implies that $v^{-1}g \in \overline{A}$ for some $v \in W$. Now, for each $h \in H$, we have $v^{-1}hv(v^{-1}g) = v^{-1}hg = v^{-1}g$, so $v^{-1}hv \in W_{v^{-1}g}$. By Proposition 6.3.1, setting $T = \{s \in S \mid v^{-1}g(e_s) = 0\}$, we find $v^{-1}Hv \subseteq W_T$.

Also, as $f(\alpha) > 0$ and $hf(\alpha) \geq 0$ for each $h \in H$, we have $g(\alpha) > 0$. This gives $g \neq 0$. If $T = S$, then $v^{-1}g(e_s) = 0$ for each $s \in S$, so $g = 0$, a contradiction. So $|T| < |S|$ and we can apply induction to the finite subgroup $v^{-1}Hv$ of the Coxeter group W_T. This gives a subset J of T and an element u of W_T such that W_J is finite and $v^{-1}Hv \subseteq uW_Ju^{-1}$, so $vuW_J(vu)^{-1}$ is a finite parabolic subgroup of W containing H, as required. □

6.4 Exercises

Section 6.1

Exercise 6.4.1 Let v be a nonzero vector of the lattice L with square norm $(v, v) = 1$ or $(v, v) = 2$. Prove that $r_v \in \mathrm{Aut}(L)$.

Exercise 6.4.2 (Cited in Examples 6.1.9 and 6.2.4) Prove that the automorphism group of the lattice $L(\mathrm{A}_n)$, defined in Example 6.1.9, is isomorphic to $\mathrm{Sym}_{n+1} \times (\mathbb{Z}/2\mathbb{Z})$.
(*Hint:* Show that $\{\pm\varepsilon_1, \ldots, \pm\varepsilon_{n+1}\}$ is a single orbit under $\mathrm{Aut}(L)$, apply Lagrange's theorem to this orbit (which states that the length of an orbit multiplied by the size of the stabilizer of a member of the orbit equals the order of the group), and use induction on n to determine the size of the stabilizer of ε_1; take care of scalar multiplication by -1.)

Exercise 6.4.3 Suppose that Y is a finite subset of $\mathbb{R}^n$ with $(x, y) \in \mathbb{Z}$ for all $x, y \in Y$. Is $\mathbb{Z}Y := \{\sum_{y \in Y} a_y y \mid a_y \in \mathbb{Z}\}$ a lattice of $\mathbb{R}^n$?

Exercise 6.4.4 Let A and B be square matrices whose entries are rational with nonzero determinants. Show that $L(A) \subseteq L(B)$ if and only if there is a matrix P with integer entries but inside $\mathrm{GL}(n, \mathbb{Q})$ (that is, invertible over the rationals) such that $A = BP$.

Exercise 6.4.5 Let A be a square matrix with rational entries and nonzero determinant. Prove that $L(A)^\circ = L(A^{-\top})$. Conclude that $[L(A)^\circ : L(A)]$ is equal to the discriminant of $L(A)$.

Section 6.2

Exercise 6.4.6 As usual, denote by $(\cdot, \cdot)$ the standard inner product on $\mathbb{R}^n$. Let L be a lattice of $\mathbb{R}^n$ and let Φ be the set of all vectors $v \in L$ such that $2(w, v)/(v, v) \in \mathbb{Z}$ for all $w \in L$. Suppose that Φ is non-empty. Show that Φ is an integral root system in the linear subspace of $\mathbb{R}^n$ spanned by Φ and that $W(\Phi)$ is a subgroup of $\mathrm{Aut}(L)$.

Exercise 6.4.7 Let Φ be an integral root system of type M. Prove that the additive group $(\mathbb{Z}\Phi)^\circ/\mathbb{Z}\Phi$ has the following structure in the respective cases.

(a) For $M = \mathrm{A}_n$, cyclic of order $n + 1$.
(b) For $M = \mathrm{D}_n$ with n odd, cyclic of order 4.
(c) For $M = \mathrm{D}_n$ with n even, the direct product of two cyclic groups of order 2 (the Klein Four group).

Exercise 6.4.8 Recall from the proof of Lemma 6.2.7 what the integral root systems of rank 2 look like in terms of the roots e_1, e_2. In Example 4.1.6 we have described Φ for A_n in terms of the standard basis $\varepsilon_1, \ldots, \varepsilon_{n+1}$ of $\mathbb{R}^{n+1}$ and in Theorem 6.2.9 we have given Φ for B_n in terms of the standard basis of $\mathbb{R}^n$. Give a similar description of the integral root system of type G_2 in terms of integer linear combinations of the standard basis of $\mathbb{R}^3$.

Exercise 6.4.9 Consider the lattice $L = L(\mathrm{D}_n)$ of Example 6.1.8.

(a) Verify that the set of vectors in L of square norm 2 is isomorphic to the root system of type M, where $M = \mathrm{A}_1$ if $n = 1$, $M = \mathrm{A}_1 \dot\cup \mathrm{A}_1$ if $n = 2$, $M = \mathrm{A}_3$ if $n = 3$, and $M = \mathrm{D}_n$ if $n \geq 4$.
(b) Let M be as in (a) and $n \geq 2$. Prove that group generated by the orthogonal reflections r_v for $v \in L$ with $(v, v) = 2$ is a Coxeter group of type M.
(c) Prove that the group generated by the orthogonal reflections r_v for $v \in L$ with $(v, v) = 2$ is a Coxeter group of type M.

(d) Prove that the automorphism group of L is isomorphic to $W(\mathrm{B}_n)$ for $n \geq 2$.

Exercise 6.4.10 Prove the following assertions regarding the lattice $L = L(\mathrm{E}_8)$ of Example 6.1.12(iii).

(a) $L = \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 + \cdots + \mathbb{Z}\alpha_8$, where $\alpha_1, \ldots, \alpha_8$ are as in Exercise 5.4.4.
(b) Let Φ be the set of vectors in L of square norm 2. Then Φ is a root system of type E_8 and $L = \mathbb{Z}\Phi$.
(c) The group $W(\Phi)$ is a subgroup of $\mathrm{Aut}(L(\mathrm{E}_8))$ and acts transitively on Φ.
(d) Put $\alpha_0 = 2\alpha_1 + 3\alpha_2 + 4\alpha_3 + 6\alpha_4 + 5\alpha_5 + 4\alpha_6 + 3\alpha_7 + 2\alpha_8$. Then α_0 is orthogonal to each α_i for $i \in [7]$ and $(\alpha_0, \alpha_8) = 1$.
(e) The set $\alpha_0^\perp \cap \Phi$ is an integral root system in $\alpha_0^\perp$ of type E_7 and $W(\alpha_0^\perp \cap \Phi)$ has a single orbit of roots $\beta \in \Phi$ with $(\alpha_0, \beta) = 1$. In particular, $W(\Phi)$ acts transitively on the set of pairs (α, β) in $\Phi \times \Phi$ with $(\alpha, \beta) = 1$.

Exercise 6.4.11 Prove that $d(L(\mathrm{E}_n)) = 1, \sqrt{2}, \sqrt{3}$ for $n = 8, 7, 6$, respectively.

Exercise 6.4.12 Let (W, S) be the Coxeter system of type H_2 and set $\tau = 2\cos(\pi/5) - 1 = 2\cos(2\pi/5)$.

(a) Express the five positive roots as linear combinations of the fundamental roots $\Delta = \{e_1, e_2\}$ with coefficients in the ring $\mathbb{Z}[\tau]$.
(b) Prove that, in the usual reflection representation, $W(\mathrm{H}_2)$ leaves invariant the additive subgroup $\mathbb{Z}[\tau]e_1 + \mathbb{Z}[\tau]e_2$ of $\mathbb{R}^2$, but no lattice of $\mathbb{R}^2$.

Exercise 6.4.13 Show that, in Example 6.2.4, the simply laced case, all inner products of roots are in $\{0, \pm 1, \pm 2\}$.

Exercise 6.4.14 Let L be a lattice of $\mathbb{R}^n$ and let p be a prime.

(a) Show that $\mathrm{Aut}(L)$ leaves invariant the set pL of scalar multiples of members of L by p. Conclude that there is a linear action of the group $\mathrm{Aut}(L)$ on L/pL.
(b) Verify that $L/pL \cong (\mathbb{Z}/p\mathbb{Z})^n$ and conclude that the action of (a) gives a homomorphism of groups $\mathrm{Aut}(L) \to \mathrm{GL}((\mathbb{Z}/p\mathbb{Z})^n)$.
(c) Suppose that L is integer valued. Prove that the image of the homomorphism in (b) lies in the orthogonal group with respect to the symmetric bilinear form κ on $(\mathbb{Z}/p\mathbb{Z})^n$ given by $\kappa(x + pL, y + pL) = (x, y) \pmod p$ for $x, y \in L$.
(d) Let L be the lattice $L(\mathrm{E}_8)$ of Example 6.1.12(iii). Prove that κ is nondegenerate and determine the kernel of the homomorphism of (c) in the case where $p = 2$.

Section 6.3

Exercise 6.4.15 Let W be a Coxeter group. Prove that $V^* = \bigcup_{w \in W} w\overline{A}$ if and only if W is finite.

Exercise 6.4.16 Let (W, S) be a Coxeter system.

(a) Prove that, for each $J \subseteq S$, the subgroup W_J is the stabilizer of a vector in $\overline{A}$.
(*Hint:* Consider $\sum_{s \in S \setminus J} f_s$, where f_s $(s \in S)$ is the dual basis of e_s $(s \in S)$.)
(b) Conclude that each parabolic subgroup of W is the stabilizer of a vector in $\bigcup_{w \in W} w\overline{A}$.

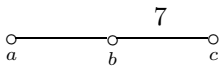
Exercise 6.4.17 Let W be the Coxeter group of type E_6. Determine if the subgroups $W_{\{1,3\}}$ and $W_{\{5,6\}}$ are conjugate in W.

Exercise 6.4.18 Let T be the group with presentation

$$T = \langle u, t \mid u^3 = t^2 = (ut)^7 = 1 \rangle.$$

(This group as acts on the hyperbolic plane in a manner consistent with the tiling of Figure 1.4.)

(a) Prove that there is an automorphism β of T such that $\beta(u) = u^{-1}$ and $\beta(t) = utu^{-1}$.
(b) Verify that β has order 2 and conclude that the semi-direct product $W = T \rtimes \langle b \rangle$, where $\langle b \rangle$ is the cyclic group of order 2, is well defined by $bx = \beta(x)b$ for each $x \in T$.
(c) Consider the elements $a = u^{-1}b$ and $c = tu^{-1}b$ of W. Prove that $(W, \{a, b, c\})$ is a Coxeter system of type



and that T consists of the elements in W of even length with respect to $\{a, b, c\}$.
(d) Which numbers occur as orders of finite elements of T?
(*Hint:* Apply the theory to W first.)

6.5 Notes

Section 6.1. The material on lattices of this section is quite standard. A good introduction to the basics of lattices is in [33].

Section 6.2. In [2] and at many other places, an integral root system as introduced in Definition 6.2.1 is called a root system. Our notion of root system (Definition 4.1.1) is the one from [13].

There is also a characterization of Coxeter types whose corresponding Coxeter groups leave invariant an additive subgroup of the space of the reflection representation isomorphic to $\mathbb{Z}^n$. Here the symmetric bilinear form is no longer positive definite, and the notion of lattice refers only to its structure as an abelian group. To distinguish such lattices from those handled in this chapter, the latter are usually called Euclidean lattices. Examples in which the form B is positive semi-definite are the so-called affine Weyl groups.

Weyl groups distinguish themselves from other Coxeter groups in that they occur in the normalizers of maximal tori (abelian subgroups all of whose elements are diagonizable in linear representations) of complex Lie groups. Cartan and Killing recognized the importance of root systems for Lie groups. A systematic treatment in connection with algebraic groups is found in the work of Chevalley. See [34] for an excellent treatment.

We did not treat *root data*, which is a slightly more general treatment of root systems. These provide a more symmetric treatment with respect to duality and furnish convenient combinatorial data for the classification of algebraic groups. They originate from work by Demazure and Grothendieck; see [34] again.

Section 6.3. The treatment mainly follows [19]. There are many more results on reflection subgroups, with which we have not dealt. For instance, Dyer's proofs that every subgroup generated by reflections in the reflection representation is again a Coxeter group, see [15].

Another interesting treatment of subgroups of Coxeter groups, in general not generated by reflections but still isomorphic to Coxeter groups, is due to Mühlherr [26]. Some of the resulting subgroups play a role as relative Weyl groups in fixed point subgroups of algebraic groups, as can be found in work of Borel and Tits and of Satake [35].

7. Coxeter groups are automatic

If A is an alphabet, then $\mathrm{M}(A)$ is the set of words in A. It is a monoid, encountered in Definition 2.1.1. A language over A is understood to be a subset of $\mathrm{M}(A)$.

Among the simplest languages in many senses are so-called regular languages. These languages and their connection with finite state automata are basic topics in computer science. We provide an ultra-brief introduction into automata (see Section 7.1). The material has been very well covered in many textbooks.

In this chapter, we will show that, for each Coxeter system (W, S) of finite rank, a regular language L over S exists such that the restriction to L of the usual map $\delta : \mathrm{M}(S) \to W$ (of Remark 2.1.6) is a bijection. This observation can be turned into a method for rewriting an arbitrary element $\underline{a} \in \mathrm{M}(S)$ to the unique member of $L \cap \delta^{-1}(\delta(\underline{a}))$, but this will not be discussed here.

In Section 7.2, we derive properties of the root system Φ, the most important of which is the finiteness of a certain set E (see Theorem 7.2.9) whose subsets will play a role in the construction of a finite state automaton accepting the regular language corresponding to W. Section 7.3 is devoted to this construction; the main result is Theorem 7.3.7.

7.1 Automata

Regular languages can be defined in various ways. We start with an approach using finite state automata.

Definition 7.1.1 A *finite state automaton* over the alphabet A consists of a finite set $\mathcal{S}$ of *states* and a transition map $\tau : A \times \mathcal{S} \to \mathcal{S}$. Moreover, there is a distinguished *initial state* $S_0 \in \mathcal{S}$ and a partition of $\mathcal{S}$ into *accept states* $\mathcal{S}_{\mathrm{y}}$ and *reject states* $\mathcal{S}_{\mathrm{n}}$. The map τ describes an action of the monoid $\mathrm{M}(A)$ (see Definition 2.1.1) on $\mathcal{S}$ determined by $\tau(a)X = \tau(a, X)$ for $a \in A$ and $X \in \mathcal{S}$. The *language* accepted by the finite state automaton is $\{\underline{a} \in \mathrm{M}(A) \mid \tau(\underline{a})S_0 \in \mathcal{S}_{\mathrm{y}}\}$. A *regular language* over A is a subset of $\mathrm{M}(A)$ accepted by a finite state automaton.

Example 7.1.2 Here is an example of a finite state automaton F over the alphabet $A = \{1, 2\}$. The $\mathcal{S}$ of F are the initial state S_0, which is also an accept state, the other accept states S_1 and S_2, and the reject state NO. The map τ is given in Table 7.1.

Table 7.1. The transition function τ of the finite state automaton F. If a value $\tau(a, X)$ is not listed, it is NO.

a	X	$\tau(a, X)$
1	S_0	S_1
2	S_0	S_2
1	S_2	S_1
2	S_1	S_2

The language accepted by F is

$$\{(12)^n 1, (21)^n 2, (12)^n, (21)^n \mid n \in \mathbb{N}\}.$$

A completely different approach uses regular expressions.

Definition 7.1.3 Let A be an alphabet and take a copy $\underline{A} := \{\underline{a} \mid a \in A\}$. A *regular expression* over A is an expression involving the letters from $\underline{A}$, the symbols $\underline{\varepsilon}$ and $\underline{\emptyset}$ (not in $\underline{A}$ or A), and built up recursively by use of the binary operators $+$ and $\cdot$ (both written as infix, usually with the dot $\cdot$ itself omitted) and the unary operator $*$ (written as an exponent).

The *language of the regular expression* x, notation, $L(x)$, is the subset of $\mathrm{M}(A)$ obtained from x by the following rules.

(i) $L(\underline{\emptyset}) = \emptyset$.
(ii) $L(\underline{\varepsilon}) = \{\varepsilon\}$.
(iii) If $a \in A$, then $L(\underline{a}) = \{a\}$.
(iv) If x and y are regular expressions, then $L(x + y) = L(x) \cup L(y)$.
(v) If x and y are regular expressions,

$$L(xy) = L(x)L(y) := \{ab \mid a \in L(x), b \in L(y)\}.$$

(vi) If x is a regular expression, then

$$L(x^*) = L(x)^* := \{a_1 a_2 \cdots a_n \mid n \in \mathbb{N}, a_1, \ldots, a_n \in L(x)\}.$$

Example 7.1.4 The regular language F of Example 7.1.2 is the language of the regular expression

$$(\underline{12})^*(\underline{1} + \underline{\varepsilon}) + (\underline{21})^*(\underline{2} + \underline{\varepsilon}).$$

Observe that the regular expression for a given language is not unique.

Theorem 7.1.5 *Let A be a finite alphabet. A language over A is regular if and only if it is the language of a regular expression over A.*

For proving that a language is not a regular language, the following famous lemma is very useful.

Lemma 7.1.6 (Pumping Lemma) *Suppose that L is a regular language over the finite alphabet A. Then there is a constant $c \in \mathbb{N}$ such that, if $z \in L$ has length $l(z) \geq c$, there are $u, v, w \in \mathrm{M}(A)$ with $l(uv) \leq c$, $l(v) \geq 1$, $z = uvw$ and, for each $i \in \mathbb{N}$, also $uv^i w \in L$.*

Example 7.1.7 Consider the subset $L = \{1^n \mid n \text{ is a prime}\}$ of $\mathrm{M}(\{1\})$. Suppose it is regular. Let c be a constant as in the Pumping Lemma 7.1.6 for L. Take a prime $p > c$ and consider $z = 1^p$. By the lemma, there are non-negative integers $a, b \in \mathbb{N}$ so that, with $u = 1^a$, $v = 1^b$ and $w = 1^{p-a-b}$, we have $a + b \leq c$, $b \geq 1$, and $1^{b(i-1)+p} = 1^a 1^{bi} 1^{p-a-b} \in L$ for each $i \in \mathbb{N}$. This implies that the sequence p, $p+b$, $p+2b, \ldots$ consists entirely of primes. But $p + pb$ has factors $b + 1$ and p, both of which are not equal to 1, a contradiction. Hence L is not regular.

7.2 Minimal roots

The main result of this section is Theorem 7.2.9. Throughout the section, we let (W, S) be a Coxeter system of finite rank n with root system Φ. When describing the action of W on Φ, we will suppress the mapping ρ of Definition 3.3.1 in our notation, and write $w\alpha$ instead of $\rho(w)\alpha$ for $\alpha \in \Phi$ and $w \in W$. Similarly, for subsets X of Φ, we will write wX instead of $\rho(w)X$.

Definition 7.2.1 For $\alpha \in \Phi^+$, the *depth* of α, notation $\mathrm{dp}(\alpha)$, is the minimal number k for which there is an element $w \in W$ of length k such that $w\alpha \in \Phi^-$. So the set $\Delta = \{e_1, \ldots, e_n\}$ consists of all roots of depth 1.

Lemma 7.2.2 *For $\alpha \in \Phi^+$ and $s \in S$, we have*

$$\mathrm{dp}(s\alpha) = \begin{cases} \mathrm{dp}(\alpha) - 1 & \text{if } B(\alpha, e_s) > 0 \\ \mathrm{dp}(\alpha) & \text{if } B(\alpha, e_s) = 0 \\ \mathrm{dp}(\alpha) + 1 & \text{if } B(\alpha, e_s) < 0 \end{cases}$$

Proof. If $B(\alpha, e_s) = 0$, then $s\alpha = \alpha$, so $\mathrm{dp}(s\alpha) = \mathrm{dp}(\alpha)$.

Suppose $B(\alpha, e_s) > 0$. Clearly, $\mathrm{dp}(s\alpha) \geq \mathrm{dp}(\alpha) - 1$, so it suffices to show $\mathrm{dp}(s\alpha) \leq \mathrm{dp}(\alpha) - 1$. Take $v \in W$ such that $v\alpha \in \Phi^-$ and $l(v) = \mathrm{dp}(\alpha)$. If $ve_s \in \Phi^-$, then take $w = vs$. By Proposition 4.1.2(iv), $l(w) < l(v)$. As $v\alpha \in \Phi^-$, we have $ws\alpha \in \Phi^-$ and so $\mathrm{dp}(s\alpha) \leq l(w) < l(v) = \mathrm{dp}(\alpha)$, as required.

Assume, therefore, $ve_s \in \Phi^+$. Now $vs\alpha = v\alpha - B(\alpha, e_s)ve_s$. Since both $v\alpha$ and $-ve_s$ are in Φ^- and $B(\alpha, e_s) > 0$, we have $vs\alpha \in \Phi^-$. Notice that $v\alpha$ and ve_s are not linearly dependent, for otherwise, α, being a scalar multiple of e_s lying in Φ^+, must be equal to e_s, contradicting $v\alpha \in \Phi^-$ and $ve_s \in \Phi^+$. Since both $v\alpha$ and $-B(\alpha, e_s)ve_s$ are linear combinations of elements Δ with non-positive coefficients, it follows that $vs\alpha \notin -\Delta$. Observe also that $v \neq 1$ as $v\alpha \in \Phi^-$. Therefore, there is $t \in S$ with $l(tv) < l(v)$. Set $w = tv$. Now $ws\alpha = tvs\alpha \in \Phi^-$ as $vs\alpha \in \Phi^-$ is not a scalar multiple of e_t. This means that $\mathrm{dp}(s\alpha) \leq l(w) = l(v) - 1 < \mathrm{dp}(\alpha)$, which establishes the case where $B(\alpha, e_s) > 0$.

Finally, suppose $B(\alpha, e_s) < 0$. Then $B(s\alpha, e_s) = B(\alpha, se_s) = -B(\alpha, e_s) > 0$, so, by the previous case, $\mathrm{dp}(\alpha) = \mathrm{dp}(s(s\alpha)) = \mathrm{dp}(s\alpha) - 1$, and we are done. □

Definition 7.2.3 For $\alpha, \beta \in \Phi^+$ we say that β *preceeds* α, notation $\beta \preceq \alpha$, if there is an element $w \in W$ of length $\mathrm{dp}(\alpha) - \mathrm{dp}(\beta)$ such that $\alpha = w\beta$.

So, β preceeds α if it occurs in a chain of minimal length starting at α and ending at a negative root whose steps are of the form γ, $s\gamma$ for some $s \in S$.

Lemma 7.2.4 *The relation $\preceq$ is a partial order on Φ^+.*

Proof. [3] Suppose that $\alpha, \beta, \gamma \in \Phi^+$ satisfy $\alpha \preceq \beta$ and $\beta \preceq \gamma$. Then there are $v, w \in W$ such that $\beta = w\alpha$ and $\gamma = v\beta$ with $\mathrm{dp}(\beta) - \mathrm{dp}(\alpha) = l(w)$ and $\mathrm{dp}(\gamma) - \mathrm{dp}(\beta) = l(v)$. In order to establish transitivity, we need that $\alpha \preceq \gamma$. As $\mathrm{dp}(\alpha) - \mathrm{dp}(\gamma) = l(v) + l(w)$ and $vw\alpha = \gamma$, in order to conclude that $\alpha \preceq \gamma$, it suffices to show $l(vw) = l(v) + l(w)$.

Choose $u \in W$ satisfying $l(u) = \mathrm{dp}(\alpha)$ and $u\alpha \in \Phi^-$. Then $uw^{-1}v^{-1}\gamma = u\alpha \in \Phi^-$, so $l(uw^{-1}v^{-1}) \geq \mathrm{dp}(\gamma)$, which gives

$$\begin{aligned} l(uw^{-1}v^{-1}) &\leq l(u) + l(w) + l(v) \\ &= \mathrm{dp}(\alpha) + \mathrm{dp}(\beta) - \mathrm{dp}(\alpha) + \mathrm{dp}(\gamma) - \mathrm{dp}(\beta) = \mathrm{dp}(\gamma) \\ &\leq l(uw^{-1}v^{-1}). \end{aligned}$$

It follows that $l(uw^{-1}v^{-1}) = l(u)+l(w)+l(v)$. As $l(uw^{-1}v^{-1}) = l(u(vw)^{-1}) \leq l(u) + l((vw)^{-1}) = l(u) + l(vw)$, this implies $l(v) + l(w) \leq l(vw)$. But, clearly, $l(vw) \leq l(v) + l(w)$, so $l(v) + l(w) = l(vw)$. Therefore, indeed $\alpha \preceq \gamma$, and $\preceq$ is transitive.

If, in addition, $\gamma = \alpha$, then $\mathrm{dp}(\gamma) = \mathrm{dp}(\alpha)$, so $l(v) + l(w) = 0$, so $v = w = 1$ in W, and $\alpha = \beta$. This shows that $\preceq$ is antisymmetric. Reflexivity is obvious: $\alpha \preceq \alpha$ follows from the choice $w = 1$ in Definition 7.2.3. □

Definition 7.2.5 Let (W, S) be a Coxeter system with root system Φ. The relation dom on Φ^+ is defined by

$$\alpha \operatorname{dom} \beta \text{ if and only if } \{w \in W \mid \alpha \in \Phi_w\} \subseteq \{w \in W \mid \beta \in \Phi_w\}$$

for each $\alpha, \beta \in \Phi^+$, A root α is called *minimal* if there are no $\beta \in \Phi^+$ with $\beta \neq \alpha$ and $\alpha \operatorname{dom} \beta$.

By E we denote the set of all minimal elements of W.

If W is finite, then $E = \Phi^+$; see Exercise 7.4.6.

Proposition 7.2.6 *For $\alpha, \beta \in \Phi^+$ and $s \in S$ the following assertions hold.*

(i) If $\alpha \operatorname{dom} \beta$ and $w \in W$ satisfies $w\beta \in \Phi^+$, then $w\alpha \operatorname{dom} w\beta$.
(ii) $\alpha \operatorname{dom} \beta$ if and only $B(\alpha, \beta) \geq 2$ and $\operatorname{dp}(\alpha) \geq \operatorname{dp}(\beta)$.
(iii) If α is minimal and $\beta \preceq \alpha$, then β is minimal.
(iv) If α is minimal and $s\alpha \in \Phi^+ \backslash E$, then $s\alpha \operatorname{dom} \alpha$.

Proof. (i). Assume $\alpha \operatorname{dom} \beta$ and $w \in W$ satisfies $w\beta \in \Phi^+$. Then $w\alpha \in \Phi^+$. If $v \in W$ satisfies $w\alpha \in \Phi_v$, then, as $\alpha \operatorname{dom} \beta$, also $w\beta \in \Phi_v$, so $w\alpha \operatorname{dom} w\beta$.

(ii). As the statement is trivial in case $\alpha = \beta$, we will assume $\alpha \neq \beta$.

(ii) $\Rightarrow$. Suppose $\alpha \operatorname{dom} \beta$. Take $w \in W$ of length $\operatorname{dp}(\alpha)$ such that $w\alpha \in \Phi^-$. write $w = sv$ with $s \in S$ and $l(v) = l(w) - 1$. Then $v\alpha \in \Phi_s = \{e_s\}$, so $v\alpha = e_s$. As $\alpha \operatorname{dom} \beta$ and $w\alpha \in \Phi^-$, we have $sv\beta = w\beta \in \Phi^-$. But $v\beta \neq v\alpha = e_s$, so $v\beta \in \Phi^-$, and $\operatorname{dp}(\beta) \leq l(v) < l(w) = \operatorname{dp}(\alpha)$.

Suppose $B(\alpha, \beta) < 2$. Then the restriction of B to $\mathbb{R}\alpha + \mathbb{R}\beta$ is positive definite and, by Proposition 5.3.2, $\langle r_\alpha, r_\beta \rangle$ is finite, contradicting $\alpha \operatorname{dom} \beta$ by Exercise 7.4.6.

(ii) $\Leftarrow$. Suppose $B(\alpha, \beta) \geq 2$ and $\operatorname{dp}(\alpha) \geq \operatorname{dp}(\beta)$. Choose $w \in W$ of length $\operatorname{dp}(\beta) - 1$ such that $w\beta \in \Delta$. Then $w\alpha \in \Phi^+$, so $\operatorname{dp}(w\alpha) \geq \operatorname{dp}(w\beta)$. Moreover, by (i), $\alpha \operatorname{dom} \beta$ if and only if $w\alpha \operatorname{dom} w\beta$. Moreover, $B(w\alpha, w\beta) = B(\alpha, \beta) \geq 2$. Therefore, it suffices to prove the assertion for the pair $w\alpha$, $w\beta$ instead of α, β. In other words, we may and shall assume $\beta \in \Delta$. In particular, $r_\beta\alpha = \alpha - B(\alpha, \beta)\beta \in \Phi^+$. Suppose now $\alpha \operatorname{dom} \beta$ does not hold, that is, there is $x \in W$ with $x\alpha \in \Phi^-$ and $x\beta \in \Phi^+$. Then $xr_\beta\alpha = x\alpha + B(\alpha, \beta)(-x\beta) \in \Phi^-$ as $B(\alpha, \beta) \geq 2 > 0$. So $\alpha, r_\beta\alpha \in \Phi_x$ and hence $\lambda\alpha + \mu r_\beta\alpha \in \Phi_x$ for any $\lambda, \mu \geq 0$ such that $\lambda\alpha + \mu r_\beta\alpha \in \Phi^+$. As $B(\alpha, r_\beta\alpha) = B(\alpha, \alpha) - B(\alpha, \beta)^2 \leq -2$, the number of such roots in infinite; see Exercise 7.4.5. Therefore $|\Phi_x|$ is infinite, a contradiction with Corollary 4.1.5.

(iii). It suffices to prove the case where $\operatorname{dp}(\alpha) = \operatorname{dp}(\beta) + 1$. So assume $\alpha = t\beta$ for some $t \in S$. By Lemma 7.2.2, $B(\beta, e_t) < 0$. Assume $\beta \notin E$, so there is $\gamma \in \Phi^+$ with $\beta \neq \gamma$ and $\beta \operatorname{dom} \gamma$. Then, by (ii), $B(\beta, \gamma) \geq 2$, so $\gamma \neq e_t$. This implies $t\gamma \in \Phi^+$. By (i), $\alpha = t\beta \operatorname{dom} t\gamma$, a contradiction with $\alpha \in E$ as $\alpha = t\gamma$ contradicts $\beta = \gamma$.

(iv). If $s\alpha \notin E$, there is $\beta \in \Phi^+$ with $s\alpha \operatorname{dom} \beta$. If $\beta = s\alpha$, there is nothing to show, so assume this is not the case. Consequently, if $w \in W$ is such that $\alpha \in \Phi_w$, then, as $(ws)(s\alpha) \in \Phi^-$, we also have $(ws)\beta \in \Phi^-$. If $s\beta \in \Phi^+$, this proves $\alpha \operatorname{dom} s\beta$.

Suppose now $\alpha \in E$. By the above, $s\beta \in \Phi^+$ would imply $\alpha \operatorname{dom} s\beta$, and hence $\alpha = s\beta$, contradicting $\beta \neq s\alpha$. Therefore, $s\beta \in \Phi^-$. This means $\beta \in \Phi_s = \{e_s\}$, so $\beta = e_s$ and $s\alpha \operatorname{dom} \alpha$. □

Example 7.2.7 Let

$$M = \widetilde{A}_1 = \overset{1}{\circ} \overset{\infty}{\text{———}} \overset{2}{\circ}$$

Then $\Phi^+ = \{m\alpha_1 + (m+1)\alpha_2, (m+1)\alpha_1 + m\alpha_2 \mid m \in \mathbb{N}\}$. Now $(\alpha_1 + 2\alpha_2) \operatorname{dom} \alpha_2$ by Proposition 7.2.6(ii) as $\operatorname{dp}(\alpha_1 + 2\alpha_2) = 2 > 1 = \operatorname{dp}(\alpha_2)$ and $B(\alpha_1 + 2\alpha_2, \alpha_2) = -2 + 4 = 2$. Similarly, $(2\alpha_1 + \alpha_2) \operatorname{dom} \alpha_1$. By Proposition 7.2.6(i), it readily follows that $E = \{\alpha_1, \alpha_2\}$.

The theorem below is a key to the construction of finite state automata for Coxeter groups. Its proof needs the following lemma.

Lemma 7.2.8 *Suppose $\alpha = \sum_{s\in S} \lambda_s e_s$ and $\beta = \sum_{s\in S} \mu_s e_s$ are positive roots such that, for each $s \in S$, either $\lambda_s = \mu_s$ or $B(\alpha, e_s) = B(\beta, e_s)$. Then $B(\alpha, \beta) = 2$.*

Proof. As $\alpha - \beta \in \mathbb{Z}\{e_s \mid \lambda_s \neq \mu_s\}$, we have

$$B(\alpha, \alpha - \beta) = \sum_{s\in S} (\lambda_s - \mu_s) B(\alpha, e_s) = \sum_{s\in S} (\lambda_s - \mu_s) B(\beta, e_s) = B(\beta, \alpha - \beta).$$

This implies $2 - B(\alpha, \beta) = B(\beta, \alpha) - 2$, and so $B(\alpha, \beta) = 2$. □

Theorem 7.2.9 *The set E of minimal roots is finite.*

Proof. We first argue that there is a finite number of values $B(\alpha, \beta)$ for $\alpha, \beta \in \Phi^+$ with $B(\alpha, \beta)$ in the interval $(-2, 2)$. Indeed, by Lemma 5.1.6, for such α and β the subgroup $\langle r_\alpha, r_\beta \rangle$ of W is finite and hence, by Theorem 6.3.4, a subgroup of a finite parabolic subgroup W_J for some $J \subseteq S$. In particular, the orders $r_\alpha r_\beta$ must divide the exponent of one of the finite number of groups W_J for spherical $J \subseteq S$. Also, if $r_\alpha r_\beta$ has order k, then $B(\alpha, \beta) = 2\cos(\pi j/k)$ for some $j \in [2k]$. Hence there is a maximal number of values, say d, that $B(\alpha, \beta)$ can take for for $\alpha, \beta \in \Phi^+$ with $B(\alpha, \beta) \in (-2, 2)$.

Suppose now that the cardinality of E is infinite. Then there are roots in E of arbitrarily large depth. In particular, there is $\beta_m \in \Phi^+$ with $\operatorname{dp}(\beta_m) = m$

for $m = (d+1)^n + 1$. There exists a sequence $\beta_1 \prec \beta_2 \prec \cdots \prec \beta_m$ such that $\mathrm{dp}(\beta_i) = i$ and $r_i\beta_{i-1} = \beta_i$ for some $r_i \in S$. By Proposition 7.2.6(iii), $\beta_i \in E$ for each $i \in [m]$.

If $s \in S$ and $B(\beta_i, e_s) \leq -2$, then α_{i+1}, the positive root of r_{i+1}, is not equal to e_s, for otherwise $B(\beta_{i+1}, e_s) \geq 2$, which would imply by Proposition 7.2.6(ii) that $\beta_{i+1} \operatorname{dom} e_s$, a contradiction to $\beta_{i+1} \in E$ (the roots β_{i+1} and e_s are disctinct as they have distinct depths). Hence, by use of $\beta_{i+1} = r_{i+1}\beta_i = \beta_i - B(\beta_i, \alpha_{i+1})\alpha_{i+1}$, and $B(\beta_i, \alpha_{i+1}) < 0$ (according to Lemma 7.2.2),

$$B(\beta_{i+1}, e_s) = B(\beta_i, e_s) - B(\beta_i, \alpha_{i+1})B(\alpha_{i+1}, e_s) \leq -2.$$

By recursion, this shows $B(\beta_j, e_s) \leq -2$ and $\alpha_j \neq e_s$ for all $j > i$. In particular, the coefficient of e_s in β_j is equal to the coefficient of e_s in $\beta_{j-1} = r_j\beta_j$, and so remains fixed for $j > i$.

Now consider the sequence of vectors $(B(\beta_i, e_s))_{s\in S}$ for $i \in [m]$. Each of the n components of the vectors are in the open interval $(-\infty, 2)$ and either take on one of the d possible values in $(-2, 2)$ or lie below -2. As $m > (d+1)^n$, there will be $i, j \in [m]$ with $i < j$ such that, for each $s \in S$, either both $B(\beta_i, e_s) < -2$ and $B(\beta_j, e_s) < -2$ in which case the coefficients of e_s in β_i and β_j are the same, or $B(\beta_i, e_s) = B(\beta_j, e_s)$. By Lemma 7.2.8, $B(\beta_i, \beta_j) = 2$, so, as $\mathrm{dp}(\beta_j) = j > i = \mathrm{dp}(\beta_i)$, by Proposition 7.2.6(ii), $\beta_j \operatorname{dom} \beta_i$, contradicting that both are in E. □

7.3 Regular languages for Coxeter groups

Throughout the section, (W, S) is a Coxeter system of finite rank n with root system Φ, positive roots $\Phi^+ = \Phi \cap (\mathbb{R}_{\geq 0}e_1 + \cdots + \mathbb{R}_{\geq 0}e_n)$, and $\Delta = \{e_1, \ldots, e_n\}$.

Theorem 7.3.1 *Let (W, S) be a Coxeter system. Then the subset of all minimal expressions in $\mathrm{M}(S)$ for elements of W is a regular language over S.*

Proof. Take subsets of E to be the accept states, so $\mathcal{S} = \mathcal{P}(E) \cup \{NO\}$, and let τ be given by

$$\tau(s, X) = \begin{cases} NO & \text{if } e_s \in X \text{ or } X = NO \\ (sX \cup \{e_s\}) \cap E & \text{if } e_s \notin X \end{cases}$$

We claim

$$\tau(\underline{r}, \emptyset) = \begin{cases} NO & \text{if } \underline{r} \text{ is not a minimal expression} \\ \Phi_{w^{-1}} \cap E & \text{if } \underline{r} \text{ is a minimal expression of } w \end{cases}$$

The proof is by induction on the length, q say, of $\underline{r}$. Let $\underline{r} = r_1 \cdots r_q$ with $r_i \in S$. If $q = 0$, then $\underline{r}$ is a minimal expression of the identity element

$1 \in W$ and $\tau(\underline{r}, \emptyset) = \emptyset = \Phi_1$, so the claim holds. Suppose $q > 0$ and write $\underline{r}' = r_2 \cdots r_q$, so $\underline{r} = r_1\underline{r}'$. If $\underline{r}'$ is not a minimal expression, then neither is $\underline{r}$, and $\tau(\underline{r}, \emptyset) = \tau(r_1, \tau(\underline{r}', \emptyset)) = \tau(r_1, NO) = NO$, as required. Suppose, therefore, that $\underline{r}'$ is a minimal expression, so $\tau(\underline{r}', \emptyset) = \Phi_{w^{-1}r_1} \cap E$ by the induction hypothesis.

If $\underline{r}$ is a minimal expression, then $l(r_1(r_1w)) = 1 + l(r_1w)$, and so, by Exercise 4.4.5,

$$\Phi_{w^{-1}} = \Phi_{(r_1w)^{-1}r_1} = \Phi_{r_1} \cup r_1\Phi_{(r_1w)^{-1}} = \{\alpha_1\} \cup r_1\Phi_{(r_1w)^{-1}}.$$

Let $\gamma \in r_1\Phi_{(r_1w)^{-1}} \cap E$. If $r_1\gamma \notin E$, then by Proposition 7.2.6(v), $r_1\gamma \operatorname{dom} \alpha_1$, so, as $r_1\gamma \in \Phi^+$ and $(r_1w)^{-1}r_1\gamma \in \Phi^-$, also $-w^{-1}\alpha_1 = (r_1w)^{-1}\alpha_1 \in \Phi^-$, so $w^{-1}\alpha_1\Phi^+$, which is equivalent to $l(r_1w) > l(w)$ by Proposition 4.1.2(iv) and the observation that the length of an element is equal to the length of its inverse. But this contradicts, the assumption that $\underline{r}$ is minimal, so $r_1\gamma \in E$. This shows $r_1(r_1\Phi_{(r_1w)^{-1}} \cap E) \subseteq E$, and implies $r_1\Phi_{(r_1w)^{-1}} \cap E = r_1\Phi_{(r_1w)^{-1}} \cap r_1E \cap E = r_1(\Phi_{(r_1w)^{-1}} \cap E) \cap E$, so

$$\begin{aligned}
\Phi_{w^{-1}} \cap E &= (\{\alpha_1\} \cup r_1\Phi_{(r_1w)^{-1}}) \cap E = \{\alpha_1\} \cup (r_1\Phi_{(r_1w)^{-1}} \cap E) \\
&= \{\alpha_1\} \cup (r_1(\Phi_{(r_1w)^{-1}} \cap E) \cap E) = (\{\alpha_1\} \cup r_1(\Phi_{(r_1w)^{-1}} \cap E)) \cap E \\
&= (\{\alpha_1\} \cup r_1\tau(\underline{r}', \emptyset)) \cap E = \tau(r_1, \tau(\underline{r}', \emptyset)) \\
&= \tau(\underline{r}, \emptyset).
\end{aligned}$$

The one but last equality holds as $l(w) > l(r_1w)$, for this implies $\alpha_1 \notin \Phi_{(r_1w)^{-1}}$ and hence $\alpha_1 \notin \tau(\underline{r}', \emptyset)$. This settles the claim in case $\underline{r}$ is minimal.

If $\underline{r}$ is not minimal, then $l(r_1w) = 1 + l(w)$, so $\tau(\underline{r}', \emptyset) = \Phi_{(r_1w)^{-1}} \cap E = \Phi_{w^{-1}r_1} \cap E = \Phi_{w^{-1}r_1} \cap E = (\{\alpha_1\} \cup r_1\Phi_{w^{-1}}) \cap E$. As $\alpha_1 \in E$, it follows that $\alpha_1 \in \tau(\underline{r}', \emptyset)$, so $\tau(\underline{r}, \emptyset) = \tau(r_1, \tau(\underline{r}', \emptyset)) = NO$.

This ends the proof of the theorem as the claim gives that the set of words accepted by the automaton coincides with the set of minimal expressions of elements from W. □

The above shows that the Coxeter groups are very special from the point of view of representative words. We will pursue this one more step by proving that we can even obtain a regular language having a single representative word for each element of W.

Definition 7.3.2 Let $<$ be an ordering on S. Extend this ordering to the ordering $<$ on $\mathrm{M}(S)$ for which $x < y$ if and only if $l(x) < l(y)$ or $l(x) = l(y)$ and x is reverse lexicographically smaller than y, which means that there is $i \in [l(x)]$ such that $x = x_1 \cdots x_q$ and $y = y_1 \cdots y_q$ with $x_j = y_j$ for $j > i$ and $x_i < y_i$. This ordering is called the *DegRevLex* ordering on $\mathrm{M}(S)$.

For $w \in W$, denote by $\mu(w)$ the unique element of $\delta^{-1}(w)$ that is minimal with respect to $<$.

It may be convenient to reinterpret the identification of S and $[n]$ in such a way that the ordering on $[n]$ is the natural one. More importantly, the DegRevLex ordering has the following properties, which are essential for what is often called a reduction ordering.

Lemma 7.3.3 *Let $<$ be a DegRevLex ordering on $\mathrm{M}(S)$, and let $a, u, v \in \mathrm{M}(S)$.*

(i) If $u < v$, then $aub < avb$.
(ii) $\varepsilon \leq v$.
(iii) The ordering $<$ is Noetherian *in the sense that every strict monotonically decreasing sequence is finite.*

The (easy) proof is left to the reader. The following lemma will provide the precise criterion why the automaton of Theorem 7.3.7 below will recognize the image of μ in $\mathrm{M}(S)$.

Lemma 7.3.4 *Let $L = \{\mu(w) \mid w \in W\}$. Suppose $w \in W$ and $\underline{r} \in \mathrm{M}(S)$ satisfy $\mu(w) = \underline{r}$ and write $\underline{r} = r_1 \cdots r_q \in$. Then the following assertions hold for each $s \in S$.*

(i) The expression $s\underline{r}$ of sw is minimal if and only if there exists no $i \in [q]$ such that $e_s = r_1 r_2 \cdots r_{i-1} \alpha_i$, where α_i is the positive root of r_i.
(ii) Let $s\underline{r}$ be a minimal expression of sw. Then $s\underline{r} \notin L$ if and only if there are $i \in [q]$ and $t \in S$ with $t < r_i$ such that $\mu(s\underline{r}) = r_1 \cdots r_i t r_{i+1} \cdots r_q \in L$, in which case $e_s = r_1 r_2 \cdots r_i e_t$.

Proof. (i) is a recall of Theorem 4.2.2.

(ii). Suppose that $s\underline{r}$ is a minimal expression of sw and let $\mu(sw) = \underline{u} = u_1 \cdots u_{q+1}$.

Then, as $l(s(sw)) < l(sw)$, the exchange condition, Theorem 4.2.2, gives that there exists $i \in [q]$ such that, in W,

$$su_1 \cdots u_{i+1} = u_1 \cdots u_i. \tag{7.1}$$

As $\underline{u} \in L$ and $\delta(s\underline{r}) = sw = \delta(\underline{u})$, we have

$$\underline{u} \leq s\underline{r}$$

Similarly, As $\underline{r} \in L$ and $\delta(\underline{r}) = w = \delta(s\underline{u}) = \delta(u_1 \cdots u_i u_{i+2} \cdots u_{q+1})$, we have

$$\underline{r} \leq u_1 u_2 \cdots u_i u_{i+2} \cdots u_{q+1}.$$

Comparing the two ordering relations, we find $r_j = u_{j+1}$ for $j > i$, so, by Lemma 7.3.3(i),

$$u_1 \cdots u_{i+1} \leq s r_1 \cdots r_i$$
$$r_1 \cdots r_i \leq u_1 \cdots u_i.$$

Set $t = u_{i+1}$. Multiplication of the second inequality by $u_{i+1} \cdots u_{q+1}$ gives

$$r_1 \cdots r_i t r_{i+1} \cdots r_q \leq \underline{u} \text{ in } \mathrm{M}(S).$$

But both sides represent the same element sw and $\underline{u}$ is minimal in $\delta^{-1}(sw)$, so $r_1 \cdots r_i t r_{i+1} \cdots r_q = \underline{u}$ in $\mathrm{M}(S)$. This implies $r_j = u_j$ for $j \leq i$, and the equality $u_1 \cdots u_{i+1} = s r_1 \cdots r_i$ in W gives $r_1 \cdots r_i t = s r_1 \cdots r_i$.

Suppose now $s\underline{r} \notin L$. Then $\underline{u} < s\underline{r}$ and so $r_1 \cdots r_i t r_{i+1} \cdots r_q < s r_1 \cdots r_q$ in $\mathrm{M}(S)$, whence $r_1 \cdots r_i t < s r_1 \cdots r_i$ in $\mathrm{M}(S)$, But $t \neq r_i$ as $t r_i \cdots r_q$ is a minimal expression, so we must have $t < r_i$, as required. Also, rewriting the equality gives $s = r_1 \cdots r_i t r_i \cdots r_1$ in W. As $r_1 \cdots r_i t$ is a minimal expression, Proposition 4.1.2(ii), (iv) implies $e_s = r_1 \cdots r_i e_t$.

Conversely, if $t < r_i$ and $s r_1 \cdots r_i = r_1 \cdots r_i t$, then $r_1 \cdots r_i t r_{i+1} \cdots r_q < s\underline{r} \in \delta^{-1}(sw)$, and so $s\underline{r} \notin L$. This proves the lemma. □

Lemma 7.3.5 *If $\Phi_u \cap \Phi_{v^{-1}} \neq \emptyset$, then $l(uv) < l(u) + l(v)$.*

Proof. Observe that $\Phi_{uv} \subseteq \Phi_v \cup v^{-1}\Phi_u$. Suppose $\gamma \in \Phi_u \cap \Phi_{v^{-1}}$. Then $-v^{-1}\gamma$ belongs to Φ_v but not to Φ_{uv}. Hence $\Phi_v \cup v^{-1}\Phi_u$ strictly contains Φ_{uv}, so, by Corollary 4.1.5, $l(uv) = |\Phi_{uv}| < |\Phi_v \cup v^{-1}\Phi_u| \leq l(v) + l(u)$, as required. □

Lemma 7.3.6 *Suppose $\beta \in \Phi^+ \backslash E$ and $u, v \in W$ satisfy $u\beta, v^{-1}\beta \in \Delta$. Then*

$$l(uv) < l(u) + l(v).$$

Proof. Let $s, t \in S$ be such that $u\beta = e_s$ and $v^{-1}\beta = e_t$. Then $\beta \in \Phi_{su} \cap \Phi t v^{-1}$. As $\beta \notin E$, there is $\gamma \in \Phi^+$ with $\gamma \neq \beta$ and $\beta \operatorname{dom} \gamma$. By the definition of dominance, we find $su\gamma, tv^{-1}\gamma \in \Phi^-$. As $\beta \neq \gamma$, also $u\gamma \neq u\beta = e_s$. Recall $\Phi_s = \{e_s\}$, so $u\gamma \notin \Phi_s$, and hence $u\gamma \in \Phi^-$. Similarly, $v^{-1}\gamma \neq e_t$ and $v^{-1}\gamma \in \Phi^-$. Now $\gamma \in \Phi_u \cap \Phi_{v^{-1}}$, so, by Lemma 7.3.5, $l(uv) < l(u) + l(v)$. □

Theorem 7.3.7 *Let (W, S) be a Coxeter system. For each DegRevLex ordering on $\mathrm{M}(S)$, the set $\{\mu(w) \mid w \in W\}$ is a regular language in $\mathrm{M}(S)$.*

Proof. Let $\mathcal{S}$ be as before, that is, $\mathcal{S} = \mathcal{P}(E) \cup \{NO\}$, but define τ by

$$\tau(s, X) = \begin{cases} NO & \text{if } X = NO \\ NO & \text{if } e_s \in X \\ (sX \cup \{e_s\} \cup \{s\alpha_t \mid t \in S \text{ and } t < s\}) \cap E & \text{if } e_s \notin X \neq NO \end{cases}$$

By L we denote the language $\{\mu(w) \mid w \in W\}$. Consider the expression $\underline{r} = r_1 \cdots r_q$ for w. We need to show that $\underline{r} \in L$ if and only if $\underline{r}$ is accepted by

the automaton. Clearly, the empty word and each symbol in S is accepted by the automaton and belongs to L. So we may assume $q > 1$ and proceed by induction on q. For each $j \in [q]$, write $\Delta_j = \{e_s \mid s \in S \text{ and } s < r_j\}$ and X_j for the state of the automaton after reading r_j. As usual, we write α_j to denote the positive root corresponding to r_j.

Suppose that, for $i \in [q-1]$, the word $r_{i+1} \cdots r_q$ is accepted by the automaton and $r_i r_{i+1} \cdots r_q$ is not. We will show $r_i r_{i+1} \cdots r_q \notin L$. By induction on q, we may assume $i = 1$, Then, for $j > 1$, we have $\alpha_j \notin X_{j+1}$ and

$$X_j = \tau(r_j, X_{j+1}) \subseteq r_j X_{j+1} \cup \{\alpha_j\} \cup r_j \Delta_j,$$

so, by recursion on j,

$$X_2 \subseteq \{r_2 \cdots r_{j-1}\alpha_j \mid j = 2, \ldots, q-1\} \cup \bigcup_{2 \le j \le q} r_2 \cdots r_j \Delta_j.$$

Rejection implies $\alpha_1 \in X_2$. If $\alpha_1 = r_2 \cdots r_{j-1}\alpha_j$ for some $j > 1$, then, by Lemma 7.3.4(i), $r_1 r_2 \cdots r_j$ is not a minimal expression, contradicting that it belongs to L. Hence $\alpha_1 = r_2 \cdots r_j e_s$ for some $j > 1$ and $e_s \in \Delta_j$. But then, by Lemma 7.3.4(ii), $r_1 r_2 \cdots r_j \notin L$, so $\underline{r} \notin L$. This shows that all words of L are accepted by the automaton.

Conversely, suppose that $\underline{r} \notin L$, and choose $i < q$ minimal such that $r_{i+1} \cdots r_q \in L$. We need to show that $\underline{r}$ is not accepted by the automaton. Again, by the induction hypothesis, we may assume $i = 1$. We claim that $\alpha_1 \in X_2$.

If the word $\underline{r}$ is not a minimal expression, then, by Lemma 7.3.4(i), $\alpha_1 = r_2 \cdots r_{j-1}\alpha_j$ for some $j > 1$. Suppose now $\alpha_1 \notin X_2$. Choose k maximal in $[j]$ such that $r_k \cdots r_2 \alpha_1 \notin X_k$ and put $\beta = r_k \cdots r_2 \alpha_1$. As $\alpha_j \in X_j$ by construction, $k < j$. Now $r_{k+1} \cdots r_2 \alpha_1 \in X_{k+1}$ by maximality of k. So $\beta \in r_k X_{k+1}$. But $r_k X_{k+1} \cap E \subseteq X_k$ and $\beta \notin X_k$, so $\beta \notin E$. Now, with the elements $u = r_2 \cdots r_k$ and $v = r_{k+1} \cdots r_{j-1}$ of W, the roots $u\beta = \alpha_1$ and $v^{-1}\beta = \alpha_j$ are both in Δ, so Lemma 7.3.6 gives $l(uv) \neq l(u) + l(v) = j - 2$, contradicting that $r_2 \cdots r_{j-1}$ is a minimal expression. Hence $\alpha_1 \in X_2$.

Therefore, we may assume that the word $\underline{r}$ is a minimal expression. As $\underline{r} \notin L$, Lemma 7.3.4(ii) gives $j \in [q]$ and $t \in S$ with $t < r_j$ such that $\mu(\underline{r}) = r_2 \cdots r_j t r_{j+1} \cdots r_q \in L$ and $\alpha_1 = r_2 r_3 \cdots r_j e_t$. Recall $\alpha_1 \notin X_2$. Let $k \le j$ be maximal such that $r_k \cdots r_j e_t \notin X_k$ and put $\beta = r_k \cdots r_j e_t$. Note $k \ge 2$. If $k = j$, then $\beta = r_j e_t \notin X_j$, but $r_j e_t \in r_j \Delta_j$ and $r_j \Delta_j \cap E \subseteq X_j$, so $\beta \notin E$.

If $k < j$, then maximality forces $r_{k+1} \cdots r_j e_t \in X_{k+1}$ and, as $r_k X_{k+1} \cap E \subseteq X_k$, again $\beta \notin E$. As before, setting $u = r_2 \cdots r_{k-1}$ and $v = r_k \cdots r_j$ in W, we find that $u\beta = r_2 \cdots r_j e_t = \alpha_1$ and $v^{-1}\beta = e_t$ are both in Δ, so Lemma 7.3.6 gives $l(uv) < l(u) + l(v) = j - 2$, contradicting that $r_2 \cdots r_{j-1}$ is a minimal expression. Hence $\alpha_1 \in X_2$.

Thus, in all cases, $\alpha_1 \in X_2$, and so $\tau(r_1, X_2) = NO$. In other words, the automaton does not accept $\underline{r}$. This proves the theorem. □

Example 7.3.8 Let $M = \widetilde{A}_1$ and recall from Example 7.2.7 that $E = \{\alpha_1, \alpha_2\}$. The automaton described in the proof of Theorem 7.3.7 for this case coincides with the one of Example 7.1.2.

7.4 Exercises

Section 7.1

Exercise 7.4.1 Show that the language $\{(ab)^i \mid i \in \mathbb{N}\}$ in $\mathrm{M}(\{a, b\})$ is regular.

Exercise 7.4.2 Show that the language $\{a^i b^i \mid i \in \mathbb{N}\}$ in $\mathrm{M}(\{a, b\})$ is not regular.

Exercise 7.4.3 Give a finite state automaton that accepts the language of the regular expression $(ab + ba)^*$ over $\{a, b\}$.

Section 7.2

Exercise 7.4.4 Let (W, R) be a Coxeter system. Prove that, for each $\alpha \in \Phi^+$, we have $\mathrm{dp}(\alpha) = \frac{1}{2}(l(r_\alpha) + 1)$.

Exercise 7.4.5 (Cited in Proposition 7.2.6(ii)) Let α, β be distinct positive roots for the Coxeter system (W, S) such that $B(\alpha, \beta) \leq -2$. Show that, for each $n \in \mathbb{N}$,

$$(r_\alpha r_\beta)^n \alpha = \lambda_n \alpha + \mu_n \beta$$

with λ_n, $\mu_n \in \mathbb{R}$ such that $\lambda_{n+1} \geq \mu_n + 1$ and $\mu_{n+1} \geq \lambda_n + 1$.

Exercise 7.4.6 (Cited in Proposition 7.2.6(ii)) Let α, β be distinct positive roots of the Coxeter system (W, S). Prove that $\alpha \operatorname{dom} \beta$ implies that the subgroup $\langle r_\alpha, r_\beta \rangle$ of W has infinite order.

Exercise 7.4.7 Determine the set of minimal elements of the Coxeter group of type $\widetilde{\mathrm{A}}_2$ (given in Exercise 2.4.11).

Section 7.3

Exercise 7.4.8 Draw the finite state automaton of the proof of Theorem 7.3.7 for the case $M = \mathrm{A}_2$ in such a way that the states become nodes and the transitions become labeled directed edges between the nodes. Give a regular expression for the language accepted by this automaton.

Exercise 7.4.9 Draw the finite state automaton of the proof of Theorem 7.3.7 for the case $M = \widetilde{\mathrm{A}}_2$ in such a way that the states become nodes and the transitions become labeled directed edges between the nodes. Give a regular expression for the language accepted by this automaton.

Exercise 7.4.10 Let (W, R) be a Coxeter system. We will use notions of Definition 5.2.6. For each spherical subset J of S, we write w_J for the longest element of W_J. Denote by A the set of all these w_J and view it as an alphabet. Consider the map $\nu : W \to \mathrm{M}(A)$ given by $\nu(1) = \varepsilon$ and $\nu(w) = w_J \nu(w_J w)$ whenever $w \in W \backslash \{1\}$. Describe the image of ν in $\mathrm{M}(A)$ and prove that it is a regular language.

7.5 Notes

Section 7.1. There are many excellent introductions to automata theory. We mention only [18].

Section 7.2 and Section 7.3. The material of these two sections is from [3] and [19]. The paper [3] proves that Coxeter groups are automatic. This implies the above results but actually means more, such as the existence, for each generator $s \in S$, of a finite state automaton that, when given two words $\underline{a}$ and $\underline{b}$ in a regular language for W as described in the text, will recognize whether $\delta(\underline{b})$ is the product of s and $\delta(\underline{a})$.

The theory of automatic groups is best explained in [7].

The conjugacy for Coxeter groups has also been solved; see [23]. However, it is still an open question whether all Coxeter groups are bi-automatic in the sense of [7].

8. Tits systems

The finite Chevalley groups, that is, the groups of Theorem 1.7.1(iii), (iv), have in common that they all have a pair of subgroups with similar characteristics; together with a little additional data, this is called a Tits system. Now that we know more about Coxeter groups, we can make their significance for these Chevalley groups clearer by means of Tits systems. The main result in this direction is Theorem 8.1.2, which illustrates how Coxeter systems emerge from Tits systems.

In the second and last section of this chapter, we look at geometry in Coxeter groups and in groups possessing a Tits system. We construct edge-colored graphs on which the Coxeter groups act by automorphisms. These graphs, called buildings, are of great significance for geometric characterizations of Coxeter groups and Chevalley groups. We do not give these characterizations for Chevalley groups, but restrict ourselves to a very simple thin version for Coxeter groups. This is Theorem 8.2.6.

8.1 Tits systems

The Chevalley groups appearing in Theorem 1.7.1(iii), (iv) have the following structure in common.

Definition 8.1.1 Let G be a group and let M be a Coxeter matrix. A *Tits system in* G is a quadruple (B, N, W, S) for which the following four conditions hold.

(i) B and N are subgroups of G generating the full group G.
(ii) $H = B \cap N$ is a normal subgroup of N with quotient group $W = N/H$.
(iii) S is a generating set of W satisfying the following relations for any $w \in W$, $r \in S$
$$BrBwB \subseteq BwB \cup BrwB.$$
(iv) For each $r \in S$, we have $rBr^{-1} \not\subseteq B$.

Observe that, if $w \in W$ has an expression $s_1 \cdots s_q$ with $s_1, \ldots, s_q \in S$, then $s_1 \cdots s_q H = H s_1 \cdots s_q$ is a well-defined coset of H in N, independent of

the minimal expression for w. As $H \subseteq B$, expressions like Br and $BrBwB$ determine well defined unions of cosets of B in G.

To show how strong the conditions of Definition 8.1.1 are, we present a few basic properties, the first of which establishes the connection with Coxeter groups. For $w \in W$, we denote by $l(w)$ the length of w with respect to S; cf. Definition 2.1.7.

Theorem 8.1.2 *Each Tits system (B, N, W, S) in a group G satisfies the following properties for each $r \in S$, $w \in W$, and $J, K, L \subseteq S$.*

(i) *The pair (W, S) is a Coxeter system.*
(ii) *$l(rw) > l(w)$ if and only if $BrBwB = BrwB$.*
(iii) *$BW_JBW_KB = BW_JW_KB$.*
(iv) *$G_J = BW_JB$ is a subgroup of G. Moreover, $G_S = G$ and $G_\emptyset = B$.*
(v) *If $w_1, w_2 \in W$ satisfy $w_1 \neq w_2$, then $Bw_1B \neq Bw_2B$.*
(vi) *$G_J \cap (G_KG_L) = (G_J \cap G_K)(G_J \cap G_L) = G_{J\cap K}G_{J\cap L}$.*

Proof. We first show that S consists of involutions in W. Let $r \in S$. Applying Definition 8.1.1(iii) with $w = r^{-1}$ yields $BrBr^{-1}B \subseteq Br^{-1}B \cup B$. So $BrBr^{-1}B$ is the union of one or two double cosets with respect to B. In view of Definition 8.1.1(iv) and $B \subseteq BrBr^{-1}B$, this implies

$$BrBr^{-1}B = Br^{-1}B \cup B. \tag{8.1}$$

Inverting the sets at both sides of the equation, we find $BrBr^{-1}B = BrB \cup B$, which, again by use of Definition 8.1.1(iv), together with (8.1) leads to

$$BrB = Br^{-1}B. \tag{8.2}$$

Applying Definition 8.1.1(iii) with $w = r$ shows $BrBrB \subseteq BrB \cup Br^2B$. On the other hand, (8.1) and (8.2) give

$$BrBrB = BrBr^{-1}B = BrB \cup B. \tag{8.3}$$

Therefore, $B = Br^2B$, i.e., $r^2H \subseteq B$. Since $r^2H \subseteq N$, by definition, we derive from Definition 8.1.1(ii) that $r^2H = H$, so $r^2 = 1 \in W$. As $r = 1$ would contradict Definition 8.1.1(iv), it follows that r is an involution of W. Taking inverses in Definition 8.1.1(iii)) we find

$$wBr \subseteq BwB \cup BwrB \text{ for all } r \in S \text{ and } w \in W. \tag{8.4}$$

(iii). Obviously, $BW_JBW_KB \supseteq BW_JW_KB$. We next show $BW_JBW_JW_KB \subseteq BW_JW_KB$. To this end, we let $g \in BW_JBW_JW_KB$. Then there are $r_1, \ldots, r_q \in J$ such that $g \in Br_1 \cdots r_qBW_JW_KB$. If $q = 0$, then $g \in BW_JW_KB$ and there is nothing to prove. Otherwise, we have

$$\begin{aligned} Br_1 \cdots r_q BW_J W_K B &\subseteq Br_1 \cdots r_{q-1} Br_q BW_J W_K B \\ &\subseteq Br_1 \cdots r_{q-1} BW_J W_K B \end{aligned}$$

by Definition 8.1.1(iii), whence $g \in Br_1 \cdots r_{q-1} BW_J W_K B$. By induction on q, it follows that $BW_J BW_J W_K B \subseteq BW_J W_K B$. But then $BW_J BW_K B \subseteq BW_J BW_J W_K B \subseteq BW_J W_K B$, and (iii) is proved.

(iv). Now G_J is clearly non-empty and closed under taking inverses. From what we have just seen, G_J is also closed under multiplication, so it is a subgroup. Finally, due to Definition 8.1.1(i), $G_\emptyset = B1B = B$, and $G_S = BSB = BNB = \langle B, N\rangle = G$, whence (iv).

(v). Suppose w_1, $w_2 \in W$ with $w_1 \neq w_2$. Without harming generality, we may assume $l(w_1) \leq l(w_2)$. If $l(w_2) = 0$, then $Bw_1B = Bw_2B$ would imply $w_1H \subseteq B \cap N = H$, whence $w_1H = H = w_2H$, a contradiction. Thus $Bw_1B \neq Bw_2B$ and we are done. Let $l(w_2) \leq 1$. Then there is an involution $r \in S$ such that $l(rw_2) < l(w_2)$. By induction on $l(w_2)$ we have $Brw_2B \neq Bw_1B, Brw_1B$, so $Brw_2B \cap BrBw_1B = \emptyset$. Now $Bw_1B = Bw_2B$ would imply $Brw_2B \cap BrBw_2B = \emptyset$, which is absurd as Brw_2B is contained in this intersection. Hence $Bw_1B \neq Bw_2B$, establishing (v).

(i) and (ii). For $r \in S$, set $C_r = \{w \in W \mid BrBwB = BrwB\}$. We first prove two claims on these C_r.

$$C_r \cap rC_r = \emptyset. \tag{8.5}$$

Suppose $w \in C_r$. Then $BrBrwB = BrBrBwB = BwB \cup BrwB$, so $rw \notin C_r$, leading to $w \notin rC_r$, and settling (8.5).

$$\text{If } \ w \in C_r \text{ and } \ s \in S \text{ with } \ ws \notin C_r, \text{ then } \ rw = ws. \tag{8.6}$$

For,

$$\begin{aligned} BwB &\subseteq BwsBsB \\ &\subseteq BrBwsBsB \quad (\text{as } ws \notin C_r) \\ &\subseteq BrBwBsBsB = BrwBsBsB \quad (\text{as } w \in C_r) \\ &= BrwB \cup BrwBsB \quad (\text{by (8.3)}) \\ &= BrwB \cup BrwsB \quad (\text{by (8.4)}) \end{aligned}$$

so $w \in \{rw, rws\}$ by (v). But $w = rw$ conflicts $r \neq 1$, so $w = rws$. This yields $rw = ws$ as required.

Now we verify the Exchange Condition (cf. Definition 4.2.1) and at the same time establish that $w \in C_r$ is equivalent to $l(rw) > l(w)$. Let $w \in W$. Suppose $w \notin C_r$. Let $r_1 \cdots r_q \in \mathrm{M}(S)$ be a minimal expression of w as a product of elements from S. Write $w_j = r_1 \cdots r_j$ for $j = 0, 1, \ldots, q$. Since $w_0 = 1 \in C_r$ and $w_q = w \notin C_r$, there is an element $j \in \{0, 1, \ldots, q-1\}$ such that $w_j \in C_r$ and $w_j r_{j+1} = w_{j+1} \notin C_r$. Applying (8.6), we obtain $rw_j = w_j r_{j+1} = w_{j+1}$.

This means $rr_1 \cdots r_{j-1} = r_1 \cdots r_j$, and implies $l(rw) < l(w)$. Next, suppose $w \in C_r$. Then by (8.5), $rw \notin C_r$, so by what we have just seen $l(w) = l(r(rw)) < l(rw)$. Consequently, $w \in C_r$ if and only if $l(rw) < l(w)$, and the Exchange Condition holds. By Theorem 4.2.2, this ends the proof of (i) and (ii).

(vi). Recall $W_J \cap W_K W_L = (W_J \cap W_K)(W_J \cap W_L)$ from Proposition 4.2.8(ii). Hence,

$$\begin{aligned} G_J \cap (G_K G_L) &= (BW_JB) \cap (BW_KBW_LB) \\ &= BW_JB \cap BW_KW_LB \quad \text{(by (iii))} \\ &= B(W_J \cap W_KW_L)B \quad \text{(by (v))} \\ &= B(W_J \cap W_K)(W_J \cap W_L)B \quad \text{(by (i))} \\ &= B(W_J \cap W_K)BB(W_J \cap W_L)B \quad \text{(by (iii))} \\ &= ((BW_JB) \cap (BW_KB))((BW_JB) \cap (BW_LB)) \quad \text{(by (iv))} \\ &= (G_J \cap G_K)(G_J \cap G_L). \end{aligned}$$

But also

$$\begin{aligned} G_J \cap G_K &= BW_JB \cap BW_KB \\ &= B(W_J \cap W_K)B \quad \text{(by (iv))} \\ &= BW_{J\cap K}B \quad \text{(by Corollary 4.2.6(iii))} \\ &= G_{J\cap K} \end{aligned}$$

and similarly $G_J \cap G_L = G_{J\cap L}$. This ends the proof of (vi) and hence the theorem. □

In view of Theorem 8.1.2(i), the pair (W, S) is a Coxeter system and so has a Coxeter type M.

Definition 8.1.3 If (B, N, W, S) is a Tits system in a group G, then its *Coxeter type* and *rank* are the Coxeter type and rank of the Coxeter system (W, S).

Example 8.1.4 Let G be a group with a Tits system (B, N, W, S) of rank 1. Then $|S| = 1$ and $W \cong W(\mathrm{A}_1)$ is the cyclic group of order 2. Write $S = \{r\}$. By Theorem 8.1.2, $G = B \cup BrB$, so G acts doubly transitively on G/B by left multiplication. The subgroup B of G is the stabilizer of the point B in this permutation representation and r corresponds to an element of G having an orbit of length 2 on B.

Conversely, suppose G acts doubly transitively on a set X of size at least 3. Take two distinct points $x, y \in X$ and set $B = G_x$. Choose an element $n \in G$ moving the pair (x, y) to the pair (y, x) of elements from X. Then $G = B \cup BnB$ and $n^2 \in B$. Define N as the subgroup of G generated by n

and set $H = B \cap N$. Now G, being generated by B and n, is also generated by B and N, so (i) of Definition 8.1.1 is satisfied. As H has index 2 in N, it is a normal subgroup of N. We also find that N/H is a cyclic group of order 2, with generator $s = nH$. We have verified (ii) of Definition 8.1.1. Condition (iii) of Definition 8.1.1 needs to be checked only for $r = s$ and $w \in \{1, s\}$. It is trivial for $w = 1$ and follows from $G = BsB \cup Bs^2B$ in case $w = s$. Now, as X has size at least 3, there is an element $b \in B$ mapping y to an element $z \neq y$. Then $nbn^{-1}x = nby = nz \neq ny = x$, showing that $nbn^{-1} \in sBs^{-1} \backslash B$. Hence (iv) of Definition 8.1.1.

The conclusion is that a Tits system of rank 1 is equivalent to a doubly transitive permutation group on a set of size at least 3.

Definition 8.1.5 A Tits system is called *split* if there is a normal subgroup U of B such that B is the semidirect product of U and H.

Example 8.1.6 In $\mathrm{SL}(2, \mathbb{F})$ consider the elements

$$u_\lambda = \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}, \quad n = \begin{pmatrix} 0 & \zeta \\ -\zeta^{-1} & 0 \end{pmatrix}, \quad h_\zeta = \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix}.$$

Put $U = \{u_\lambda \mid \lambda \in \mathbb{F}\}$, $H = \{h_\zeta \mid \zeta \in \mathbb{F}^*\}$, $B = UH$ and $N = H \cup nH$. Then B is the subgroup of $\mathrm{SL}(2, \mathbb{F})$ of all upper triangular matrices, U is the normal subgroup of B consisting of all upper triangular matrices with ones on the main diagonal and B is the semidirect product of U and H. Moreover, every element of $\mathrm{SL}(2, \mathbb{F})$ can be written in the form $u_\lambda h_\zeta$ or $u_\lambda n_1 h_\zeta u_\mu$ for certain $\lambda, \mu \in \mathbb{F}$ and $\zeta \in \mathbb{F} \backslash \{0\}$, so $\mathrm{SL}(2, \mathbb{F}) = B \cup Un_1B = B \cup BsB$, where $s = n_1H$. Also, H has index 2 in N, and so $W = N/H$ is cyclic, with generator s. As B is the stabilizer of the projective point corresponding to the first standard basis vector, the $\mathrm{SL}(2, \mathbb{F})$-set $\mathrm{SL}(2, \mathbb{F})/B$ coincides with the projective line over $\mathbb{F}$ and so has cardinality $|\mathbb{F}| + 1$, at least three. The $\mathrm{SL}(2, \mathbb{F})$-action on $\mathrm{SL}(2, \mathbb{F})/B$ is doubly transitive, as follows from the fact that $\mathrm{SL}(2, \mathbb{F})$ has exactly two double cosets with respect to B. (It is the action on the projective line over $\mathbb{F}$.) Therefore, $(B, N, W, \{s\})$ is a split Tits system of rank 1.

By expanding H to all invertible diagonal matrices of size 2, we can extend the above to a Tits system for $\mathrm{GL}(2, \mathbb{F})$.

Example 8.1.7 The group $G = \mathrm{GL}(n + 1, \mathbb{F})$ has a split Tits system (B, N, W, S) with B the subgroup of upper triangular matrices, N the group of monomial matrices (that is, with a single nonzero entry in each row and in each column). Then $H = B \cap N$ is the group of diagonal matrices of $\mathrm{GL}(n+1, \mathbb{F})$. It is normal in N with quotient group $W = N/H \cong \mathrm{Sym}_{n+1} = W(\mathrm{A}_n)$. For π a permutation on $n+1$ letters, denote by M_π the permutation matrix of size $n + 1$ corresponding to π, so $M_\pi e_j = e_{\pi j}$, where $e_1, \ldots, e_{n+1}$

is the standard basis of $\mathbb{F}^{n+1}$. Then $S = \{M_{(i,i+1)}H \mid i \in [n]\}$ is the set of fundamental reflections of W, viewed as a Coxeter group of type A_n. Then (B, N, W, S) is a Tits system in G. The subgroup U of all upper triangular matrices with ones on the diagonal is normal in B and $B = U \rtimes H$, so the Tits system is split.

For $i \in [n]$, the set $G_{\{i\}} = B \cup BM_{(i,i+1)}B$ is a subgroup of G, of the form $U_i \rtimes (\mathrm{SL}(2, \mathbb{F}) \cdot H)$, where U_i is the subgroup of U of all upper triangular matrices with ones on the diagonal whose $(i, i+1)$-entry is zero. This can be seen by use of Example 8.1.6 and helps to prove that (B, N, W, S) is a Tits system (proving this is Exercise 8.3.2).

Identify, as usual, $[n]$ with S via $i \mapsto M_{(i,i+1)}H$ and let $\varepsilon_1, \ldots, \varepsilon_{n+1}$ be the standard basis of $\mathbb{R}^{n+1}$. For $J \subseteq S$, the subgroup G_J of G consists of all matrices of size $n+1$ whose entries (i, j) are zero whenever $i > j$ and $\varepsilon_j - \varepsilon_i \notin \sum_{k \in J} \mathbb{R}_{\geq 0}(\varepsilon_k - \varepsilon_{k+1})$. In geometric terms, $G_{S \setminus \{j\}}$ is the stabilizer in G of the linear subspace $\langle e_i \mid i \leq j \rangle$ of $\mathbb{F}^{n+1}$.

Most of the Tits systems encountered in Chevalley groups are split.

Theorem 8.1.8 (Tits systems of Chevalley groups) *Each finite simple Chevalley group has a Tits system as indicated in Table 8.1.*

Table 8.1. Types M of Tits systems in the Chevalley groups of Theorem 1.7.1.

group	condition	M
$\mathrm{SL}(n, q)$	$n \geq 3$ and $(n, q) \neq (2, 2), (2, 3)$	A_{n-1}
$\mathrm{O}(2n+1, q)$	$n \geq 2$	B_n
$\mathrm{Sp}(2n, q)$	$n \geq 3$	C_n
$\mathrm{O}^+(2n, q)$	$n \geq 4$	D_n
$\mathrm{E}_n(q)$	$n = 6, 7, 8$	E_n
$\mathrm{F}_4(q)$		F_4
$\mathrm{G}_2(q)$		G_2
${}^2\mathrm{A}_{n-1}(q) = \mathrm{U}(n, q)$	$n \geq 4$	$\mathrm{B}_{\lfloor n/2 \rfloor}$
${}^2\mathrm{B}_2(2^{2m+1})$	$m \geq 1$	A_1
${}^2\mathrm{D}_n(q) = \mathrm{O}^-(2n, q)$	$n \geq 4$	B_{n-1}
${}^3\mathrm{D}_4(q)$		G_2
${}^2\mathrm{E}_6(q)$		F_4
${}^2\mathrm{F}_4(2^{2m+1})$	$m \geq 0$	$\mathrm{I}_2^{(8)}$
${}^2\mathrm{G}_2(3^{2m+1})$	$m \geq 1$	A_1

8.2 A combinatorial characterization of Coxeter groups

A Tits system in a group G gives rise to a geometry on which G acts as a group of automorphisms. This geometry is called a building and will be

presented here as an edge-colored graph. Let (W, S) be a Coxeter system. Observe that the quadruple $(\{1\}, W, W, S)$ satisfies the first three conditions of a Tits system, but not the fourth. This phenomenon will recur in the guise of thin buildings below, as opposed to the thick buildings coming from Tits systems. According to Exercise 8.3.4, these thin buildings appear abundantly in those thick buildings.

In Corollary 3.3.6, we have seen that the subgroups of W of the form W_J for $J \subseteq S$ are Coxeter groups themselves. Here we study the permutation representation of W on the collection of cosets W/W_J. In fact, we construct edge-colored graphs on W/W_J on which W acts as a group of automorphisms. We pay most attention to the case where $J = \emptyset$, in which case the graphs are called buildings.

Definition 8.2.1 For $J \subseteq S$, the *Coxeter graph* of (W, S) on J is the edge-colored graph Γ whose vertex set is W/W_J, whose color set is $S\backslash J$ and in which two distinct cosets gW_J and hW_J, for $g, h \in W$, are r-adjacent (for $r \in S\backslash J$) if and only if $g^{-1}h \in W_J r W_J$, notation $gW_J \sim_r hW_J$. If $J = \emptyset$, then Γ is also called the *chamber system* of (W, S).

Since $W_J r W_J = W_J r^{-1} W_J$, the relations $\sim_r$ are symmetric, so Γ is an undirected graph.

Lemma 8.2.2 *The action of the group W by left multiplication on the Coxeter graph Γ preserves each of the relations $\sim_r$. In particular, W acts on Γ as a group of automorphisms.*

Proof. Let $w \in W$. If $gW_J \sim_r hW_J$, then $g^{-1}h \in W_J r W_J$, so $(wg)^{-1}(wh) \in W_J r W_J$, proving $wgW_J \sim_r whW_J$. Hence left multiplication by w is an automorphism of Γ. □

Example 8.2.3 Let (W, S) be of type A_{n-1}, so $W \cong \mathrm{Sym}_n$. Take $k \in [n-1]$ and set $J = [n-1]\backslash\{k\}$. Then there is just one color, k, and so Γ is an ordinary graph. Now $W_J = W_{[k-1]} \times W_{\{k+1,\ldots,n-1\}}$, so $|W_J| = k! \cdot (n-k)!$ and $|W/W_J| = \binom{n}{k}$. This suggest a correspondence between Γ and the collection of k-subsets of $[n]$.

Denote by ∂ the graph-theoretic distance function $W \times W \to \mathbb{N}$ on the chamber system Γ of (W, S). Thus, $\partial(x, y) = l(y^{-1}x)$ for $x, y \in W$. For $J \subseteq S$, write $\sim_J$ to denote $\bigcup_{j \in J} \sim_j$. A connected component of $\sim_J$ in Γ is called a *J-cell*. The J-cell containing x is the subset xW_J of W. The chamber system Γ has the following combinatorial properties.

Proposition 8.2.4 *Let (W, S) be a Coxeter system of type M and denote by Γ its chamber system. Then the following statements hold.*

(i) *Γ is connected.*
(ii) *For $i, j \in S$ with $i \neq j$, the graph structure induced on each $\{i, j\}$-cell by the relations i and j is a $2m_{ij}$-gon.*
(iii) *For each J-cell of Γ and each $x, w \in W$, there is a unique chamber y in the J-cell D containing x such that, for each $z \in D$, we have $\partial(w, z) = \partial(w, y) + \partial_J(y, z)$, where ∂_J represents the distance between x and y measured in the graph on D with adjacencies coming solely from J.*

Proof. (i). The S-cell containing 1 is $W_S = W$. This proves that Γ is connected.

(ii). The $\{i, j\}$-cell containing x is $xW_{\{i,j\}}$. Each vertex is on precisely one edge of each color from $\{i, j\}$, and paths of length $2m_{ij}$ with alternating colors along the edges are closed. Hence the graph with edges from the colors i and j is a single cycle of length $2m_{ij}$.

(iii). For $u \in D = xW_J$ and w as stated, we have $\partial(w, u) = l(w^{-1}u)$. Take $y' \in W^J \cap w^{-1}xW_J$ (see Definition 2.2.2) and write $y = wy'$. If $z \in xW_J$, then $z = yv$ for some $v \in W_J$ with $l(z) = l(y) + l(v)$, so, by Corollary 4.2.6 and Lemma 2.2.3, $\partial(z, y) + \partial_J(y, w) = l(v) + l_J(y') = l(y'v) = l(w^{-1}z) = \partial(z, w)$ as required. □

Definition 8.2.5 Let C be a set and S a collection of distinct equivalence relations on C. If M is a Coxeter diagram whose nodes are indexed by S, then (C, S) is called a *thin chamber system of type M* if properties (i) and (ii) of Proposition 8.2.4 are satisfied and each equivalence class has size two. Here, for $J \subseteq S$, the *J-cell* of an element c of C is the connected component of the graph containing c whose adjacencies are the relations in J; the chamber system is called *connected* if there is a single S-cell in C. The members of C are called *chambers*.

If C is a thin chamber system of type M, then it is called a *building* if (iii) of Proposition 8.2.4 (the *gate property*) holds, where ∂ is the graph-theoretic distance in Γ (with adjacency $x \sim y$ if and only if x and y are distinct and x and y are s-equivalent for some $s \in S$).

Proposition 8.2.4 has the following converse.

Theorem 8.2.6 *Let M be a finite Coxeter diagram and Γ be a thin building of type M. Then Γ is the chamber system of a Coxeter system of type M.*

Proof. Write n for the size of M and put $S = [n]$. Denote by C the set of chambers of Γ.

As Γ is thin, for each $i \in [n]$ and chamber $c \in C$, there is a unique chamber, denoted ci, in C, that is i-adjacent to c and distinct from c. So there are permutations p_i of C (for $i \in [n]$) such that $p_i(c) = ci$. Observe

that the subgroup $\langle p_1, \ldots, p_n \rangle$ of $\mathrm{Sym}(C)$ is a quotient of the Coxeter group of type M. This follows easily because the p_i satisfy the defining relations: $p_i^2(c) = (ci)i = c$ for every chamber c, and the braid relations $p_i p_j p_i \cdots = p_j p_i p_j \cdots$ are satisfied due to the condition that the $\{i,j\}$-cells are $2m_{ij}$-gons. As a consequence, the map $S \to \{p_i \mid i \in [n]\}$ given by $s_i \mapsto p_i$ extends to a homomorphism $\phi : W(M) \to \mathrm{Sym}(C)$. Note that, for $w \in W = W(M)$, the element $ew = \phi(w^{-1})e$ is well defined and can be computed as $p_{s_q} p_{s_{q-1}} \cdots p_{s_1} e$ for any expression $s_1 s_2 \cdots s_q$ of w. If $w \in W$ and $d, e \in C$ are such that $\phi(w)e = d$, then w corresponds to a path from e to d of length $l(w)$.

We show that the homomorphism ϕ is injective. In fact, we even show that the W-action on C is regular, that is, for each $c \in C$ and $w \in W$ we only have $\phi(w)c = c$ if $w = 1$.

Suppose not. Then there is an element $w \in W$ of length $q > 0$ and a chamber $e \in C$ with $\phi(w)e = e$. Let q be minimal with this property. Take a minimal expression $s_1 \cdots s_q \in \mathrm{M}(S)$ for w. Consider the closed path e, $e_1 = \phi(s_1)e = es_1$, $e_2 = e_1 s_2$, $\ldots$, $e_q = e_{q-1}s_q = e$ in Γ. Thus, $e_j \sim_{s_j} e_{j-1}$ for each $j \in [q]$, where $e_q = e_0 = e$.

Clearly, $q > 1$. If $q = 2h + 1$, then $\{e_h, e_{h+1}\}$ is an $\{s_{h+1}\}$-cell and the paths $e, e_1, \ldots, e_h$ and $e = e_q, e_{q-1} \ldots, e_{h+1}$ have both length h, so, by the gate property, one of the two chambers e_h and e_{h+1}, say e_h, has distance less than h to e in Γ. Suppose this distance is realized by $v \in W$ of length $l(v) < h$, so $e_h = \phi(v)e$ with $v \in W$ of length less than h. By the minimal choice of q, we then have $s_1 \cdots s_h v = 1 \in W$, so $v^{-1} s_{h+1} \cdots s_q$ is of length less than q and corresponds to a closed path in Γ starting at e. Again by the minimal choice of q, we derive $v^{-1} s_{h+1} \cdots s_q = 1$, so $w = (s_1 \cdots s_h)(s_{h+1} \cdots s_q) = v^{-1} v = 1$, a contradiction.

Suppose, therefore $q = 2h$. Then the $\{s_{h+1}, s_h\}$-cell D containing e_h also contains e_{h-1} and e_{h+1}. Both these chambers have a path of length $h - 1$ to e. By the gate property there is a chamber d in D of distance less than $h - 1$ to e. First of all, by the gate property applied to d, all distances within D along the $\{i,j\}$-adjacencies, are the distances within Γ. For, d itself must be the unique member f of D such that $\partial(d, y) = \partial(d, f) + \partial_{\{i,j\}}(f, y)$ for all $y \in D$ (take $y = d$ to see this).

Now the closed path starting at e, along the original closed path to e_{h-1}, next to d in D and then back to e along a path of minimal length has length smaller than q and so the corresponding element of w represents the identity in W. Also the closed path starting at e, along the original closed path to e_{h+1}, then to d in D, and finally back to e along a path of minimal length, has length smaller than q and so represents the identity in W. As a consequence, the closed path from e_{h-1} to e_{h+1} via e_h and then back to e_{h-1} via d is in D and can be chosen fully with $\{i,j\}$-adjacencies. As $d \neq e_h$ (in view of distinct distances to e), the chamber d must be the opposite of e_h inside D, so the paths of minimal length from d to e_h via e_{h-1} and via e_{h+1} represent the

same (longest) element of $W_\{i,j\}$. But now the closed path we started with is a product of three paths corresponding to the trivial element of W and so must correspond to the trivial element of W itself, the final contradiction. □

Now that we have seen that a thin building of type M comes from the regular representation of a Coxeter system of type M, we focus on similar structures in a thick setting. This means that the equivalence classes have size at least three.

Definition 8.2.7 Let C be a set and S a collection of distinct equivalence relations on C. For $s \in S$, we will say that x and y are s-adjacent, and write $x \sim_s y$, if they are s-equivalent and not equal.

As before, for $J \subseteq S$, the *J-cell* of an element c of C is the connected component of the graph containing c in which adjacency is the union of all $\sim_j$ for $j \in J$; the chamber system is called *connected* if there is a single S-cell in C. The members of C are called *chambers*.

If $|S| = 2$, and $m \in \mathbb{N}$, $m \geq 2$, then (C, S) is called a *generalized m-gon* if the following two properties are satisfied.

(i) The graph on C with adjacencies $\sim_S$ is bipartite and connected.
(ii) For each $g < 2m$ there are no $2g$-gons in C.
(iii) The diameter of C is precisely m.

If M is a Coxeter diagram whose nodes are indexed by S, then (C, S) is called a *chamber system* of type M if the following three properties are satisfied

(i) C is connected.
(ii) For each pair $i, j \in S$, the $\sim_{\{i,j\}}$-graph on each $\{i, j\}$ cell in C is a *generalized m_{ij}-gon*.
(iii) For each J-cell of Γ and each $x, w \in C$, there is a unique y in the J-cell D containing x such that, for each z in D, we have $\partial(z, w) = \partial(z, y) + \partial_J(y, x)$, where ∂_J represents the distance between x and y measured in the graph on D with adjacencies coming solely from J.

Finally, (C, S) is called thick, if, for each $s \in S$, each $\{s\}$-cell has size at least three.

Example 8.2.8 Consider a projective plane with lines of size at least 3 and at least 3 lines per point. Let C be the set of all pairs consisting of a point and a line incident to the point in that plane. Define the equivalence relation p by letting c and d be p-equivalent if and only if c and d have the same point and the equivalence relation l by letting c and d be l-adjacent if and only if c and d have the same line. Then $(C, \{p, l\})$ is a thick generalized 3-gon.

Lemma 8.2.9 *Let (B, N, W, S) be a Tits system in G. Then $s_1 \cdots s_q \in \mathrm{M}(S)$ is a minimal expression of $w \in W$ if and only if $BwB = Bs_1Bs_2B \cdots Bs_qB$.*

Proof. If $s_1 \cdots s_q \in \mathrm{M}(S)$ is a minimal expression of $w \in W$, then, by induction on q and application of Theorem 8.1.2(ii), we find $BwB = Bs_1Bs_2B \cdots Bs_qB$.

Conversely, suppose $w \in W$ and $s_1, \ldots, s_q \in S$ satisfy

$$BwB = Bs_1Bs_2B \cdots Bs_qB.$$

By Theorem 8.1.2(v), $w = s_1 \cdots s_q$, so it remains to verify $q = l(w)$. If $q = 0$, there is nothing to show, so we proceed by induction on q. Let $q > 0$ and choose $j \in [q]$ minimal such that $s_j s_{j+1} \cdots s_q \in \mathrm{M}(S)$ is a minimal expression. Assume $j > 1$. Now, by Theorem 8.1.2(ii),

$$\begin{aligned} BwB &= Bs_1Bs_2B \cdots Bs_qB \\ &= Bs_1B \cdots Bs_{j-1}Bs_j \cdots s_qB \\ &= Bs_1B \cdots Bs_{j-2}Bs_{j-1}s_j \cdots s_qB \cup Bs_1B \cdots Bs_{j-2}Bs_j \cdots s_qB \\ &\supseteq BwB \cup Bs_1 \cdots s_{j-2}s_j \cdots s_qB \supseteq Bs_1 \cdots s_{j-2}s_j \cdots s_qB, \end{aligned}$$

so, by Theorem 8.1.2(v), $w = s_1 \cdots s_{j-1}s_j \cdots s_q$, a contradiction with the parity of $l(w)$. Hence $j = 1$ and $s_1 \cdots s_q$ is a minimal expression of w, as required. □

Definition 8.2.10 Let G be a group with a Tits system (B, N, W, S) of type M. Let Γ be the pair consisting of the set G/B and the equivalence relations s for $s \in S$ according to which gB and hB are s-equivalent if and only if $g^{-1}h \in G_{\{s\}}$. Then Γ is called the *chamber system of* the Tits system (B, N, W, S).

Lemma 8.2.11 *Let (B, N, W, S) be a Tits system in a group G of rank 2. Then the corresponding chamber system is a thick generalized m_{ij}-gon.*

Proof. This is direct from Lemma 8.2.9. □

Proposition 8.2.12 *Let (B, N, W, S) be a Tits system of type M in a group G. Then the corresponding chamber system Γ is a thick building and G acts on Γ as a group of automorphisms.*

Proof. The proof runs along the same lines of argument as Proposition 8.2.4.

(i). In view of Definition 8.1.1(iii), the S-cell containing B consists of all cosets of B in $\bigcup_{w \in W} BwB$ for $w \in W$. By Theorem 8.1.2(iv), this union coincides with G. Therefore, every chamber is connected to B.

(ii). The $\{i, j\}$-cell containing gB is set of all B-cosets in $gG_{\{i,j\}}$. The result now follows easily from Lemma 8.2.9.

(iii). By Lemmas 8.2.9 and 2.2.3. □

The thick building obtained as in Proposition 8.2.12 has many thin buildings of the same Coxeter type as substructures; see Exercise 8.3.4. In particular, the study of the mutual positions of any two chambers in the thick building can be reduced to a study in the thin building underlying the corresponding Coxeter group.

8.3 Exercises

Section 8.1

Exercise 8.3.1 For $n \geq 4$, the alternating group Alt_n is doubly transitive on $[n]$. For which n does this permutation representation give rise to a Tits sytem of rank 1? For which n does it give rise to a split Tits system?

Exercise 8.3.2 (Cited in Example 8.1.7) Show that (B, N, W, S) of Example 8.1.7 is a Tits system.

Section 8.2

Exercise 8.3.3 Note that the permutations p_i ($i \in [n]$) of the proof of Theorem 8.2.6 are not automorphisms of the chamber system Γ. Nevertheless Γ has a group of automorphisms isomorphic to W. Find this group and prove that it is indeed a Coxeter group.

Exercise 8.3.4 Let (B, N, W, S) be a Tits system of type M in a group G. Show that the set $A = NB/B$, together with the relations on A induced from S, is a thin building of type M. Conclude, by use of translations by elements of G, that each pair of chambers of the building of the Tits system lies in a copy gA of A for some $g \in G$.

Exercise 8.3.5 Consider the permutations $a = (1,2)(3,4)$, $b = (1,2)(4,5)$, and $c = (1,3)(2,4)$ in $G = \mathrm{Alt}_5$.

(a) Prove that there is a surjective homomorphism of groups $W(\mathrm{H}_3) \to \mathrm{Alt}_5$ determined by $s_1 \mapsto a$, $s_2 \mapsto b$, and $s_3 \mapsto c$, where $S = \{s_1, s_2, s_3\}$ is the fundamental generating set of $W(\mathrm{H}_3)$.

(b) For $s \in S$, let s-adjacency $\sim_s$ on Alt_5 be given by $u \sim_s v$ if and only if $u = vs$. Prove that the edge-colored graph on Alt_5 arising in this way is a thin chamber system of type H_3 that does not satisfy the gate property.

8.4 Notes

Section 8.1. The theory of Tits systems is developed in [38]. See [41, 32, 5] for excellent introductions to the theory and the geometric highlights. A self-contained classification of split Tits systems of spherical type and rank at least 2 as well as a classification of arbitrary Tits systems of spherical type and rank at least 3 is given in [39].

Section 8.2. The classification of thick buildings of spherical type is dealt with in [38]. A consequence of the result is that they all come from groups with a Tits system if the rank is at least 3. Many but not all come from algebraic groups. The exceptions are due to slight deviations from the algebraic groups case. For instance, the groups $\mathrm{GL}(n, \mathbb{D})$, for $\mathbb{D}$ a noncommutative division ring, have a Tits system but are not algebraic. A very thorough treatment will appear in a new book by Weiss on buildings on affine type, one of the many topics not dealt with in these notes.

As for rank 2, for $m = 3, 4$ wild examples of finite thick buildings of type $\mathrm{I}_2^{(m)}$ are known, but for $m = 6, 8$ none other than the examples coming from finite Chevalley groups are known. These are the only values of m greater than 2 for which finite thick buildings of type $\mathrm{I}_2^{(m)}$ exist. See [28, 4, 40] for more details.

References

1. G. Baumslag. *Topics in Combinatorial Group Theory (Lectures in Mathematics. ETH Zrich)*, Birkäuser, 1993
2. N. Bourbaki. *Groupes et algèbres de Lie, Chap 4, 5, et 6.* Hermann, Paris 1968
3. B. Brink and R.B. Howlett. *A finiteness property and an automatic structure for Coxeter groups.* Math. Ann. **296** (1993) 179–190
4. A.E. Brouwer, A.M. Cohen, A. Neumaier. *Distance-regular Graphs.* Springer-Verlag, Berlin 1989 Ergebnisse der Math. u.i. Grenzgeb. 3. Folge Band 18
5. K.S. Brown. *Buildings.* Springer-Verlag, New York 1989
6. F. Buekenhout and A.M. Cohen *Diagram Geometry*, in preparation, `http://www.win.tue.nl/~amc/buek`
7. J.W. Cannon, D.B.A. Epstein, D.B. Holt, S.V.F. Levy, M.S. Paterson, W.P. Thurston. *Word processing in groups.* Word processing in groups. Jones and Bartlett Publishers, Boston, MA, 1992
8. A.M. Cohen, H. Cuypers, H. Sterk (eds). *Some Tapas of Computer Algebra.* Springer-Verlag, Heidelberg, 1999
9. J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker, R.A. Wilson. *Atlas of finite groups.* Oxford University Press, Eynsham, UK, 1985 `http://brauer.maths.qmul.ac.uk/Atlas/v3/`
10. H.S.M. Coxeter. *Finite groups generated by reflections and their subgroups generated by reflections.* Proc. Cambridge Phil. Soc. **30** (1934) 466–282
11. H.S.M. Coxeter. *The complete enumeration of finite groups of the form* $R^2 = (R_iR_j)^{k_{ij}} = 1$. J. London Math. SOc. **10** (1935) 21–25
12. H.S.M. Coxeter. *Regular polytopes - Dover 1948* (3rd edition).1973
13. V.V. Deodhar. *On the root system of a Coxeter group.* Comm. Algebra **10**1982 611–630
14. V.V. Deodhar. *Some characterizations of Coxeter groups.* l'Enseignement Mathématique **32**1986 111–120
15. M. Dyer. *Reflection subgroups of Coxeter systems.* J. Algebra **135** (1990) 57–73
16. E. Formanek & C. Procesi. The automorphism group of a free group is not linear. J. Algebra **149** (1992) 494–499
17. D. Gorenstein, R. Lyons, and R. Solomon. *The classification of the finite simple groups.* Mathematical Surveys and Monographs **40**, American Mathematical Society, Providence, RI, 1994
18. J.E. Hopcroft and J.D. Ullman. *Introduction to automata theory, languages, and computation.* Addison-Wesley 1979
19. R.B. Howlett. *Miscellaneous facts about Coxeter groups.* Report 93-38, School of Mathematics and Statistics, The University of Sydney, 1993
20. J.E. Humphreys. *Finite reflection groups and Coxeter groups.* Cambridge studies in advanced mathematics **29** Cambridge University Press 1990
21. D.L. Johnson, *Presentations of groups*, Cambridge University Press, Cambridge 1997

22. D. Knuth and P. Bendix. *Simple word problems in universal algebras.* Computational Problems in Abstract Algebra (Ed. J. Leech) (1970) 263–297
23. D. Krammer. *The conjugacy problem for Coxeter groups.* PhD. Thesis, Utrecht, 1994
24. S.A. Linton. *On vector enumeration.* Linear Algebra Appl. **192** (1993) 235–248
25. H. Matsumoto. *Générateurs et relations des groupes de Weyl généralisés.* C.R. Acad. Sci. Paris. **258** (1964) 3419–3422
26. B. Mühlherr. *Coxeter groups in Coxeter groups.* pp. 277–287 in Finite Geometry and Combinatorics (Deinze 1992). London Math. Soc. Lecture Note Series **191**, Cambridge University Press, Cambridge, 1993
27. B. Mühlherr. *On isomorphisms between Coxeter groups.* Designs, Codes, Cryptography. **21** (2000) 189
28. S. Payne & J. Thas. *Finite generalized quadrangles.* Pitman, New York 1985
29. P. Papi. *A characterization of a special ordering in a root system.* Proc. Amer. Math. Soc. **120** (1994) 661–665
30. D. Passman. *Permutation groups.* W. A. Benjamin, Inc., New York-Amsterdam, 1968
31. F.C. Piper & A. Wagner. *Faithful orbits of collineation groups.* Math. Z. **107** (1968) 212–220
32. M. Ronan. *Lectures on Buildings.* Acad. Press, Boston 1989
33. J-P. Serre. *A Course in Arithmetic.* Springer Verlag, Berlin, 1996
34. T.A. Springer. *Linear algebraic groups, second edition.* Birkhäuser, Basel 1991
35. I. Satake. *Classification theory of semisimple algebraic groups.* Lecture Notes in Pure and Appl. Math., Marcel Dekker, New York 1971
36. R. Stanley. *On the number of reduced dxecompositions of elements of Coxeter groups.* European J. Combinatorics **5** (1984) 359–327
37. J. Tits. *Le problème des mots dans les groupes de Coxeter*, Sympos. Math. Rome 1967/1968, Acad. Press, London **1** (1969) 175–185
38. J. Tits. *Buildings of spherical type and finite BN-pairs.* Lecture Notes in Math. 386. Springer-Verlag, Berlin, 1974
39. J. Tits & R. Weiss. *Moufang polygons.* Springer 2002
40. H. Van Maldeghem. *Generalized polygons.* Monographs in Mathematics, vol. 93, Birkhäuser, Basel 1998
41. R.M. Weiss. *The structure of spherical buildings.* Princeton University Press 2003
42. E.W. Weisstein. *Klein quartic.* MathWorld-A Wolfram Web Resource. `http://mathworld.wolfram.com/KleinQuartic.html`
43. H. Wielandt. *Finite permutation groups.* Academic Press, New York, 1964

Glossary

abelian: A group G is abelian if $gh = hg$ for all $g, h \in G$.

absolutely irreducible: A representation of a group G on a vector space V over a field $\mathbb{F}$ is called *absolutely irreducible* if the representation of G induced on $V \otimes \overline{\mathbb{F}}$, where $\overline{\mathbb{F}}$ is the algebraic closure of $\mathbb{F}$, is irreducible.

algebra: An algebra over a field $\mathbb{F}$ is a vector space A over $\mathbb{F}$ together with an associative bilinear map $A \times A \to A;\ (a, b) \mapsto a \cdot b$, referred to as the multiplication on A, such that, for all $a, b \in A$ and $\lambda \in \mathbb{F}$,

$$\lambda(ab) = (\lambda a) \cdot b = a \cdot (\lambda b).$$

Cayley graph: Let G be a group, and let S be a subset of the group elements not containing the identity element. The Cayley graph corresponding to the pair (G, S) is the directed graph whose vertices are the elements of G. Two vertices $g, h \in G$ are connected by an edge (g, h) whenever $gh^{-1} \in S$.

centralizer: Let S be a subset of a group G, then the subgroup $C_G(S) = \{g \in G \mid gsg^{-1} = s \text{ for all } s \in S\}$ of G is the centralizer of S in G.

center: Let G be a group. The center of G is formed by the elements $g \in G$ which satisfy $ghg^{-1} = h$ for all $h \in G$.

conjugate: A subset X of a group G is conjugate to another subset Y if there is $g \in G$ such that $gXg^{-1} = Y$.

coset: A coset of a subgroup H of a group G is a subset of the form gH for some $g \in G$, which is defined as $\{gh \mid h \in H\}$. Often, this is also called a left coset. Less frequently, it is called a right coset, a notion we preserve for sets of the form Hg.

discrete: A subset of $\mathbb{R}^n$, supplied with the standard inner product, is discrete in $\mathbb{R}^n$ if there is a real positive number μ such that any two elements of the subset are at Euclidean distance at least μ.

double coset: A double coset corresponding to two subgroups H and K of a group G is a subset of the form HgK for some $g \in G$, which is defined as $\{hgk \mid h \in H \wedge k \in K\}$.

doubly transitive: The group action of a group G on a set X is called doubly transitive, if for every four points $x_1, x_2, y_1, y_2 \in X$, there is a group element $g \in G$ such that $gx_i = y_i$ for $i = 1, 2$.

embedding: An embedding of a group G in a group H is an injective group homomorphism from G to H.

Euclidean distance: Given two vectors $v, w \in \mathbb{R}^n$, supplied with the standard inner product, the Euclidean distance between them is $\sqrt{(v-w, v-w)}$.

Euclidean length: Given a vector $v \in \mathbb{R}^n$, supplied with the standard inner product, its Euclidean length is $\sqrt{(v, v)}$, that is the Euclidean distance between v and 0.

First Isomorphism Theorem: If $\phi : G \to H$ is a homomorphism of groups, then $\operatorname{Im}\phi$ is a group isomorphic to $G/\operatorname{Ker}\phi$ and $\phi = \overline{\phi} \circ \pi$, where $\pi : G \to G/\operatorname{Ker}\phi$ is the natural quotient map and $\overline{\phi}$ is a uniquely determined homomorphism $G/\operatorname{Ker}\phi \to H$.

free module: A module is called free if it has a spanning set of linearly independent elements. So, if M is a module over R, then M is free (over R) if there exists a subset B of M such that $M = \sum_{b \in B} Rb$ and if λ_b for $b \in B$ are elements of R satisfying $\sum_{b \in B} \lambda_b b = 0$, then $\lambda_b = 0$ for all $b \in B$.

index: The index of a subgroup H in a group G is the cardinality of G/H, the set of cosets of H in G.

involution: A group element of order 2.

Klein Four group: The group $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$. In other words, the only non-cyclic group of order four.

linear: A group G is linear if it is isomorphic to a subgroup of $\mathrm{GL}(V)$ for some finite-dimensional vector space V. If so, and the underlying field of the vector space is the reals, then we say that G is linear over the reals.

monoid: A set M supplied with a distinguished element 1 and a binary map $M \times M \to M$, referred to a multiplication, is called a monoid if the binary map is associative and both left and right multiplication by 1 is the identity on M. In formulas, with $(a, b) \mapsto a \cdot b$ denoting the map, for all $a, b, c \in M$,

$$(a \cdot b) \cdot c = a \cdot (b \cdot c)$$
$$1 \cdot b = b \cdot 1 = b$$

monomial: A matrix is called monomial if each row and each column contains exactly one nonzero entry.

norm: The norm of a vector in $\mathbb{R}^n$, supplied with the standard inner product, is its Euclidean length.

normal: A subgroup H of a group G is normal if $gHg^{-1} = H$ for all $g \in G$. Here gHg^{-1} stands for the subset $\{ghg^{-1} \mid h \in H\}$ of G, which is a subgroup of G, conjugate to H.

normalizer: Let S be a subset of a group G, then the subgroup $N_G(S) = \{g \in G \mid gSg^{-1} = S\}$ of G is the normalizer of S in G.

quotient group: Let N be a normal subgroup of a group G. Then the quotient group of G by N is denoted G/N. It is the set of all left cosets of N in G, that is, $G/N = \{gN \mid g \in G\}$. For each gN and hN in G/N, the product of gN and hN is $(gN)(hN) = ghN$.

simple: A group is simple if its only normal subgroups are the group itself and the trivial group.