

---

## The alternating groups

### 2.1 Introduction

The most familiar of the (finite non-abelian) simple groups are the alternating groups  $A_n$ , which are subgroups of index 2 in the symmetric groups  $S_n$ . In this chapter our main aims are to define these groups, prove they are simple, determine their outer automorphism groups, describe in general terms their subgroups, and construct their covering groups. At the end of the chapter we briefly introduce reflection groups as a generalisation of the symmetric groups, as they play an important role not only in the theory of groups of Lie type, but also in the construction of many sporadic groups, as well as in the elucidation of much exceptional behaviour of low-dimensional classical groups.

By way of introduction we bring in the basic concepts of permutation group theory, such as  $k$ -transitivity and primitivity, before presenting one of the standard proofs of simplicity of  $A_n$  for  $n \geq 5$ . Then we prove that  $\text{Aut}(A_n) \cong S_n$  for  $n \geq 7$ , while for  $n = 6$  there is an exceptional outer automorphism of  $S_6$ . The subgroup structure of  $A_n$  and  $S_n$  is described by the O’Nan–Scott Theorem, which we state and prove after giving a detailed description of the subgroups which arise in that theorem.

Next we move on to the covering groups, and construct the Schur double covers  $2 \cdot A_n$  for all  $n \geq 4$ . We also construct the exceptional triple covers  $3 \cdot A_6$  and  $3 \cdot A_7$  (and hence  $6 \cdot A_6$  and  $6 \cdot A_7$ ), but make no attempt to prove the fact that there are no other covers. Finally, we define and prove the Coxeter presentation for  $S_n$  on the fundamental transpositions  $(i, i+1)$ , as an introduction to reflection groups in general. We state Coxeter’s classification theorem for real reflection groups, and the crystallographic restriction, for future use.

### 2.2 Permutations

We first define the *symmetric group*  $\text{Sym}(\Omega)$  on a set  $\Omega$  as the group of all permutations of that set. Here a *permutation* is simply a bijection from the

set to itself. If  $\Omega$  has cardinality  $n$ , then we might as well take  $\Omega = \{1, \dots, n\}$ . The resulting symmetric group is denoted  $S_n$ , and called *the* symmetric group of degree  $n$ .

Since a permutation  $\pi$  of  $\Omega$  is determined by the images  $\pi(1)$  ( $n$  choices),  $\pi(2)$  ( $n-1$  choices, as it must be distinct from  $\pi(1)$ ),  $\pi(3)$  ( $n-2$  choices), and so on, we see that the number of permutations is  $n(n-1)(n-2)\dots 2 \cdot 1 = n!$  and therefore  $|S_n| = n!$ .

A permutation  $\pi$  may conveniently be written simply as a list of the images  $\pi(1), \dots, \pi(n)$  of the points in order, or more explicitly, as a list of the points  $1, \dots, n$  with their images  $\pi(1), \dots, \pi(n)$  written underneath them. For example,  $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 2 & 3 & 4 \end{pmatrix}$  denotes the permutation fixing 1, and mapping 2 to 5, 3 to 2, 4 to 3, and 5 to 4. If we draw lines between equal numbers in the two rows, the lines cross over each other, and the crossings indicate which pairs of numbers have to be interchanged in order to produce this permutation. In this example, the line joining the 5s crosses the 4s, 3s and 2s in that order, indicating that we may obtain this permutation by first swapping 5 and 4, then 5 and 3, and finally 5 and 2. A single interchange of two elements is called a *transposition*, so we have seen how to write any permutation as a product of transpositions. Of course, for any given permutation there are many ways of doing this.

### 2.2.1 The alternating groups

An alternative interpretation of this picture is to read it from bottom to top, and record the *positions* of the strings that are swapped. In this example, we first swap the second and third strings, then the third and fourth, and finally the fourth and fifth. Thus the second string moves to the fifth position, the third string moves to the second position, and so on. In this way we have written our permutation as a product of swaps of *adjacent* strings. Moreover, the product of two permutations can be expressed by concatenating any two corresponding lists of swapping strings.

But if we write the identity permutation as a product of such transpositions, and the line connecting the *is* crosses over the line connecting the *js*, then they must cross back again: thus the number of crossings for the identity element is even. It follows that if  $\pi$  is written in two different ways as a product of such transpositions, then either the number of transpositions is even in both cases, or it is odd in both cases. Therefore the map  $\phi$  from  $S_n$  onto the group  $\{\pm 1\}$  of order 2 defined by  $\phi(\pi) = 1$  whenever  $\pi$  is the product of an even number of transpositions, is a (well-defined) group homomorphism. As  $\phi$  is onto, its kernel is a normal subgroup of index 2, which we call the *alternating* group of degree  $n$ . It has order  $\frac{1}{2}n!$ , and its elements are called the *even* permutations. The other elements of  $S_n$  are the *odd* permutations. (An alternative proof that  $A_n$  has index 2 in  $S_n$  can be found in Exercise 2.1.)

The notation for permutations as functions on the left (where  $\pi\rho$  means  $\rho$  followed by  $\pi$ ) is unfortunately inconsistent with the normal convention for permutations that  $\pi\rho$  means  $\pi$  followed by  $\rho$ . Therefore we adopt a different notation, writing  $a^\pi$  instead of  $\pi(a)$ , to avoid this confusion. We then have  $a^{\pi\rho} = \rho(\pi(a))$ , and permutations are read from left to right, rather than right to left as for functions.

### 2.2.2 Transitivity

Given a group  $H$  of permutations, i.e. a subgroup of a symmetric group  $S_n$ , we are interested in which points can be mapped to which other points by elements of the group  $H$ . If every point can be mapped to every other point, we say  $H$  is *transitive* on the set  $\Omega$ . In symbols, this is expressed by saying that for all  $a$  and  $b$  in  $\Omega$ , there exists  $\pi \in H$  with  $a^\pi = b$ . In any case, the set  $\{a^\pi \mid \pi \in H\}$  of points reachable from  $a$  is called the *orbit* of  $H$  containing  $a$ . It is easy to see that the orbits of  $H$  form a partition of the set  $\Omega$ .

More generally, if we can simultaneously map  $k$  points wherever we like, the group is called *k-transitive*. This means that (for  $k \leq n$ ) for every list of  $k$  distinct points  $a_1, \dots, a_k$  and every list of  $k$  distinct points  $b_1, \dots, b_k$  there exists an element  $\pi \in H$  with  $a_i^\pi = b_i$  for all  $i$ . In particular, 1-transitive is the same as transitive.

For example, it is easy to see that the symmetric group  $S_n$  is *k-transitive* for all  $k \leq n$ , and that the alternating group  $A_n$  is *k-transitive* for all  $k \leq n-2$ .

It is obvious that if  $H \neq 1$  is *k-transitive* then  $H$  is  $(k-1)$ -transitive, and is therefore *m-transitive* for all  $m \leq k$ . There is however a concept intermediate between 1-transitivity and 2-transitivity which is of interest in its own right. This is the concept of *primitivity*, which is best explained by defining what it is not.

### 2.2.3 Primitivity

A *block system* for a subgroup  $H$  of  $S_n$  is a partition of  $\Omega$  preserved by  $H$ ; that is, a set of mutually disjoint non-empty subsets of  $\Omega$  whose union is  $\Omega$ . We call the elements of the partition *blocks*. In other words, if two points  $a$  and  $b$  are in the same block of the partition, then for all elements  $\pi \in H$ , the points  $a^\pi$  and  $b^\pi$  are also in the same block as each other. There are two block systems which are always preserved by every group: one is the partition consisting of the single block  $\Omega$ ; at the other extreme is the partition in which every block consists of a single point. These are called the *trivial* block systems. A non-trivial block system is often called a *system of imprimitivity* for the group  $H$ . If  $n \geq 3$  then any group which has a system of imprimitivity is called *imprimitive*, and any non-trivial group which is not imprimitive is called *primitive*. (It is usual also to say that  $S_2$  is primitive, but that  $S_1$  is neither primitive nor imprimitive.)

It is obvious that

$$\text{if } H \text{ is primitive, then } H \text{ is transitive.} \quad (2.1)$$

For, if  $H \neq 1$  is not transitive, then the orbits of  $H$  form a system of imprimitivity for  $H$ , so  $H$  is not primitive. On the other hand, there exist plenty of transitive groups which are not primitive. For example, in  $S_4$ , the subgroup  $H$  of order 4 generated by  $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$  and  $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$  is transitive, but preserves the block system  $\{\{1, 2\}, \{3, 4\}\}$ . It also preserves the block systems  $\{\{1, 3\}, \{2, 4\}\}$  and  $\{\{1, 4\}, \{2, 3\}\}$ . Of course, in any block system for a transitive imprimitive group, all the blocks have the same size.

Another important basic result about primitive groups is that

$$\text{every 2-transitive group is primitive.} \quad (2.2)$$

For, if  $H$  is imprimitive, we can choose three distinct points  $a$ ,  $b$  and  $c$  such that  $a$  and  $b$  are in the same block, while  $c$  is in a different block. (This is possible since the blocks have at least two points, and there are at least two blocks.) Then there can be no element of  $H$  taking the pair  $(a, b)$  to the pair  $(a, c)$ , so it is not 2-transitive.

## 2.2.4 Group actions

Suppose that  $G$  is a subgroup of  $S_n$  acting transitively on  $\Omega$ . Let  $H$  be the stabiliser of the point  $a \in \Omega$ , that is,  $H = \{g \in G \mid a^g = a\}$ . Then the points of  $\Omega$  are in natural bijection with the (right) cosets  $Hg$  of  $H$  in  $G$ . This bijection is given by  $Hx \leftrightarrow a^x$ . It is left as an exercise for the reader (see Exercise 2.2) to prove that this is a bijection. In particular,  $|G : H| = n$ .

We can turn this construction around, so that given any subgroup  $H$  in  $G$ , we can let  $G$  act on the right cosets of  $H$  according to the rule  $(Hx)^g = Hxg$ . Numbering the cosets of  $H$  from 1 to  $n$ , where  $n = |G : H|$ , we obtain a permutation action of  $G$  on these  $n$  points, or in other words a group homomorphism from  $G$  to  $S_n$ . If this homomorphism is injective, we say  $G$  acts *faithfully*.

## 2.2.5 Maximal subgroups

This correspondence between transitive group actions on the one hand, and subgroups on the other, permits many useful translations between combinatorial properties of  $\Omega$  and group-theoretical properties of  $G$ . For example, a primitive group action corresponds to a maximal subgroup, where a subgroup  $H$  of  $G$  is called *maximal* if there is no subgroup  $K$  with  $H < K < G$ . More precisely:

**Proposition 2.1.** *Suppose that the group  $G$  acts transitively on the set  $\Omega$ , and let  $H$  be the stabiliser of  $a \in \Omega$ . Then  $G$  acts primitively on  $\Omega$  if and only if  $H$  is a maximal subgroup of  $G$ .*

*Proof.* We prove both directions of this in the contrapositive form. First assume that  $H$  is not maximal, and choose a subgroup  $K$  with  $H < K < G$ . Then the points of  $\Omega$  are in bijection with the (right) cosets of  $H$  in  $G$ . Now the cosets of  $K$  in  $G$  are unions of  $H$ -cosets, so correspond to sets of points, each set containing  $|K : H|$  points. But the action of  $G$  preserves the set of  $K$ -cosets, so the corresponding sets of points form a system of imprimitivity for  $G$  on  $\Omega$ .

Conversely, suppose that  $G$  acts imprimitively, and let  $\Omega_1$  be the block containing  $a$  in a system of imprimitivity. Since  $G$  is transitive, it follows that the stabiliser of  $\Omega_1$  acts transitively on  $\Omega_1$ , but not on  $\Omega$ . Therefore this stabiliser strictly contains  $H$  and is a proper subgroup of  $G$ , so  $H$  is not maximal.

### 2.2.6 Wreath products

The concept of imprimitivity leads naturally to the idea of a *wreath product* of two permutation groups. Recall the *direct product*

$$G \times H = \{(g, h) \mid g \in G, h \in H\} \quad (2.3)$$

with identity element  $1_{G \times H} = (1_G, 1_H)$  and group operations

$$\begin{aligned} (g_1, h_1)(g_2, h_2) &= (g_1 g_2, h_1 h_2), \\ (g, h)^{-1} &= (g^{-1}, h^{-1}). \end{aligned} \quad (2.4)$$

Recall also the *semidirect product*  $G:H$  or  $G:\phi H$ , where  $\phi : H \rightarrow \text{Aut}(G)$  describes an action of  $H$  on  $G$ . We define  $G:H = \{(g, h) \mid g \in G, h \in H\}$  with identity element  $1_{G:H} = (1_G, 1_H)$  and group operations

$$\begin{aligned} (g_1, h_1)(g_2, h_2) &= (g_1 g_2^{\phi(h_1^{-1})}, h_1 h_2), \\ (g, h)^{-1} &= ((g^{-1})^{\phi(h)}, h^{-1}). \end{aligned} \quad (2.5)$$

Now suppose that  $H$  is a permutation group acting on  $\Omega = \{1, \dots, n\}$ . Define  $G^n = G \times G \times \dots \times G = \{(g_1, \dots, g_n) \mid g_i \in G\}$ , the direct product of  $n$  copies of  $G$ , and let  $H$  act on  $G^n$  by permuting the  $n$  subscripts. That is  $\phi : H \rightarrow \text{Aut}(G^n)$  is defined by

$$\phi(\pi^{-1}) : (g_1, \dots, g_n) \mapsto (g_{1\pi}, \dots, g_{n\pi}). \quad (2.6)$$

Then the *wreath product*  $G \wr H$  is defined to be  $G^n : \phi H$ . For example, if  $H \cong S_n$  and  $G \cong S_m$  then the wreath product  $S_m \wr S_n$  can be formed by taking  $n$  copies of  $S_m$ , each acting on one of the sets  $\Omega_1, \dots, \Omega_n$  of size  $m$ , and then permuting the subscripts  $1, \dots, n$  by elements of  $H$ . This gives an imprimitive action of  $S_m \wr S_n$  on  $\Omega = \bigcup_{i=1}^n \Omega_i$ , preserving the partition of  $\Omega$  into the  $\Omega_i$ . More generally, any (transitive) imprimitive group can be embedded in a wreath product: if the blocks of a system of imprimitivity for  $G$  are  $\Omega_1, \dots, \Omega_k$ , then clearly all the  $\Omega_i$  have the same size, and  $G$  is a subgroup of  $\text{Sym}(\Omega_1) \wr S_k$ .

## 2.3 Simplicity

### 2.3.1 Cycle types

An alternative notation for a permutation  $\pi$  is obtained by considering the *cycles* of  $\pi$ . These are defined by taking an element  $a \in \Omega$ , which maps under  $\pi$  to  $a^\pi$ : this in turn maps to  $a^{\pi^2}$ , which maps to  $a^{\pi^3}$  and so on. Because  $\Omega$  is finite, eventually we get a repetition  $a^{\pi^j} = a^{\pi^k}$  and therefore  $a^{\pi^{j-k}} = a$ . Thus the first time we get a repetition is when we get back to the start of the cycle, which can now be written  $(a, a^\pi, a^{\pi^2}, \dots, a^{\pi^{k-1}})$ , where  $k$  is the *length* of the cycle. Repeating this with a new element  $b$  not in this cycle, we get another cycle of  $\pi$ , disjoint from the first. Eventually, we run out of elements of  $\Omega$ , at which point  $\pi$  is written as a product of disjoint cycles.

The *cycle type* of a permutation is simply a list of the lengths of the cycles, usually abbreviated in some way. Thus the identity has cycle type  $(1^n)$  and a transposition has cycle type  $(2, 1^{n-2})$ . Note, incidentally, that a cycle of *even* length is an *odd* permutation, and vice versa. Thus a permutation is even if and only if it has an even number of cycles of even length.

If  $\rho \in S_n$  is another permutation, then  $\pi^\rho = \rho^{-1}\pi\rho$  maps  $a^\rho$  via  $a$  and  $a^\pi$  to  $a^{\pi\rho}$ . Therefore each cycle  $(a, a^\pi, a^{\pi^2}, \dots, a^{\pi^{k-1}})$  of  $\pi$  gives rise to a corresponding cycle  $(a^\rho, a^{\pi\rho}, a^{\pi^2\rho}, \dots, a^{\pi^{k-1}\rho})$  of  $\pi^\rho$ . So the cycle type of  $\pi^\rho$  is the same as the cycle type of  $\pi$ . Conversely, if  $\pi$  and  $\pi'$  are two permutations with the same cycle type, we can match up the cycles of the same length, say  $(a, a^\pi, a^{\pi^2}, \dots, a^{\pi^{k-1}})$  with  $(b, b^{\pi'}, b^{\pi'^2}, \dots, b^{\pi'^{k-1}})$ . Now define a permutation  $\rho$  by mapping  $a^{\pi^j}$  to  $b^{\pi'^j}$  for each integer  $j$ , and similarly for all the other cycles, so that  $\pi' = \pi^\rho$ . Thus two permutations are conjugate in  $S_n$  if and only if they have the same cycle type.

By performing the same operation to conjugate a permutation  $\pi$  to itself, we find the centraliser of  $\pi$ . Specifically, if  $\pi$  is an element of  $S_n$  of cycle type  $(c_1^{k_1}, c_2^{k_2}, \dots, c_r^{k_r})$ , then the centraliser of  $\pi$  in  $S_n$  is a direct product of  $r$  groups  $C_{c_i} \wr S_{k_i}$  (see Exercise 2.25).

### 2.3.2 Conjugacy classes in the alternating groups

Next we determine the conjugacy classes in  $A_n$ . The crucial point is to determine which elements of  $A_n$  are centralised by odd permutations. Given an element  $g$  of  $A_n$ , and an odd permutation  $\rho$ , either  $g^\rho$  is conjugate to  $g$  by an element  $\pi$  of  $A_n$  or it is not. In the former case,  $g$  is centralised by the odd permutation  $\rho\pi^{-1}$ , while in the latter case, every odd permutation maps  $g$  into the same  $A_n$ -conjugacy class as  $g^\rho$ , and so no odd permutation centralises  $g$ .

If  $g$  has a cycle of even length, it is centralised by that cycle, which is an odd permutation. Similarly, if  $g$  has two cycles of the same odd length (possibly of length 1!), it is centralised by an element  $\rho$  which interchanges the two cycles: but then  $\rho$  is the product of an odd number of transpositions, so is an odd permutation.

On the other hand, if  $g$  does not contain an even cycle or two odd cycles of the same length, then it is the product of disjoint cycles of distinct odd lengths, and every element  $\rho$  centralising  $g$  must map each of these cycles to itself. The first point in each cycle can be mapped to an arbitrary point in that cycle, but then the images of the remaining points are determined. Thus we obtain all such elements  $\rho$  as products of powers of the cycles of  $g$ . In particular  $\rho$  is an even permutation.

This proves that  $g$  is centralised by no odd permutation if and only if  $g$  is a product of disjoint cycles of distinct odd lengths. It follows immediately that the conjugacy classes of  $A_n$  correspond to cycle types if there is a cycle of even length or there are two cycles of equal length, whereas a cycle type consisting of distinct odd lengths corresponds to two conjugacy classes in  $A_n$ .

For example, in  $A_5$ , the cycle types of even permutations are  $(1^5)$ ,  $(3, 1^2)$ ,  $(2^2, 1)$ , and  $(5)$ . Of these, only  $(5)$  consists of disjoint cycles of distinct odd lengths. Therefore there are just five conjugacy classes in  $A_5$ .

### 2.3.3 The alternating groups are simple

It is easy to see that a subgroup  $H$  of  $G$  is normal if it is a union of whole conjugacy classes in  $G$ . The group  $G$  is *simple* if it has precisely two normal subgroups, namely 1 and  $G$ . Every non-abelian simple group  $G$  is *perfect*, i.e.  $G' = G$ .

The numbers of elements in the five conjugacy classes in  $A_5$  are 1, 20, 15, 12 and 12 respectively. Since no proper sub-sum of these numbers including 1 divides 60, there can be no subgroup which is a union of conjugacy classes, and therefore  $A_5$  is a simple group.

We now prove by induction that  $A_n$  is simple for all  $n \geq 5$ . The induction starts when  $n = 5$ , so we may assume  $n > 5$ . Suppose that  $N$  is a non-trivial normal subgroup of  $A_n$ , and consider  $N \cap A_{n-1}$ , where  $A_{n-1}$  is the stabiliser in  $A_n$  of the point  $n$ . This is normal in  $A_{n-1}$ , so by induction is either 1 or  $A_{n-1}$ . In the second case,  $N \geq A_{n-1}$ , so contains all the elements of cycle type  $(3, 1^{n-3})$  and  $(2^2, 1^{n-4})$  (since it is normal). But it is easily seen that every even permutation is a product of such elements, so  $N = A_n$ . Therefore we can assume that  $N \cap A_{n-1} = 1$ , which means that every non-identity element of  $N$  is fixed-point-free (i.e. fixes no points). Thus  $|N| \leq n$ , for if  $x, y \in N$  map the point 1 to the same point then  $xy^{-1}$  fixes 1 so is trivial.

But  $N$  must contain a non-trivial conjugacy class of elements of  $A_n$ , and it is not hard to show that if  $n \geq 5$  then there is no such class with fewer than  $n$  elements. We leave this verification as an exercise (Exercise 2.10). This contradiction proves that  $N$  does not exist, and so  $A_n$  is simple. (An alternative proof of simplicity of  $A_n$  is given in Exercise 3.4.)

## 2.4 Outer automorphisms

### 2.4.1 Automorphisms of alternating groups

If  $n \geq 4$  then  $A_n$  has trivial centre, so that  $A_n \cong \text{Inn}(A_n) \leq \text{Aut}(A_n)$ . Moreover, each element of  $S_n$  induces an automorphism of  $A_n$ , by conjugation in  $S_n$ , so  $S_n$  is (isomorphic to) a subgroup of  $\text{Aut}(A_n)$ . It turns out that for  $n \geq 7$  it is actually the whole of  $\text{Aut}(A_n)$ . We prove this next. (I am grateful to Chris Parker for supplying this argument.)

First we observe that, since  $(a, b, c)(a, b, d) = (a, d)(b, c)$ , the group  $A_n$  is generated by its 3-cycles. Indeed, it is generated by the 3-cycles  $(1, 2, 3)$ ,  $(1, 2, 4)$ ,  $\dots$ ,  $(1, 2, n)$ . Also note that for  $n \geq 5$ ,  $A_n$  has no subgroup of index  $k$  less than  $n$ —for if it did there would be a homomorphism from  $A_n$  onto a transitive subgroup of  $A_k$ , contradicting the fact that  $A_n$  is simple. We next prove:

**Lemma 2.2.** *If  $n \geq 7$  and  $A_{n-1} \cong H \leq A_n$ , then  $H$  is the stabiliser of one of the  $n$  points on which  $A_n$  acts.*

*Proof.* By the above remark,  $H$  cannot act on a non-trivial orbit of length less than  $n - 1$ , so if it is not a point stabiliser then it must act transitively on the  $n$  points. For  $n = 7$  this is impossible, as 7 does not divide the order of  $A_6$ . For  $n > 8$ , each element of  $H$  which corresponds to a 3-cycle of  $A_{n-1}$  centralises a subgroup isomorphic to  $A_{n-4}$ , with  $n - 4 \geq 5$ , so again by the above remark this subgroup must have an orbit of at least  $n - 4$  points. Therefore the ‘3-cycles’ of  $H$  can move at most four points, so must act as 3-cycles on the  $n$  points. The same is true for  $n = 8$ , as the 3-cycles centralise  $A_5$ , which contains  $C_2 \times C_2$ , whereas the elements of cycle type  $(3^2, 1^2)$  do not centralise  $C_2 \times C_2$  in  $A_8$ .

Now the elements of  $H$  corresponding to  $(1, 2, 3)$  and  $(1, 2, 4)$  in  $A_{n-1}$  generate a subgroup isomorphic to  $A_4$ , and therefore map to cycles  $(a, b, c)$  and  $(a, b, d)$  in  $A_n$ . Similarly, the elements corresponding to  $(1, 2, j)$  must all map to  $(a, b, x)$ . It follows that the images  $(a, b, x)$  of the  $n - 3$  generating elements of  $H$  together move exactly  $n - 1$  points. Therefore  $H$  is one of the point stabilisers isomorphic to  $A_{n-1}$ , as required.

Now we are ready to prove the theorem:

**Theorem 2.3.** *If  $n \geq 7$  then  $\text{Aut}(A_n) \cong S_n$ .*

*Proof.* Any automorphism of  $A_n$  permutes the subgroups, and in particular permutes the  $n$  subgroups isomorphic to  $A_{n-1}$ . But these subgroups are in natural one-to-one correspondence with the  $n$  points of  $\Omega$ , and therefore any automorphism acts as a permutation of  $\Omega$ , so is an element of  $S_n$ .

The theorem is also true for  $n = 5$  and for  $n = 4$  (see Exercise 2.16).



### 2.4.2 The outer automorphism of $S_6$

Of all the symmetric groups,  $S_6$  is perhaps the most remarkable. One manifestation of this is its exceptional outer automorphism. This is an isomorphism from  $S_6$  to itself which does not correspond to a permutation of the underlying set of six points. What this means is that there is a completely different way for  $S_6$  to act on six points.

To construct a non-inner automorphism  $\phi$  of  $S_6$  we first note that  $\phi$  must map the point stabiliser  $S_5$  to another subgroup  $H \cong S_5$ . However,  $H$  cannot fix any of the six points on which  $S_6$  acts, so  $H$  must be transitive on these six points.

Thus our first job is to construct a transitive action of  $S_5$  on six points. This may be obtained in a natural way as the action of  $S_5$  by conjugation on its six Sylow 5-subgroups. (If we wish to avoid using Sylow's theorems at this point we can simply observe that the 24 elements of order 5 belong to six cyclic subgroups  $\langle(1, 2, x, y, z)\rangle$ , and that these are permuted transitively by conjugation by elements of  $S_5$ .)

Going back to  $S_6$ , we have now constructed our transitive subgroup  $H$  of index 6. Thus  $S_6$  acts naturally (and transitively) on the six cosets  $Hg$  by right multiplication. More explicitly, we can define a group homomorphism  $\phi : S_6 \rightarrow \text{Sym}(\{Hg \mid g \in S_6\}) \cong S_6$ . The kernel of  $\phi$  is trivial, since  $S_6$  has no non-trivial normal subgroups of index 6 or more. Hence  $\phi$  is a group isomorphism, i.e. an automorphism of  $S_6$ .

But  $\phi$  is not an inner automorphism, because it maps the transitive subgroup  $H$  to the stabiliser of the trivial coset  $H$ , whereas inner automorphisms preserve transitivity. [A more sophisticated version of this construction is given in Section 3.3.5 in the discussion of  $\text{PSL}_2(5)$ . An alternative construction of the outer automorphism of  $S_6$  is given in Section 4.2.]

This is the only outer automorphism of  $S_6$ , in the sense that  $S_6$  has index 2 in its full automorphism group. Indeed, we can prove the stronger result that the outer automorphism group of  $A_6$  has order 4. For any automorphism maps the 3-cycles to elements of order 3, which are either 3-cycles or products of two disjoint 3-cycles. Therefore it suffices to show that any automorphism which maps 3-cycles to 3-cycles is in  $S_6$ . But this follows by the same argument as in Lemma 2.2 and Theorem 2.3 (see Exercise 2.18).

## 2.5 Subgroups of $S_n$

There are a number of more or less obvious subgroups of the symmetric groups. In order to simplify the discussion it is usual to (partly) classify the maximal subgroups first, and to study arbitrary subgroups by looking at them as subgroups of the maximal subgroups. In this section we describe some important classes of (often maximal) subgroups, and prove maximality in a few cases.

The converse problem, of showing that any maximal subgroup is in one of these classes, is addressed in Section 2.6.

The first two classes are the intransitive subgroups and the transitive imprimitive subgroups. The other four are types of maximal primitive subgroups of  $S_n$  which are ‘obvious’ to the experts, and are generally labelled the primitive wreath product, affine, diagonal, and almost simple types. We shall not prove that any of these are maximal, and indeed sometimes they are not.

### 2.5.1 Intransitive subgroups

If  $H$  is an intransitive subgroup of  $S_n$ , then it has two or more orbits on the underlying set of  $n$  points. If these orbits have lengths  $n_1, \dots, n_r$ , then  $H$  is a subgroup of the subgroup  $S_{n_1} \times \dots \times S_{n_r}$  consisting of all permutations which permute the points in each orbit, but do not mix up the orbits. If  $r > 2$ , then we can mix up all the orbits except the first one, to get a group  $S_{n_1} \times S_{n_2 + \dots + n_r}$  which lies between  $H$  and  $S_n$ . Therefore, in this case  $H$  cannot be maximal.

On the other hand, if  $r = 2$ , we have the subgroup  $H = S_k \times S_{n-k}$  of  $S_n$ , and it is quite easy to show this is a maximal subgroup, as long as  $k \neq n - k$ . For, we may as well assume  $k < n - k$ , and that the factor  $S_k$  acts on  $\Omega_1 = \{1, 2, \dots, k\}$ , while the factor  $S_{n-k}$  acts on  $\Omega_2 = \{k + 1, \dots, n\}$ . If  $g$  is any permutation not in  $H$ , let  $K$  be the subgroup generated by  $H$  and  $g$ . Our aim is to show that  $K$  contains all the transpositions of  $S_n$ , and therefore is  $S_n$ .

Now  $g$  must move some point in  $\Omega_2$  to a point in  $\Omega_1$ , but cannot do this to all points in  $\Omega_2$ , since  $|\Omega_2| > |\Omega_1|$ . Therefore we can choose  $i, j \in \Omega_2$  with  $i^g \in \Omega_1$  and  $j^g \in \Omega_2$ . Then  $(i, j) \in H$  so  $(i^g, j^g) \in H^g \leq K$ . Conjugating this transposition by elements of  $H$  we obtain all the transpositions of  $S_n$  (except those which are already in  $H$ ), and therefore  $K = S_n$ . This implies that  $H$  is a maximal subgroup of  $S_n$ . Note that we have now completely classified the intransitive maximal subgroups of  $S_n$ , so any other maximal subgroup must be transitive. For example, the intransitive maximal subgroups of  $S_6$  are  $S_5$  and  $S_4 \times S_2$ .

### 2.5.2 Transitive imprimitive subgroups

In the case when  $k = n - k$ , this proof breaks down, and in fact the subgroup  $S_k \times S_k$  is not maximal in  $S_{2k}$ . This is because there is an element  $h$  in  $S_{2k}$  which interchanges the two orbits of size  $k$ , and normalises the subgroup  $S_k \times S_k$ . For example we may take  $h = (1, k + 1)(2, k + 2) \dots (k, 2k)$ . Indeed, what we have here is the wreath product of  $S_k$  with  $S_2$ . This can be shown to be a maximal subgroup of  $S_{2k}$  by a similar method to that used above (see Exercise 2.27).

More generally, if we partition the set of  $n$  points into  $m$  subsets of the same size  $k$  (so that  $n = km$ ), then the wreath product  $S_k \wr S_m$  can act on this partition: the *base group*  $S_k \times \dots \times S_k$  consists of permutations of each of the

$m$  subsets separately, while the wreathing action of  $S_m$  acts by permuting the  $m$  orbits of the base group. It turns out that this subgroup is maximal in  $S_n$  also (see Exercise 2.28). Thus we obtain a list of all the transitive imprimitive maximal subgroups of  $S_n$ . These are the groups  $S_k \wr S_m$  where  $k > 1$ ,  $m > 1$  and  $n = km$ . For example, the transitive imprimitive maximal subgroups of  $S_6$  are  $S_2 \wr S_3$  (preserving a set of three blocks of size 2, for example generated by the three permutations  $(1, 2)$ ,  $(1, 3, 5)(2, 4, 6)$  and  $(3, 5)(4, 6)$ ) and  $S_3 \wr S_2$  (preserving a set of two blocks of size 3, for example generated by the three permutations  $(1, 2, 3)$ ,  $(1, 2)$  and  $(1, 4)(2, 5)(3, 6)$ ).

### 2.5.3 Primitive wreath products

We have completely classified the imprimitive maximal subgroups of  $S_n$ , so all the remaining maximal subgroups of  $S_n$  must be primitive. To see an example of a primitive subgroup of  $S_n$ , consider the case when  $n = k^2$ , and arrange the  $n$  points in a  $k \times k$  array. Let one copy of  $S_k$  act on this array by permuting the columns around, leaving each row fixed as a set. Then let another copy of  $S_k$  act by permuting the rows around, leaving each column fixed as a set. These two copies of  $S_k$  commute with each other, so generate a group  $H \cong S_k \times S_k$ . Now  $H$  is imprimitive, as the rows form one system of imprimitivity, and the columns form another. But if we adjoin the permutation which reflects in the main diagonal, so mapping rows to columns and vice versa, then we get a group  $S_k \wr S_2$  which turns out to be primitive. For example, there is a primitive subgroup  $S_3 \wr S_2$  in  $S_9$ , which however turns out not to be maximal. In fact the smallest case which is maximal is the subgroup  $S_5 \wr S_2$  in  $S_{25}$ .

Generalising this construction to an  $m$ -dimensional array in the case when  $n = k^m$ , with  $k > 2$  and  $m > 1$ , we obtain a primitive action of the group  $S_k \wr S_m$  on  $k^m$  points. To make this more explicit, we identify  $\Omega$  with the Cartesian product  $\Omega_1^m$  of  $m$  copies of a set  $\Omega_1$  of size  $k$ , and let an element  $(\pi_1, \dots, \pi_m)$  of the base group  $S_k^m$  act by

$$(a_1, \dots, a_m) \mapsto (a_1^{\pi_1}, \dots, a_m^{\pi_m}) \quad (2.7)$$

for all  $a_i \in \Omega_1$ . The wreathing action of  $\rho^{-1} \in S_m$  is then given by the natural action permuting the coordinates, thus:

$$\rho^{-1} : (a_1, \dots, a_m) \mapsto (a_{1\rho}, \dots, a_{m\rho}). \quad (2.8)$$

This action of the wreath product is sometimes called the *product action*, to distinguish it from the imprimitive action on  $km$  points described in Section 2.5.2 above. We shall not prove maximality of these subgroups in  $S_n$  or  $A_n$ , although they are in fact maximal in  $A_n$  if  $k \geq 5$  and  $k^{m-1}$  is divisible by 4, and maximal in  $S_n$  if  $k \geq 5$  and  $k^{m-1}$  is not divisible by 4.

### 2.5.4 Affine subgroups

The affine groups are essentially the symmetry groups of vector spaces. Let  $p$  be a prime, and let  $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$  denote the field of order  $p$  (for more on finite

fields see Section 3.2). Let  $V$  be the vector space of  $k$ -tuples of elements of  $\mathbb{F}_p$ . Then  $V$  has  $p^k$  elements, and has a symmetry group which is the semidirect product of the group of translations  $t_a : v \mapsto v + a$ , by the general linear group  $\mathrm{GL}_k(p)$  consisting of all invertible  $k \times k$  matrices over  $\mathbb{F}_p$ . This group, sometimes denoted  $\mathrm{AGL}_k(p)$ , and called the *affine general linear group*, acts as permutations of the vectors, so is a subgroup of  $S_n$  where  $n = p^k$ . The translations form a normal subgroup isomorphic to the additive group of the vector space, which is isomorphic to a direct product of  $k$  copies of the cyclic group  $C_p$ . In other words it is an *elementary abelian* group of order  $p^k$ , which we denote  $E_{p^k}$ , or simply  $p^k$ . With this notation,  $\mathrm{AGL}_k(p) \cong p^k : \mathrm{GL}_k(p)$ .

An example of an affine group is the group  $\mathrm{AGL}_3(2) \cong 2^3 : \mathrm{GL}_3(2)$ , which acts as a permutation group on the 8 vectors of  $\mathbb{F}_2^3$ , and so embeds in  $S_8$ . Indeed, it is easy to check that all its elements are even permutations, so it embeds in  $A_8$ . Another example is  $\mathrm{AGL}_1(7) \cong 7:6$  which is a maximal subgroup of  $S_7$ . Note however that its intersection with  $A_7$  is a group  $7:3$  which is *not* maximal in  $A_7$ . These groups  $7:6$  and  $7:3$  are examples of *Frobenius groups*, which are by definition transitive non-regular permutation groups in which the stabiliser of any two points is trivial. Other examples of Frobenius groups are the *dihedral* groups  $D_{2n} \cong n:2$  of symmetries of the regular  $n$ -gon.

### 2.5.5 Subgroups of diagonal type

The diagonal type groups are less easy to describe. They are built from a non-abelian simple group  $T$ , and have the shape

$$T^k . (\mathrm{Out}(T) \times S_k) \cong (T \wr S_k) . \mathrm{Out}(T). \quad (2.9)$$

Here there is a normal subgroup  $T \wr S_k$ , extended by a group of outer automorphisms which acts in the same way on all the  $k$  copies of  $T$ . This group contains a subgroup  $\mathrm{Aut}(T) \times S_k$  consisting of a diagonal copy of  $T$  (i.e. the subgroup of all elements  $(t, \dots, t)$  with  $t \in T$ ), extended by its outer automorphism group and the permutation group. This subgroup has index  $|T|^{k-1}$ , so the permutation action of the group on the cosets of this subgroup gives an embedding of the whole group in  $S_n$ , where  $n = |T|^{k-1}$ .

The smallest example of such a group is  $(A_5 \times A_5) : (C_2 \times C_2)$  acting on the cosets of a subgroup  $S_5 \times C_2$ . This group is the semidirect product of  $A_5 \times A_5 = \{(g, h) \mid g, h \in A_5\}$  by the group  $C_2 \times C_2$  of automorphisms generated by  $\alpha : (g, h) \mapsto (g^\pi, h^\pi)$ , where  $\pi$  is the transposition  $(1, 2)$ , and  $\beta : (g, h) \mapsto (h, g)$ . The point stabiliser is the centraliser of  $\beta$ , generated by  $\alpha$ ,  $\beta$  and  $\{(g, g) \mid g \in A_5\}$ . Therefore an alternative way to describe the action of the group on 60 points is as the action by conjugation on the 60 conjugates of  $\beta$ .

### 2.5.6 Almost simple groups

Finally, there are the almost simple primitive groups. A group  $G$  is called *almost simple* if it satisfies  $T \leq G \leq \mathrm{Aut}(T)$  for some simple group  $T$ . Thus

it consists of a simple group, possibly extended by adjoining some or all of the outer automorphism group. If  $M$  is any maximal subgroup of  $G$ , then the permutation action of  $G$  on the cosets of  $M$  is primitive, so  $G$  embeds as a primitive subgroup of  $S_n$ , where  $n = |G : M|$ . The class of almost simple maximal subgroups of  $S_n$  is chaotic in general, and to describe them completely would require complete knowledge of the maximal subgroups of all almost simple groups—a classic case of reducing an impossible problem to an even harder one!

However, a result of Liebeck, Praeger and Saxl [120] states that (subject to certain technical conditions) every such embedding of  $G$  in  $S_n$  is maximal unless it appears in their explicit list of exceptions. It is also known that as  $n$  tends to infinity, for almost all values of  $n$  there are no almost simple maximal subgroups of  $S_n$  or  $A_n$ .

## 2.6 The O’Nan–Scott Theorem

The O’Nan–Scott theorem gives us a classification of the maximal subgroups of the alternating and symmetric groups. Roughly speaking, it tells us that every maximal subgroup of  $S_n$  or  $A_n$  is of one of the types described in the previous section. It does not tell us exactly what the maximal subgroups are, but it does provide a first step towards writing down the list of maximal subgroups of  $A_n$  or  $S_n$  for any particular reasonable value of  $n$ .

**Theorem 2.4.** *If  $H$  is any proper subgroup of  $S_n$  other than  $A_n$ , then  $H$  is a subgroup of one or more of the following subgroups:*

- (i) *an intransitive group  $S_k \times S_m$ , where  $n = k + m$ ;*
- (ii) *an imprimitive group  $S_k \wr S_m$ , where  $n = km$ ;*
- (iii) *a primitive wreath product,  $S_k \wr S_m$ , where  $n = k^m$ ;*
- (iv) *an affine group  $\text{AGL}_d(p) \cong p^d : \text{GL}_d(p)$ , where  $n = p^d$ ;*
- (v) *a group of shape  $T^m \cdot (\text{Out}(T) \times S_m)$ , where  $T$  is a non-abelian simple group, acting on the cosets of a subgroup  $\text{Aut}(T) \times S_m$ , where  $n = |T|^{m-1}$ ;*
- (vi) *an almost simple group acting on the cosets of a maximal subgroup of index  $n$ .*

Note that the theorem does not assert that all these subgroups are maximal in  $S_n$ , or in  $A_n$ . This is a rather subtle question. As we noted in Section 2.5.6, the last category of subgroups also requires us to know all the maximal subgroups of all the finite simple groups, or at least those of index  $n$ . In practice, this means that we can only ever hope to get a *recursive* description of the maximal subgroups of  $A_n$  and  $S_n$ .

In view of the fundamental importance of the O’Nan–Scott Theorem, we shall give a proof. However, this proof is not easy, and could reasonably be omitted at a first reading.

### 2.6.1 General results

In this section we collect a number of general facts about (finite) groups which will be useful in the proof of the O’Nan–Scott theorem, as well as being of more general importance. Throughout this section we assume that  $H$  acts faithfully on a set  $\Omega$ .

**Lemma 2.5.** *Every non-trivial normal subgroup  $N$  of a primitive group  $H$  is transitive.*

*Proof.* Otherwise the orbits of  $N$  form a system of imprimitivity for  $H$ .

A normal subgroup  $N$  of a group  $H$  is called *minimal* if  $N \neq 1$  and  $N$  contains no normal subgroup of  $H$  except 1 and  $N$ .

**Lemma 2.6.** *Any two distinct minimal normal subgroups  $N_1$  and  $N_2$  of any group  $H$  commute.*

*Proof.* By normality,  $[N_1, N_2] \leq N_1 \cap N_2 \trianglelefteq H$ , so by minimality

$$[N_1, N_2] = N_1 \cap N_2 = 1.$$

A subgroup  $K$  of a group  $N$  is called *characteristic* if it is fixed by all automorphisms of  $N$ . The following is obvious:

**Lemma 2.7.** *If  $K$  is characteristic in  $N$  and  $N$  is normal in  $H$  then  $K$  is normal in  $H$ .*

A group  $K \neq 1$  is called *characteristically simple* if  $K$  has no proper non-trivial characteristic subgroups. Thus Lemma 2.7 is saying that any minimal normal subgroup of  $H$  is characteristically simple.

**Lemma 2.8.** *If  $K$  is characteristically simple then it is a direct product of isomorphic simple groups.*

*Proof.* If  $T$  is any minimal normal subgroup of  $K$ , then so is  $T^\alpha$  for any  $\alpha \in \text{Aut}K$ . So by the proof of Lemma 2.6 either  $T^\alpha = T$  or  $T \cap T^\alpha = 1$ . In the latter case  $TT^\alpha = T \times T^\alpha$  is a direct product. Since  $K$  is characteristically simple, it is generated by all the  $T^\alpha$ . By induction we obtain that  $K$  is a direct product of a certain number of such  $T^\alpha$ . But then any normal subgroup of  $T$  is normal in  $K$ , so by minimality of  $T$ ,  $T$  is simple.

**Corollary 2.9.** *Every minimal normal subgroup  $N$  of a finite group  $H$  is a direct product of isomorphic simple groups (not necessarily non-abelian).*

*Proof.* By minimality,  $N$  is characteristically simple.

A group  $N$  is called *regular* on  $\Omega$  if for each pair of points  $a$  and  $b$  in  $\Omega$ , there is exactly one element of  $N$  mapping  $a$  to  $b$ . In particular  $N$  is transitive and  $|N| = |\Omega|$ , and every non-identity element of  $N$  is fixed-point-free.

**Lemma 2.10.** *If  $H$  is primitive, and  $N$  is a non-trivial normal subgroup of  $H$ , then either  $C_H(N)$  is trivial, or  $C_H(N)$  is regular and  $|C_H(N)| = |\Omega|$ .*

*Proof.* Clearly  $C_H(N)$  is normal in  $H$ , so by Lemma 2.5, if  $C_H(N) \neq 1$  then both  $N$  and  $C_H(N)$  are transitive. Moreover, if  $1 \neq x \in C_H(N)$  has any fixed points, then the set of fixed points of  $x$  is preserved by  $N$ . This contradiction implies that every element of  $C_H(N)$  is fixed-point-free. This means that  $C_H(N)$  is regular.

This has a number of important consequences.

**Corollary 2.11.** *If  $H$  is primitive, and  $N_1$  and  $N_2$  are non-trivial normal subgroups of  $H$ , and  $[N_1, N_2] = 1$ , then  $N_2 = C_H(N_1)$  and vice versa. In particular,  $H$  contains at most two minimal normal subgroups, and if it has an abelian normal subgroup then it has only one minimal normal subgroup.*

*Proof.* By Lemma 2.5,  $N_1$  is transitive, and by Lemma 2.10,  $C_H(N_2)$  is regular. But  $N_1 \subseteq C_H(N_2)$ , and therefore  $N_1$  and  $C_H(N_2)$  have the same order and are equal.

**Corollary 2.12.** *With the same notation,  $N_1 \cong N_2$ .*

*Proof.* The result is trivial if  $N_1 = N_2$ , so assume  $N_1 \neq N_2$ , and therefore  $N_1 \cap N_2 = 1$ . Fix a point  $x \in \Omega$ , and let  $K$  be the stabiliser of  $x$  in the group  $N_1 N_2$ . Then  $K \cap N_1 = K \cap N_2 = 1$  as  $N_1$  and  $N_2$  are regular. Therefore  $KN_1 = KN_2 = N_1 N_2$ , and by the third isomorphism theorem

$$K \cong K/(K \cap N_1) \cong KN_1/N_1 = N_2 N_1/N_1 \cong N_2/(N_1 \cap N_2) \cong N_2$$

and similarly  $K \cong N_1$ .

**Lemma 2.13.** *Suppose that  $H$  is primitive and  $N$  is a non-trivial normal subgroup of  $H$ . Let  $K$  be the stabiliser in  $H$  of a point. Then  $KN = H$ .*

*Proof.* By Lemma 2.5,  $N$  is transitive, so the result follows by the orbit–stabiliser theorem.

The following result is called the *Dedekind modular law* and although it is very easy to prove it is surprisingly useful.

**Lemma 2.14.** *If  $K$ ,  $X$  and  $N$  are subgroups of a group  $G$  and  $X \leq N$ , then  $N \cap (KX) = (N \cap K)X$ .*

*Proof.* It is obvious that  $(N \cap K)X \leq N \cap (KX)$ . Conversely, if  $k \in K$  and  $x \in X$  satisfy  $kx \in N$ , then also  $k \in N$ , so  $kx \in (N \cap K)X$ .

A subgroup  $X$  of  $H$  is called  *$K$ -invariant* if  $K \leq N_H(X)$ .

**Lemma 2.15.** *Suppose that  $H$  is primitive and  $N$  is a minimal normal subgroup of  $H$ . Let  $K$  be the stabiliser in  $H$  of a point. Then  $K \cap N$  is maximal among  $K$ -invariant proper subgroups of  $N$ .*

*Proof.* If  $K \cap N < X < N$  and  $K \leq N_H(X)$  then  $KX$  is a subgroup of  $H$ . Moreover,  $X$  contains elements (of  $N$ ) not in  $K$ , so  $K < KX$ ; and  $H$  contains elements (of  $N$ ) not in  $X$ , so  $N \cap (KX) = (N \cap K)X = X < N$  and therefore  $KX < KXN = KN = H$ . This contradicts the maximality of  $K$  in  $H$ .

### 2.6.2 The proof of the O’Nan–Scott Theorem

With this preparation we are ready to embark on the proof of the theorem. Let  $H$  be a subgroup of  $S_n$  not containing  $A_n$ , and let  $N$  be a minimal normal subgroup of  $H$ . Let  $K$  be the stabiliser in  $H$  of a point.

*Reduction to the case  $N$  unique and non-abelian.*

Certainly  $H$  is either intransitive (giving case (i) of the theorem), or transitive imprimitive (giving case (ii) of the theorem), or primitive. So we may assume from now on that  $H$  is primitive.

If  $N$  is abelian, then by Corollary 2.9 it is an elementary abelian  $p$ -group, and by Lemma 2.10 it acts regularly, and by Corollary 2.11,  $N = C_H(N)$ . Therefore  $H$  is affine (case (iv) of the theorem).

Otherwise, all minimal normal subgroups of  $H$  are non-abelian. If there is more than one minimal normal subgroup, say  $N_1$  and  $N_2$ , then by Corollaries 2.11 and 2.12  $N_1 \cong N_2$  and both  $N_1$  and  $N_2$  act regularly on  $\Omega$ .

Thus  $N_1$  and  $N_2$  act in the same way on the  $n$  points, so there is an element  $x$  of  $S_n$  conjugating  $N_1$  to  $N_2$ . Moreover, by Corollary 2.11,  $N_2 = C_H(N_1)$ . Therefore  $x$  conjugates  $N_2$  to  $N_1$ , and  $\langle H, x \rangle$  has a unique minimal normal subgroup  $N = N_1 \times N_2$ . So this case reduces to the case when there is a unique minimal normal subgroup.

*The case  $N$  unique and non-abelian.*

From now on, we can assume that  $H$  has a unique minimal normal subgroup,  $N$ , which is non-abelian. If  $N$  is simple, then  $C_H(N) = 1$  and so we are in case (vi) of the theorem. Otherwise,  $N$  is non-abelian, non-simple, say  $N = T_1 \times \cdots \times T_m$  with  $T_i \cong T$  simple for all  $1 \leq i \leq m$ , and  $m > 1$ , and  $H$  permutes the  $T_i$  transitively by conjugation. Also, by Lemma 2.13 we have  $KN = H$ , where  $K$  is the stabiliser in  $H$  of a point.

For each  $i$ , let  $K_i$  be the image of  $K \cap N$  under the natural projection from  $N$  to  $T_i$ . In particular,  $K \cap N \leq K_1 \times \cdots \times K_m$ . We divide into two cases: either  $K_i \neq T_i$  for some  $i$  (and therefore for all  $i$ ) or  $K_i = T_i$  for all  $i$ .

*Case 1:  $K_i \neq T_i$ .*

Now  $K$  normalises  $K_1 \times \cdots \times K_m$ , so that, in this case, by maximality (Lemma 2.15), we have  $K \cap N = K_1 \times \cdots \times K_m$ , and  $K$  permutes the  $K_i$  transitively since  $H = KN$ . Let  $k$  be the index of  $K_i$  in  $T_i$ . Then  $H$  is evidently contained in the group  $S_k \wr S_m$  acting in the product action (case (iii) of the theorem).



Case 2:  $K_i = T_i$ .

This is the hardest case. For the purposes of this proof define the *support* of an element  $(t_1, \dots, t_m) \in T_1 \times \dots \times T_m = N$  to be the set  $\{i \mid t_i \neq 1\}$ . Let  $\Omega_1$  be a minimal (non-empty) subset of  $\{1, \dots, m\}$  such that  $K \cap N$  contains an element whose support is  $\Omega_1$ . Then the subgroup of all elements of  $K \cap N$  with support  $\Omega_1$  still maps onto  $T_i$ , for each  $i \in \Omega_1$ , since it maps onto a normal subgroup and  $T_i$  is simple. Now if  $\Omega_2$  is another such set, intersecting  $\Omega_1$  non-trivially, then there are elements  $x$  and  $y$  in  $K \cap N$  such that  $[x, y] \neq 1$  has support contained in  $\Omega_1 \cap \Omega_2$ . Minimality of  $\Omega_1$  implies that  $\Omega_1 \cap \Omega_2 = \Omega_1$ . In other words,  $\Omega_1$  is a block in a block system invariant under  $K$ , and therefore under  $H = KN$ .

The blocks cannot have size 1, for then  $K$  contains  $N$ , a contradiction. Now

$$n = |\Omega| = |H : K| = |N : N \cap K| \quad (2.10)$$

since  $H = KN$  and  $KN/N \cong K/N \cap K$ . If the block system is non-trivial, with  $l$  blocks of size  $k$ , say, and  $l > 1$ , then  $N \cong T^{kl}$  and  $N \cap K \cong T^l$  so  $n = |T|^{(k-1)l}$ . Thus we see that  $H$  lies inside  $S_r \wr S_l$ , in its product action, where  $r = |T|^{k-1}$ . This is case (iii) of the theorem again.

Otherwise, the block system is trivial, so  $K \cap N$  is a diagonal copy of  $T$  inside  $T_1 \times \dots \times T_m$ , and we can choose our notation such that it consists of the elements  $(g, g, \dots, g)$  for all  $g \in T$ . Also  $n = |T|^{m-1}$ , and the  $n$  points can be identified with the  $n$  conjugates of  $K \cap N$  by elements of  $N$ . The largest subgroup of  $S_n$  preserving this setup is as in case (v) of the theorem. This concludes the proof of the O’Nan–Scott Theorem.

## 2.7 Covering groups

### 2.7.1 The Schur multiplier

We have seen that the alternating groups arise as (normal) subgroups of the symmetric groups, such that  $S_n/A_n \cong C_2$ . They also arise as *quotients* of bigger groups  $2 \cdot A_n$ , by a subgroup  $C_2$ , so that  $2 \cdot A_n/C_2 \cong A_n$ . Under the natural quotient map, each element  $\pi$  of  $A_n$  comes from two elements of  $2 \cdot A_n$ . We label these two elements  $+\pi$  and  $-\pi$ , but it must be understood that there is no canonical choice of which element gets which sign: your choice of signs may be completely different from mine. To avoid confusion, we write the cycles in  $2 \cdot A_n$  with square brackets instead of round ones.

This group  $2 \cdot A_n$  is called the *double cover* of  $A_n$ . More generally, if  $G$  is any finite group, we say that  $\tilde{G}$  is a *covering group* of  $G$  if  $Z(\tilde{G}) \leq \tilde{G}'$  and  $\tilde{G}/Z(\tilde{G}) \cong G$ . If the centre has order 2, 3, etc., the covering group is often referred to as a *double*, *triple*, etc., cover as appropriate. It turns out that every finite perfect group  $G$  has a unique maximal covering group  $\hat{G}$ , with

the property that every other covering group is a quotient of  $\widehat{G}$ . This is called the *universal cover*, and its centre is called the *Schur multiplier* of  $G$ . On the other hand, if  $G$  is not perfect there may be more than one maximal covering group. For example, the group  $C_2 \times C_2$  has four: one is isomorphic to the quaternion group  $Q_8$  and the other three are isomorphic to the dihedral group  $D_8$ . [The *quaternion group*  $Q_8$  consists of the elements  $\pm 1, \pm i, \pm j, \pm k$  and the multiplication is given by  $i^2 = j^2 = k^2 = -1$ ,  $ij = -ji = k$ ,  $jk = -kj = i$ , and  $ki = -ik = j$ .]

### 2.7.2 The double covers of $A_n$ and $S_n$

To define  $2 \cdot A_n$  it suffices to define the multiplication. One way to do this is to define a double cover of the whole symmetric group, as follows. First choose arbitrarily the element  $[1, 2]$ , mapping to the transposition  $(1, 2)$  of  $S_n$ . Then define all the elements  $[i, j]$  inductively by the rule  $[i, j]^{\pm\pi} = -[i^\pi, j^\pi]$  if  $\pi$  is an odd permutation. Then define the elements mapping to cycles  $(a_i, a_{i+1}, \dots, a_j)$  by  $[a_i, a_{i+1}, \dots, a_j] = [a_i, a_{i+1}][a_i, a_{i+2}] \cdots [a_i, a_j]$ .

Finally, all elements are obtained by multiplying together disjoint cycles in the usual way. However, we must be careful not to permute the cycles, or start a cycle at a different point, as this may change  $+\pi$  into  $-\pi$ . For example, our rules tell us that

$$[1, 2] = [1, 2]^{[1, 2]} = -[2, 1]$$

while

$$\begin{aligned} [1, 2]^{[3, 4]} &= -[1, 2] \\ \Rightarrow [1, 2][3, 4] &= -[3, 4][1, 2]. \end{aligned} \tag{2.11}$$

Any product can now be computed using these rules, by first writing each cycle as a product of transpositions, and then simplifying. However, it is not obvious that if we compute the same product in two different ways, then we get the same answer. You will have to take this on trust for now. [A proof can be obtained by embedding the symmetric group in an orthogonal group, and using the construction of the double cover of the orthogonal group in Section 3.9.]

For example, consider the case  $n = 4$ . There are 6 transpositions in  $S_4$ , lifting to 12 elements  $\pm[i, j]$  in the double cover. These elements square to  $\pm 1$ , but they are all conjugate, so either they all square to 1 or they all square to  $-1$ . Let us suppose for simplicity that  $[i, j]^2 = 1$  for all  $i$  and  $j$ . Next there are some elements like  $[1, 2][3, 4]$ . We have already seen that  $[3, 4][1, 2] = -[1, 2][3, 4]$  and therefore

$$\begin{aligned} [1, 2][3, 4][1, 2][3, 4] &= -[3, 4][1, 2][1, 2][3, 4] \\ &= [3, 4][3, 4] \\ &= -1. \end{aligned} \tag{2.12}$$

Similarly the elements  $\pm[1, 3][2, 4]$  and  $\pm[1, 4][2, 3]$  square to  $-1$ , so together these elements form a copy of the quaternion group of order 8. The method for multiplying elements together can best be demonstrated by an example, such as the following.

$$\begin{aligned} [2, 1, 3][3, 1, 4] &= [2, 1][2, 3][3, 1][3, 4] \\ &= [2, 1][3, 1]^{[2, 3]}[2, 3][3, 4] \\ &= -[2, 1][2, 1][2, 3][3, 4] \\ &= [2, 1][2, 1][3, 2][3, 4] \\ &= [3, 2, 4] \end{aligned}$$

In this way we obtain two double covers of  $S_n$ : the first one, denoted  $2 \cdot S_n^+$ , is the one in which the elements  $[i, j]$  have order 2. The second one, in which the elements  $[i, j]$  square to the central involution  $-1$ , is denoted  $2 \cdot S_n^-$ . Both contain the same subgroup of index 2, the double cover  $2 \cdot A_n$  of  $A_n$ .

See Section 3.3.1 for an explicit representation of  $2 \cdot S_4$  as  $\text{GL}_2(3)$ . See also Sections 5.6.8 and 5.6.1, and Exercises 2.35 and 2.37, for descriptions of  $2 \cdot A_4$  and  $2 \cdot A_5$  as groups of unit quaternions.

### 2.7.3 The triple cover of $A_6$

The double covers of the alternating groups, described in Section 2.7.2, are in fact the only covering groups of  $A_n$  for  $n \geq 8$ , and for  $n = 4$  or  $5$ , but  $A_6$  and  $A_7$  have exceptional triple covers as well. These can both be seen as the groups of symmetries of certain sets of vectors in complex 6-space. We let  $\omega = e^{2\pi i/3} = (-1 + \sqrt{-3})/2$  be a primitive (complex) cube root of unity, and consider the vectors  $(0, 0, 1, 1, 1, 1)$ ,  $(0, 1, 0, 1, \omega, \bar{\omega})$  and their multiples by  $\omega$  and  $\bar{\omega} = \omega^2$ . Then take the images of these vectors under the group  $S_4$  of coordinate permutations generated by  $(1, 2)(3, 4)$ ,  $(3, 4)(5, 6)$ ,  $(1, 3, 5)(2, 4, 6)$  and  $(1, 3)(2, 4)$  (that is, the stabiliser in  $A_6$  of the partition  $\{\{1, 2\}, \{3, 4\}, \{5, 6\}\}$ , which we shall write as  $(12 \mid 34 \mid 56)$  for short). These vectors come in triples of scalar multiples, and there are 15 such triples. Indeed, each triple consists of the three vectors whose zeroes are in a given pair of coordinates.

In addition to the above coordinate permutations, this set of 45 vectors is invariant under other monomial elements (that is, products of permutations and diagonal matrices). For example, it is a routine exercise to verify that the set is invariant under  $(1, 2, 3)\text{diag}(1, 1, 1, 1, \bar{\omega}, \omega)$ , i.e. the map

$$(x_1, \dots, x_6) \mapsto (x_3, x_1, x_2, x_4, \bar{\omega}x_5, \omega x_6). \quad (2.13)$$

This group  $G$  of symmetries now acts on the 6 coordinate positions, inducing all even permutations. Thus we obtain a homomorphism from  $G$  onto  $A_6$ , whose kernel consists of diagonal matrices. But any element of the kernel must take each of the 45 vectors to a scalar multiple of itself (since it does not move the zeroes), so is a scalar. Hence the kernel is the group of scalars

$\{1, \omega, \bar{\omega}\}$  of order 3. Thus we have constructed a group  $G$  of order 1080 with  $Z(G) \cong C_3$  and  $G/Z(G) \cong A_6$ .

Finally notice that  $(4, 5, 6)\text{diag}(\omega, \bar{\omega}, 1, 1, 1, 1)$  is also a symmetry, and its commutator with  $(1, 2, 3)\text{diag}(1, 1, 1, 1, \bar{\omega}, \omega)$  is  $\text{diag}(\omega, \dots, \omega)$ , so the scalars are inside  $G'$ . Therefore  $G = G'$ , since  $A_6$  is simple, so  $G$  is perfect.

This group, written  $3 \cdot A_6$ , can be extended to a group  $3 \cdot S_6$  by adjoining the map which interchanges the last two coordinates and then replaces every coordinate by its complex conjugate.

This construction of  $3 \cdot A_6$  and  $3 \cdot S_6$  is of fundamental importance for the sporadic groups, as well as for much of the exceptional behaviour of small classical and exceptional groups. Compare for example Section 5.2.1 on the hexacode, used for constructing the Mathieu group  $M_{24}$ , Sections 3.12.2 and 3.12.3 on exceptional covers of  $\text{PSU}_4(3)$  and  $\text{PSL}_3(4)$ , and Section 5.6.8 on the exceptional double cover of  $G_2(4)$ .

### 2.7.4 The triple cover of $A_7$

Now the groups  $3 \cdot A_7$  and  $3 \cdot S_7$  can be described by extending the above set of 45 vectors to a set of 63 by adjoining the 18 images of  $(2, 0, 0, 0, 0, 0)$  under  $3 \cdot A_6$ . There are now some new symmetries, such as

$$\frac{1}{2} \begin{pmatrix} 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & \omega & \bar{\omega} \\ 0 & 1 & 1 & 0 & \bar{\omega} & \omega \\ 0 & 1 & \bar{\omega} & \omega & 1 & 0 \\ 0 & 1 & \omega & \bar{\omega} & 0 & 1 \end{pmatrix}. \quad (2.14)$$

Indeed there are just 7 ‘coordinate frames’ consisting of 6 mutually orthogonal vectors (up to scalar multiplication) from the set of 63. We label the standard coordinate frame with the number 7, and the frame given by the rows of the above matrix with the number 1. Similarly we obtain frames 2 to 6 containing the vectors  $(0, 2, 0, 0, 0, 0), \dots, (0, 0, 0, 0, 0, 2)$  respectively. With this numbering, the matrix (2.14) corresponds to the permutation  $(1, 7)(5, 6)$  of  $A_7$ .

This gives a map from our group onto the group  $A_7$  of permutations of the 7 coordinate frames. The kernel  $K$  of this map fixes each of the 7 frames, and therefore fixes the intersection of every pair of frames. But each of the 21 triples  $\{v, \omega v, \bar{\omega} v\}$  of vectors is the intersection of two frames, so each triple is fixed by  $K$ , and the argument given above for  $3 \cdot A_6$  shows that  $K$  consists of scalars.

Therefore the group  $G$  we have constructed satisfies  $K = Z(G) \cong C_3$  and  $G/Z(G) \cong A_7$ , as well as  $G = G'$ . This group is denoted  $3 \cdot A_7$ .

## 2.8 Coxeter groups

### 2.8.1 A presentation of $S_n$

We have looked at the symmetric groups as groups of permutations of points, but for many purposes we want to use linear algebra, so it is convenient to consider the points as basis vectors in a vector space. More formally, let  $V = \mathbb{R}^n$  be the canonical real vector space of dimension  $n$ , and let  $\{e_1, \dots, e_n\}$  be the canonical basis, so that  $e_1 = (1, 0, 0, \dots, 0)$  and so on. Let  $S_n$  act on this vector space by permuting the basis vectors in the natural way, that is  $e_i^\pi = e_{i^\pi}$ . (Here we write linear maps as superscripts rather than as functions, for conformity with our notation for permutations. Note that  $\pi^{-1}$ , not  $\pi$ , maps the general vector  $\sum_{i=1}^n \lambda_i e_i$  to  $\sum_{i=1}^n \lambda_{i^\pi} e_i$ .)

Now the transpositions  $(i, j)$  have a single eigenvalue  $-1$ , and all other eigenvalues 1: specifically,  $e_i - e_j$  is an eigenvector with eigenvalue  $-1$ , while  $e_i + e_j$  and  $e_k$  for  $i \neq k \neq j$  are linearly independent eigenvectors with eigenvalue 1. Such linear maps are called *reflections*, because they fix a space of dimension  $n - 1$ , and ‘reflect’ across this subspace by negating all vectors in the orthogonal 1-space. We call  $S_n$  a *reflection group* since it is generated by these reflections.

The symmetric group  $S_n$  can be generated by the  $n - 1$  *fundamental* transpositions  $(i, i + 1)$ , or by the corresponding *fundamental reflections* acting on  $V$ . Obviously, these reflections have order 2, and commute if they are not adjacent, while if they are adjacent, their product  $(i, i + 1)(i + 1, i + 2) = (i, i + 2, i + 1)$  has order 3. What is not so obvious is that these relations are all that you need to work in  $S_n$ . To make this more precise, we define a *presentation* for a group  $G$ , written  $G \cong \langle X \mid R \rangle$ , to consist of a set  $X$  of *generators* and a set  $R$  of *relations*, which are equations in the generators, sufficient to define the entire multiplication table of  $G$ . For example the dihedral group has a presentation

$$D_{2n} \cong \langle a, b \mid a^2 = b^2 = (ab)^n = 1 \rangle. \quad (2.15)$$

Thus we are asserting that  $S_n$  is defined by the so-called *Coxeter presentation*

$$\langle r_1, \dots, r_{n-1} \mid r_i^2 = 1, (r_i r_j)^2 = 1 \text{ if } |i - j| > 1, (r_i r_{i+1})^3 = 1 \rangle. \quad (2.16)$$

To prove this, by induction on  $n$ , note first that it works for  $n = 2$ . Now assume  $n > 2$ , and we prove that the subgroup  $H$  generated by  $r_1, \dots, r_{n-2}$  has index at most  $n$ . But  $r = r_{n-1}$  commutes with  $K = \langle r_1, \dots, r_{n-3} \rangle$ , which by induction has index at most  $n - 1$  in  $H$ . Therefore  $r$  has at most  $n - 1$  images under conjugation by  $H$ . Moreover, every element in  $H \cup HrH$  is in one of the cosets  $Hx$ , where  $x$  is either the identity or one of these (at most)  $n - 1$  conjugates of  $r$ .

We need to show that  $G = H \cup HrH$ . To do this we show that

$$(H \cup HrH)g \subseteq H \cup HrH \quad (2.17)$$

for all  $g \in G$ . Then, as  $1 \in H \cup HrH$ , we have

$$G \subseteq H \cup HrH. \quad (2.18)$$

Plainly, if  $g \in H$ , then the claim (2.17) holds. So, as  $G = \langle H, r \rangle$ , we may assume that  $g = r$ . By induction we assume that  $H = K \cup KqK$  where  $q = r_{n-2}$ . We have  $Hr \subseteq HrH$  and, as every element of  $K$  commutes with  $r$

$$\begin{aligned} HrHr &= Hr(K \cup KqK)r \\ &= H(Kr^2 \cup KrqrK) \\ &= H(K \cup KqrqK) \\ &\subseteq H(K \cup HrH) \\ &= H \cup HrH. \end{aligned} \quad (2.19)$$

This proves the claim.

### 2.8.2 Real reflection groups

The idea of a reflection group, introduced in Section 2.8.1 for the symmetric groups, turns out to be extremely important in many areas of mathematics. The finite real reflection groups were investigated and completely classified by Coxeter. We do not have space here to prove this classification, so we shall merely state it.

Every finite reflection group in  $n$ -dimensional real orthogonal space (so-called *Euclidean space*) can be generated by  $n$  reflections, and is defined by the angles between the reflecting vectors (by which we mean vectors in the  $-1$ -eigenspaces of the generating reflections). Notice that two reflections generate a dihedral group: if the order of this group is  $2k$ , then the reflecting vectors can be chosen to be at an angle  $\pi - \pi/k$  to each other—that is, as near to being opposite as possible. Indeed, it turns out that we can always choose the generating reflections so that every pair has this property, in an essentially unique way.

We draw a diagram consisting of nodes representing the  $n$  generating (or *fundamental*) reflections, joined by edges labelled  $k$  whenever the product of the two reflections has order  $k > 2$ . Any labels which are 3 are usually omitted, for simplicity.

If this diagram is disconnected, it means that all the reflections in one component commute with all the reflections in all the other components, so the reflection group is a direct product of smaller reflection groups. Thus we only really need to describe the connected components of the diagrams. The ones which occur are shown in Table 2.1. The last column of this table gives some indication of the structure of the corresponding reflection groups, which will be explained in more detail in Section 3.12.4.

We saw in Section 2.8.1 that the diagram for  $A_n$  gives a presentation for the group  $S_{n+1}$ , by taking abstract generators of order 2 corresponding to the nodes of the diagram, and specifying that their products have order 2



discrete subgroup of the additive group  $\mathbb{R}^n$ , as well as spanning  $\mathbb{R}^n$  as a vector space. Such a subgroup is called a *lattice*. We call the reflecting vectors *roots*, and the lattice is the corresponding *root lattice*. The term *root system* is used here to denote the set of roots as a subset of the ambient Euclidean space, although in the literature it often has a more abstract definition. The roots corresponding to the vertices of the diagram are called the *fundamental* or *simple* roots.

For vertices joined by a single edge, corresponding to the symmetries of a triangle, we can take the vectors defining the reflections to be all the same length. For vertices joined by a double edge, corresponding to symmetries of a square, the vectors may be taken as the vertices of the square together with the midpoints of the edges: the fundamental reflections must then be one of each type, so that one vector is  $\sqrt{2}$  times as long as the other. We put an arrow on the double edge pointing from the long vector to the short one. [Dynkin originally used open circles for the long roots, and filled circles for the short roots.] Now the diagram  $B_n$  comes in two varieties:  $B_n$  with the arrow pointing outwards and  $C_n$  with the arrow pointing inwards.

Similarly in the case of triple edges, corresponding to symmetries of a regular hexagon, one vector is  $\sqrt{3}$  times as long as the other, and again we put an arrow pointing from the long vector to the short one.

The root systems are of types  $A_n$  ( $n \geq 1$ ),  $B_n$  ( $n \geq 2$ ),  $C_n$  ( $n \geq 3$ ),  $D_n$  ( $n \geq 4$ ),  $E_6$ ,  $E_7$ ,  $E_8$ ,  $F_4$  and  $G_2$ , this last being another name for  $I_2(6)$ . The corresponding diagrams are called *Dynkin diagrams*.

## 2.8.4 Weyl groups

The crystallographic reflection groups arise in many contexts, where they are usually called Weyl groups. The Weyl group of type  $A_n$  is just the symmetric group  $S_{n+1}$ , while that of type  $B_n$  (and  $C_n$ ) is  $S_2 \wr S_n$  and that of type  $D_n$  is a subgroup of index two in the latter. For  $G_2 = I_2(6)$  we get a dihedral group of order 12, and for  $F_4$  a group of order 1152. The Weyl groups of types  $E_6$ ,  $E_7$  and  $E_8$  are especially interesting groups which we shall meet again later. Writing  $W(X_n)$  for the Weyl group of type  $X_n$ , we have the following descriptions of exceptional Weyl groups in terms of orthogonal groups (see Chapter 3).

$$\begin{aligned} W(F_4) &\cong GO_4^+(3) \cong 2^{1+4}:(S_3 \times S_3), \\ W(E_6) &\cong GO_6^-(2) \cong U_4(2):2, \\ W(E_7) &\cong GO_7(2) \times 2 \cong Sp_6(2) \times 2, \\ W(E_8) &\cong 2 \cdot GO_8^+(2) \cong 2 \cdot \Omega_8^+(2):2. \end{aligned} \tag{2.21}$$

In a similar vein, the reflection group of type  $H_4$  is a subgroup of index 2 in  $GO_4^+(5)$ . More details concerning the exceptional Weyl groups are given in Section 3.12.4.



## Further reading

For a comprehensive modern treatment of permutation groups at an introductory level I would recommend the book ‘Permutation groups’ by Dixon and Mortimer [53]. There one can find a detailed proof of the O’Nan–Scott Theorem, and a construction of the Mathieu groups (see Chapter 5) by building up one step at a time from  $\text{PSL}_3(4)$  via  $M_{22}$  and  $M_{23}$  to  $M_{24}$ , and from  $\text{PSL}_2(9)$  via  $M_{11}$  to  $M_{12}$ . An older classic which still has a lot to offer is Wielandt’s book ‘Finite permutation groups’ [170]. Another classic text is Passman’s book ‘Permutation groups’ [145], which develops the subject from the beginning with the study of multiply-transitive groups as one of its principal aims. Highlights are elucidation of the structure of Frobenius groups, that is, transitive permutation groups in which the stabiliser of two points is trivial but the stabiliser of one point is not (or more generally,  $3/2$ -transitive groups, defined as transitive groups in which all non-trivial orbits of the point stabiliser have the same length), and a construction of the Mathieu groups by Witt’s method. Another more modern advanced treatment, which covers a variety of diverse topics, including the O’Nan–Scott Theorem, and infinite permutation groups, is ‘Permutation groups’ by Cameron [19].

For a more specialised treatment of the symmetric groups and their representation theory, see ‘The representation theory of the symmetric group’ by James and Kerber [97], or ‘The symmetric group’ by Sagan [151]. A full and approachable account of the classification of finite real reflection groups (i.e. Coxeter groups) is given by Benson and Grove in ‘Finite reflection groups’ [73]. For a more advanced treatment of Coxeter groups and related topics see Humphreys ‘Reflection groups and Coxeter groups’ [85]. For presentations in general see Coxeter and Moser ‘Generators and relations for discrete groups’ [40] or Johnson ‘Presentations of groups’ [103].

## Exercises

**2.1.** For a permutation  $\pi \in S_n$  define

$$\varepsilon(\pi) = \prod_{1 \leq i < j \leq n} \frac{i - j}{i^\pi - j^\pi} \in \mathbb{Q}.$$

Show that  $\varepsilon(\pi) = \pm 1$  and that  $\varepsilon$  is a group homomorphism from  $S_n$  onto  $C_2 = \{1, -1\}$ . Hence obtain another proof that the sign of a permutation is well-defined.

**2.2.** Let  $G < S_n$  act transitively on  $\Omega = \{1, \dots, n\}$  and let  $H$  be the point stabiliser  $\{g \in G \mid a^g = a\}$  for some fixed  $a \in \Omega$ . Prove that  $\phi : a^g \mapsto Hg$  is a bijection between  $\Omega$  and the set  $G : H$  of right cosets of  $H$  in  $G$ .

Prove also that  $Hg = \{x \in G \mid a^x = a^g\}$ .

**2.3.** Prove that the orbits of a group  $H$  acting on a set  $\Omega$  form a partition of  $\Omega$ .

**2.4.** Show that  $A_n$  is not  $(n-1)$ -transitive on  $\{1, 2, \dots, n\}$ .

**2.5.** Let  $G$  act transitively on  $\Omega$ . Show that the average number of fixed points of the elements of  $G$  is 1, i.e.

$$\frac{1}{|G|} \sum_{g \in G} |\{x \in \Omega \mid x^g = x\}| = 1.$$

**2.6.** Verify that the semidirect product  $G \rtimes_{\phi} H$  defined in Section 2.2 is a group. Show that the subset  $\{(g, 1_H) \mid g \in G\}$  is a normal subgroup isomorphic to  $G$ , and that the subset  $\{(1_G, h) \mid h \in H\}$  is a subgroup isomorphic to  $H$ .

**2.7.** Suppose that  $G$  has a normal subgroup  $A$  and a subgroup  $B$  satisfying  $G = AB$  and  $A \cap B = 1$ . Prove that  $G \cong A \rtimes_{\phi} B$ , where  $\phi : B \rightarrow \text{Aut} A$  is defined by  $\phi(b) : a \mapsto b^{-1}ab$ .

**2.8.** Prove that if the permutation  $\pi$  on  $n$  points is the product of  $k$  disjoint cycles (including trivial cycles), then  $\pi$  is an even permutation if and only if  $n - k$  is an even integer.

**2.9.** Determine the number of conjugacy classes in  $A_8$ , and write down one element from each class.

**2.10.** Show that if  $n \geq 5$  then there is no non-trivial conjugacy class in  $A_n$  with fewer than  $n$  elements.

**2.11.** Prove that  $\text{Inn}(G) \trianglelefteq \text{Aut}(G)$ .

**2.12.** Write down all the elements of  $\text{Aut}(C_2 \times C_2)$ . To which well-known group is it isomorphic?

**2.13.** Calculate  $\text{Inn}(G)$  when  $G = D_8$ . Show that  $\text{Aut}(G) \cong D_8$ .

**2.14.** Show that  $\text{Aut}(Q_8) \cong S_4$ , where  $Q_8 = \langle i, j \mid i^2 = j^2 = (ij)^2 \rangle$  is the quaternion group of order 8.

**2.15.** Show that if  $p$  is an odd prime then

$$\text{Aut}(C_{p^n}) \cong C_{p^n - p^{n-1}} \cong C_{p^{n-1}} \times C_{p-1}.$$

**2.16.** Prove that  $\text{Aut}(A_4) \cong S_4$  and  $\text{Aut}(A_5) \cong S_5$ .

**2.17.** Use Lemma 2.2 to show that if  $n \geq 6$  then  $A_n$  cannot act transitively on a set of  $n+1$  points.

**2.18.** Use the argument of Lemma 2.2 and Theorem 2.3 to show that any automorphism of  $A_6$  which maps 3-cycles to 3-cycles is realised by an element of  $S_6$ .

**2.19.** Construct the outer automorphism of  $S_6$  combinatorially, as follows. From the 6 ‘points’, show that there are 15 ‘duads’ (pairs of points), and 15 ‘synthemes’ (partitions of the 6 points into three duads), and 6 ‘synthemetic totals’ (partitions of the 15 duads into five synthemes). [Thus  $S_6$  permutes the 6 synthemetic totals.]

Show that any two synthemetic totals intersect in a unique syntheme, that any partition of the synthemetic totals into three pairs determines a unique duad, and that any ‘synthemetic total’ on the synthemetic totals corresponds to a point in a natural way.

**2.20.** Let  $S_5$  act on the 10 unordered pairs  $\{a, b\} \subset \{1, 2, 3, 4, 5\}$ . Show that this action is primitive. Determine the stabiliser of one of the 10 pairs, and deduce that it is a maximal subgroup of  $S_5$ .

**2.21.** The previous question defines a primitive embedding of  $S_5$  in  $S_{10}$ . Show that this  $S_5$  is not maximal in  $S_{10}$ .

[Hint: construct a primitive action of  $S_6$  on 10 points, extending this action of  $S_5$ .]

**2.22.** If  $k < \frac{n}{2}$ , show that the action of  $S_n$  on the  $\binom{n}{k}$  unordered  $k$ -tuples is primitive.

**2.23.** If  $G$  acts  $k$ -transitively on  $\{1, 2, \dots, n\}$  for some  $k > 1$ , and  $H$  is the stabiliser of the point  $n$ , show that  $H$  acts  $(k-1)$ -transitively on the subset  $\{1, 2, \dots, n-1\}$ .

**2.24.** Let  $G$  be the group of permutations of 8 points  $\{\infty, 0, 1, 2, 3, 4, 5, 6\}$  generated by  $(0, 1, 2, 3, 4, 5, 6)$  and  $(1, 2, 4)(3, 6, 5)$  and  $(\infty, 0)(1, 6)(2, 3)(4, 5)$ . Show that  $G$  is 2-transitive. Show that the Sylow 7-subgroups of  $G$  have order 7, and that their normalisers have order 21. Show that there are just 8 Sylow 7-subgroups, and deduce that  $G$  has order 168. Show that  $G$  is simple.

**2.25.** Let  $x$  be an element in  $S_n$  of cycle type  $(c_1^{n_1}, \dots, c_k^{n_k})$ , where  $c_1, \dots, c_k$  are distinct positive integers. Show that the centraliser of  $x$  in  $S_n$  is isomorphic to  $(C_{c_1} \wr S_{n_1}) \times \dots \times (C_{c_k} \wr S_{n_k})$ .

**2.26.** Show that if  $H \cong \text{AGL}_3(2) \cong 2^3:\text{GL}_3(2)$  is a subgroup of  $S_8$ , and  $K = H^g$  where  $g$  is an odd permutation, then  $H$  and  $K$  are not conjugate in  $A_8$ .

**2.27.** Prove that  $S_k \wr S_2$  is maximal in  $S_{2k}$  for all  $k \geq 2$ .

**2.28.** Prove that  $S_k \wr S_m$  is maximal in  $S_{km}$  for all  $k, m \geq 2$ .

**2.29.** Prove that the ‘diagonal’ subgroups of  $S_n$  constructed in Section 2.5.5 are primitive.

**2.30.** Show that if  $H$  is abelian and transitive on  $\Omega$ , then it is regular on  $\Omega$ .

**2.31.** Use the O’Nan–Scott theorem to write down as many maximal subgroups of  $S_5$  as you can. Can you prove your subgroups are maximal?

**2.32.** Do the same for  $A_5$ .

**2.33.** Let  $G$  be a simple group,  $H$  a maximal subgroup of  $G$ , and  $K$  a minimal normal subgroup of  $H$ . Prove that  $H = N_G(K)$  and that  $K$  is characteristically simple.

**2.34.** Use Exercise 2.33 to determine the maximal subgroups of  $A_5$  from first principles.

**2.35.** The real quaternion algebra  $\mathbb{H}$  (see Section 4.3.1) is made by linearising the quaternion group  $Q_8$ , identifying the central element  $i^2$  of  $Q_8$  with the real number  $-1$ , and extending the multiplication bilinearly. Show that the quaternion  $\omega = \frac{1}{2}(-1+i+j+k)$ , where  $k = ij$ , satisfies  $\omega^3 = 1$  and  $\omega^{-1}i\omega = j$ . Deduce that the group generated by  $i$  and  $\omega$  is a double cover of  $A_4$ , permuting the four coordinate axes  $\langle 1 \rangle$ ,  $\langle i \rangle$ ,  $\langle j \rangle$ ,  $\langle k \rangle$ .

**2.36.** Prove the following presentations:

- (i)  $\langle x, y \mid x^2 = y^3 = (xy)^3 = 1 \rangle \cong A_4$ ;
- (ii)  $\langle x, y \mid x^2 = y^3 = (xy)^4 = 1 \rangle \cong S_4$ ;
- (iii)  $\langle x, y \mid x^2 = y^3 = (xy)^5 = 1 \rangle \cong A_5$ .

**2.37.** Show that the subgroup of the unit quaternions generated by  $i$  and  $1 + \sigma i + \tau j$ , where  $\sigma = \frac{1}{2}(\sqrt{5} - 1)$  and  $\tau = \frac{1}{2}(\sqrt{5} + 1)$ , is a double cover of  $A_5$ .

[Hint: show that modulo  $-1$  these elements satisfy the relations given in Exercise 2.36(iii).]

**2.38.** Use the outer automorphism of  $S_6$  to prove that the two double covers  $2 \cdot S_6^+$  and  $2 \cdot S_6^-$  of  $S_6$  are isomorphic.

**2.39.** Write down the 15 vectors which are images of  $(0, 0, 1, 1, 1, 1)$  and  $(0, 1, 0, 1, \omega, \bar{\omega})$  under the group  $S_4$  generated by the coordinate permutations  $(1, 2)(3, 4)$ ,  $(1, 3, 5)(2, 4, 6)$  and  $(1, 3)(2, 4)$ .

Verify that the map  $(x_1, \dots, x_6) \mapsto (x_3, x_1, x_2, x_4, \bar{\omega}x_5, \omega x_6)$  preserves this set of vectors up to scalar multiplication by  $\omega$  and  $\bar{\omega}$ .

**2.40.** Show that the reflection group of type  $A_3$  is the group of symmetries of a regular tetrahedron.

**2.41.** Show that the reflection group of type  $B_3$  is the group of symmetries of the cube/octahedron, and is isomorphic to  $C_2 \times S_4$ .

**2.42.** Show that the reflection group of type  $H_3$  is the group of symmetries of the dodecahedron/icosahedron, and is isomorphic to  $C_2 \times A_5$ .

**2.43.** Show that the root system of type  $B_3$  consists of the midpoints of the edges and faces of a cube.

**2.44.** Show that the root system of type  $C_3$  consists of the vertices and the midpoints of the edges of a regular octahedron.

**2.45.** Show that the long roots of the  $B_n$  root system (or the short roots of the  $C_n$  root system) form a root system of type  $D_n$ . What type of root system do the short roots of the  $B_n$  root system (or the long roots of the  $C_n$  root system) form?



<http://www.springer.com/978-1-84800-987-5>

The Finite Simple Groups

Wilson, R.

2009, XV, 298 p., Hardcover

ISBN: 978-1-84800-987-5