Chapter 1

The alternating groups

1.1 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, and prove they are simple.

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 $\mathrm{Aut}(A_n) \cong S_n$ 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.

1.2 Permutations

We first define the *symmetric group* $\mathrm{Sym}(\Omega)$ on a set Ω as the group of all permutations of that set. Here a *permutation* is simply a bijection from the set to itself. If Ω has cardinality n, then we might as well take $\Omega = \{1, \ldots, n\}$. The resulting symmetric group is denoted S_n, and called *the* symmetric group of degree n.

Since a permutation π of Ω 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 have that the number of permutations is $n(n-1)(n-2)\ldots 2.1 = n!$ and therefore $|S_n| = n!$.

A permutation π may be written simply as a list of the images $\pi(1), \ldots, \pi(n)$ of the points in order, or more explicitly, as a list of the points $1, \ldots, n$ with their images $\pi(1), \ldots, \pi(n)$ 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.

1.2.1 The alternating groups

A single interchange of two elements is called a *transposition*, so we have seen how to write any permutation as a product of transpositions. However, there are many different ways of doing this. But if we write the identity permutation as a product of 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. If we follow one permutation by another, it is clear that the number of transpositions required for the product is the sum of the number of transpositions for the two original permutations. It follows that if π is written in two different ways as a product of transpositions, then either the number of transpositions is even in both cases, or it is odd in both cases. Therefore the map ϕ from S_n onto the group $\{\pm 1\}$ of order 2 defined by $\phi(\pi) = 1$ whenever π is the product of an even number of transpositions, is a (well-defined) group homomorphism. As ϕ 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.

The notation for permutations as functions (where $\pi\rho$ means ρ followed by π) is unfortunately inconsistent with the normal convention for permutations that $\pi\rho$ means π followed by ρ. Therefore we adopt a different notation, writing a^π 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.

1.2.2 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 Ω. In symbols, this is expressed by saying that for all a and b in Ω, 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 Ω.

More generally, if we can simultaneously map k points wherever we like, the group is called *k-transitive*. This means that for every list of k distinct points $a_1, \ldots, a_k$ and every list of k distinct points $b_1, \ldots, b_k$ 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 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.

1.2.3 Primitivity

A *block system* for a subgroup H of S_n is a partition of Ω preserved by H; 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^π and b^π 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 Ω; 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

$$\text{if } H \text{ is primitive, then } H \text{ is transitive.} \tag{1.1}$$

For, if H 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 $\{\{1,4\},\{2,3\}\}$.

Another important basic result about primitive groups is that

$$\text{every 2-transitive group is primitive.} \tag{1.2}$$

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.

1.2.4 Group actions

Suppose that G is a subgroup of S_n acting transitively on Ω. Let H be the stabilizer of the point $a \in \Omega$, that is, $H = \{g \in G : a^g = a\}$. Then the points of

Ω 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 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.

1.2.5 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 Ω and properties of the group 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 1. *Suppose that the group G acts transitively on the set Ω, and let H be the stabilizer of $a \in \Omega$. Then G acts primitively on Ω 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 Ω 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 Ω.

Conversely, suppose that G acts imprimitively, and let Ω_1 be the block containing a in a system of imprimitivity. Since G is transitive, it follows that the stabilizer of Ω_1 acts transitively on Ω_1, but not on Ω. Therefore this stabilizer strictly contains H and is a proper subgroup of G, so H is not maximal. □

1.2.6 Wreath products

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

$$G \times H \quad = \quad \{(g, h) : g \in G, h \in H\} \tag{1.3}$$

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

$$\begin{aligned} (g_1, h_1)(g_2, h_2) &= (g_1, g_2, h_1 h_2) \\ (g, h)^{-1} &= (g^{-1}, h^{-1}). \end{aligned} \tag{1.4}$$

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

$$\begin{aligned}(g_1,h_1)(g_2,h_2) &= (g_1 g_2^{\phi(h_1^{-1})}, h_1 h_2)\\ (g,h)^{-1} &= ((g^{-1})^{\phi(h)}, h^{-1}).\end{aligned} \tag{1.5}$$

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

$$\phi(\pi) \quad : \quad (g_1,\ldots,g_n) \mapsto (g_{1^{\pi^{-1}}},\ldots,g_{n^{\pi^{-1}}}). \tag{1.6}$$

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 Ω_1, ..., Ω_n of size m, and then permuting the subscripts 1, ..., 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 Ω into the Ω_i. More generally, any (transitive) imprimitive group can be embedded in a wreath product: if the blocks of imprimitivity for G are Ω_1, ..., Ω_k, then G is a subgroup of $\mathrm{Sym}(\Omega_1) \wr S_k$.

1.3 Simplicity

1.3.1 Cycle types

An alternative notation for a permutation π is obtained by considering the *cycles* of π. These are obtained by taking an element $a \in \Omega$, which maps under π to a^π: this in turn maps to a^{π^2}, which maps to a^{π^3} and so on. Because Ω 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 $(a, a^\pi, a^{\pi^2}, \ldots, a^{\pi^{k-1}})$, where k is the *length* of the cycle. Repeating this with a new element b not in this cycle, we get another cycle of π, disjoint from the first. Eventually, we run out of elements of Ω, at which point π 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^ρ via a and a^π to $a^{\pi\rho}$. Therefore each cycle $(a, a^\pi, a^{\pi^2}, \ldots, a^{\pi^{k-1}})$ of π gives rise to a corresponding cycle $(a^\rho, a^{\pi\rho}, a^{\pi^2\rho}, \ldots, a^{\pi^{k-1}\rho})$. So the cycle type of π^ρ is the same as the cycle type of π. Conversely, if π and π' are two permutations with the same cycle type, we can match up the cycles of the same length, say $(a, a^\pi, a^{\pi^2}, \ldots, a^{\pi^{k-1}})$ with $(b, b^{\pi'}, b^{\pi'^2}, \ldots, b^{\pi'^{k-1}})$. Now define a permutation ρ by mapping a^{π^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 π to itself, we find the centralizer of π. Specifically, if π is an element of S_n of cycle type $(c_1^{k_1}, c_2^{k_2}, \ldots, c_r^{k_r})$, then the centralizer of π in S_n is a direct product of r groups $C_{c_i} \wr S_{k_i}$.

1.3.2 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 centralized by odd permutations. Given an element g of A_n, and an odd permutation ρ, either g^ρ is conjugate to g by an element π of A_n or it is not. In the former case, g is centralized 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^ρ, and so no odd permutation centralizes g.

If g has a cycle of even length, it is centralized by that cycle, which is an odd permutation. Similarly, if g has two odd cycles of the same length, it is centralized by an element ρ which interchanges the two cycles: but then ρ 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 ρ centralizing 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 ρ as products of powers of the cycles of g. In particular ρ is an even permutation.

This proves that g is centralized 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.

1.3.3 The alternating groups are simple

A subgroup H of G is called *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 $N \cap A_{n-1}$. 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), and $|N| \leq n$.

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. This contradiction proves that N does not exist, and so A_n is simple.

1.4 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 1.5.

1.4.1 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 $n_1, \ldots, n_r$, then H is a subgroup of the subgroup $S_{n_1} \times \cdots \times S_{n_r}$ 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 $S_{n_1} \times S_{n_2 + \cdots + n_r}$ 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 $\Omega_1 = \{1, 2, \ldots, k\}$, while the factor S_{n-k} acts on $\Omega_2 = \{k + 1, \ldots, n\}$. 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 Ω_2 to a point in Ω_1, but cannot do this to all points in Ω_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 $S_4 \times S_2$.

1.4.2 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 normalizes the subgroup $S_k \times S_k$. For example we may take $h = (1, k+1)(2, k+2)\cdots(k, 2k)$. 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.

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* $S_k \times \cdots \times S_k$ 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. 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 $n = km$. All the remaining maximal subgroups of S_n must therefore be primitive. 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 $(1, 4)(2, 5)(3, 6)$).

1.4.3 Primitive wreath products

As 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. We 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, we obtain 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}.

Generalizing this construction to an m-dimensional array in the case when $n = k^m$, with $k > 1$ 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 Ω with the Cartesian product ${\Omega_1}^m$ of m copies of a set Ω_1 of size k, and let an element $(\pi_1, \ldots, \pi_m)$ of the base group ${S_k}^m$ act by

$$(a_1, \ldots, a_m) \quad \mapsto \quad ({a_1}^{\pi_1}, \ldots, {a_m}^{\pi_m}) \tag{1.7}$$

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

$$(a_1, \ldots, a_m) \quad \mapsto \quad (a_{1^{\rho^{-1}}}, \ldots, a_{m^{\rho^{-1}}}) \tag{1.8}$$

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 1.4.2 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.

There are three other types of maximal primitive subgroups of S_n which are 'obvious' to the experts, which are generally labelled the affine, diagonal, and almost simple types. Again, we shall not prove that any of these are maximal, and indeed sometimes they are not.

1.4.4 Affine subgroups

The affine groups are essentially the symmetry groups of vector spaces. Let $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ denote the field of order p, and 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 stabilizer of two points is trivial.

1.4.5 Subgroups of diagonal type

The diagonal type groups are built from a non-abelian simple group T, and have the shape $T^k.(\mathrm{Out}(T) \times S_k) \cong (T \wr S_k).\mathrm{Out}(T)$. Here we have 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. In here we have a subgroup $\mathrm{Aut}(T) \times S_k$ consisting of a diagonal copy of T (i.e. the subgroup of all elements $(t, \ldots, t)$ with $t \in T$), extended by its outer automorphism group and the permutation group. This subgroup has index $|T|^{k-1}$, so if we take the permutation action of the group on the cosets of this subgroup, we obtain 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 $A_5 \times A_5 = \{(g, h) : g, h \in A_5\}$ by the group $C_2 \times C_2$ of automorphisms generated by $\alpha : (g, h) \mapsto (g^\pi, h^\pi)$, where π is the transposition $(1, 2)$, and $\beta : (g, h) \mapsto (h, g)$. The point stabilizer is the centralizer of β, generated by α, β and $\{(g, g) : g \in A_5\}$. Therefore an alternative way to describe the action of our group on 60 points is as the action by conjugation on the 60 conjugates of β. We can then show by direct calculation that α and β act as even permutations, so our group $(A_5 \times A_5){:}(C_2 \times C_2)$ embeds in A_{60}. In fact, it is a maximal subgroup.

1.4.6 Almost simple groups

Finally, we have 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 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 one problem to a harder one!

However, a result of Liebeck, Praeger and Saxl 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.

1.5 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—that is too much to ask, rather like asking what are all the prime numbers. It does however 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 1. *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:*

1. *An intransitive group $S_k \times S_m$, where $n = k + m$;*
2. *An imprimitive group $S_k \wr S_m$, where $n = km$;*
3. *A primitive wreath product, $S_k \wr S_m$, where $n = k^m$;*
4. *An affine group $AGL_d(p) \cong p^d{:}GL_d(p)$, where $n = p^d$;*
5. *A group of shape $T^m.(\mathrm{Out}(T) \times S_m)$, where T is a non-abelian simple group, acting on the cosets of the 'diagonal' subgroup $\mathrm{Aut}(T) \times S_m$, where $n = |T|^{m-1}$;*
6. *An almost simple group acting on the cosets of a maximal subgroup.*

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 1.4.6, 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.