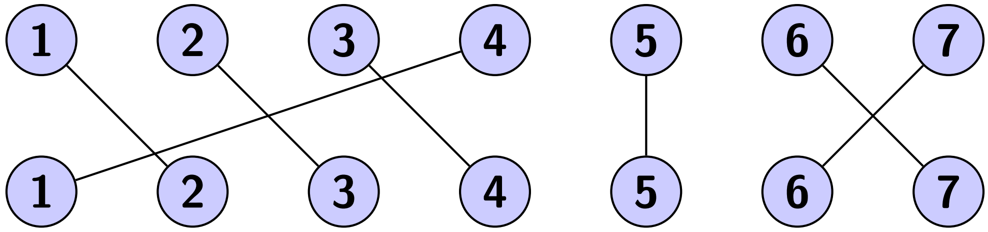

FIGURE 2. A representation of the permutation $(1, 2, 3, 4)(5)(6, 7)$

4. THE ALTERNATING GROUPS

Throughout this section Ω is a finite set of order n. In what follows we will often assume, without comment, that the set Ω is equal to the set $\{1, \ldots, n\}$, and we will write $\mathrm{Sym}(\Omega)$ or $\mathrm{Sym}(n)$ for the *symmetric group* on Ω, the set of all permutations of the set Ω.

Our aim in this section is to take a first look at $\mathrm{Alt}(\Omega)$, the alternating group on Ω, noting down some basic properties. Let us begin by reminding ourselves of its definition:

4.1. **Definition.** Recall that a *transposition* is an element of $\mathrm{Sym}(\Omega)$ that fixes all but two elements of Ω, and these two it swaps. In cycle notation, then, a transposition g is written (α, β) where α and β are the two elements of Ω that are swapped by g.

Our first exercise is easy and fundamental.

(E4.1) *Every element of* $\mathrm{Sym}(\Omega)$ *can be written as a finite product of transpositions.*[12]

Now define the function

$$\begin{aligned} &\mathrm{sgn} : \mathrm{Sym}(n) \to C_2, \\ &g \mapsto \begin{cases} 1, & \text{if } g \text{ is a product of an even number of transpositions;} \\ -1, & \text{if } g \text{ is a product of an odd number of transpositions.} \end{cases} \end{aligned} \tag{3}$$

Note that we write C_2 for the cyclic group of order 2.

Lemma 4.1. *The function* sgn *is a group homomorphism.*

Proof. The key thing to check here is that sgn is a well-defined function - once this is established, the fact that it is a group homomorphism is immediate.

To check well-definedness we must show that no permutation g can be written as a product of transpositions in two different ways, one with an even number of transpositions, the other with an odd number. Suppose, for a contradiction, that such a g does exist. Clearly the same property holds for g^{-1} and we conclude that the same property holds for $1 = gg^{-1}$.

We must show, then, that the identity permutation cannot be written as a product of an odd number of transpositions. To see this, let us represent a permutation $g \in \mathrm{Sym}(\Omega)$ as two rows, both labelled $1, \ldots, n$ with lines taking the upper row to the lower row according to the action of g. Rather than explain this rigorously, we refer to Figure 2 which should make clear what is going on. Observe that if we represent a transposition (i, j) in this way, then the number of 'crossings' in the diagram is an odd number - the lines originating at i and j cross each other once, plus they each cross every line originating at a number k such that $i < k < j$. Since these are all the crossings for a transposition, their number is odd.

We can multiply two permutations using this notation, by writing one on top of the other and connecting the relevant lines. If we consider a product of an odd number of transpositions, then the representation we obtain will have an odd number of crossings - an odd number at each level, and an odd number of levels.

On the other hand observe that if the product of k permutations is equal to the identity, then the representation of this product will have an even number of crossings, since any two lines that cross must cross 'back again'. We are done. □

[12]Put another way - and using terminology introduced in the previous chapter - this exercise asserts, precisely, that $\mathrm{Sym}(\Omega)$ is *generated* by the set of all transpositions.

The function sgn is clearly surjective, hence its kernel is a normal subgroup of $\mathrm{Sym}(\Omega)$ of index 2. We define $\mathrm{Alt}(\Omega)$ to be equal to the kernel of sgn, i.e. $\mathrm{Alt}(\Omega)$ is the set of all permutations that can be written as a product of an even number of transpositions.

In what follows we will sometimes write $\mathrm{Alt}(n)$ as a synonym for $\mathrm{Alt}(\Omega)$.

(E4.2) *If Ω is an infinite set, then one defines the* finitary symmetric group *to be the set of all permtuations that fix all but a finite number of elements of Ω.*

(1) *Prove that $\mathrm{FinSym}(\Omega)$ is a group.*
(2) *Prove that $\mathrm{FinSym}(\Omega)$ is generated by the set of all transpositions.*
(3) *Prove that the function* sgn *given at* (3) *is a group homomorphism from $\mathrm{FinSym}(\Omega)$ to C_2.*
(4) *(Harder) Prove that the kernel of* sgn *(known as the* finitary alternating group*) is an infinite simple group.*

4.2. **Conjugacy classes.** For a fixed positive integer n, we define a *partition of n* to be a non-decreasing list of positive integers, λ, that sum to n; i.e.

$$\lambda = [\underbrace{1,\dots,1}_{n_1}, \underbrace{2,\dots,2}_{n_2}, \underbrace{3,\dots,3}_{n_3}, \dots]$$

where $n = \sum_i in_i$. We write the partition λ as $1^{n_1}2^{n_2}3^{n_3}\cdots$.

Recall that if $g \in \mathrm{Sym}(\Omega)$, then g can be written as the product of a disjoint set of cycles from $\mathrm{Sym}(\Omega)$. If we order the multiset of lengths of these cycles appropriately, then we obtain a partition of n, and this partition is called the *cycle type* of g. We have the following result from basic group theory.

(E4.3) *Let g, h be two elements of $\mathrm{Sym}(\Omega)$. Then g and h are conjugate in $\mathrm{Sym}(\Omega)$ if and only if they have the same cycle type.*

Exercise (E3.18) implies that $\mathrm{Alt}(\Omega)$ is a union of conjugacy classes of $\mathrm{Sym}(\Omega)$.

(E4.4)*Let C be a conjugacy class of $\mathrm{Sym}(\Omega)$ corresponding to partition $1^{n_1}2^{n_2}3^{n_3}\cdots$. Then $C \subset \mathrm{Alt}(\Omega)$ if and only if*

$$n_2 + n_4 + n_6 + \cdots$$

is even.

We are interested in describing the conjugacy classes of $\mathrm{Alt}(\Omega)$. An immediate corollary of (E4.3) is the following.

Corollary 4.2. *Let g, h be two elements of $\mathrm{Alt}(\Omega)$. If g and h are conjugate in $\mathrm{Alt}(\Omega)$, then g and h have the same cycle type.*

We would like to prove a converse. The following lemma does the job.

Lemma 4.3. *Let C be a conjugacy class of $\mathrm{Sym}(\Omega)$ that is a subset of $\mathrm{Alt}(\Omega)$. Either C is a conjugacy class of $\mathrm{Alt}(\Omega)$ or C is the union of two conjugacy classes of $\mathrm{Alt}(\Omega)$ of equal size. The latter happens if and only if, for $g \in C$, $C_{\mathrm{Sym}(\Omega)}(g) \leq \mathrm{Alt}(\Omega)$.*

Proof. Let $g \in C$ and let $K := C_{\mathrm{Sym}(\Omega)}(g)$. The orbit-stabilizer theorem implies that

$$|C| = \frac{|\mathrm{Sym}(\Omega)|}{|K|}$$

Clearly $C_{\mathrm{Alt}(\Omega)}(g) = K \cap \mathrm{Alt}(\Omega)$.

Case 1: Suppose that $K \leq \mathrm{Alt}(\Omega)$. Then (by the orbit-stabilizer theorem) the conjugacy class of g in $\mathrm{Alt}(\Omega)$ has size

$$\frac{|\mathrm{Alt}(\Omega)|}{|K|} = \frac{1}{2}|C|.$$

Note that if the supposition is true for some $g \in C$, then it is true for all $g \in C$. Thus the result follows.

Case 2: Suppose that $K \not\leq \mathrm{Alt}(\Omega)$. Then $C_{\mathrm{Alt}(\Omega)}$ is an index 2 subgroup of K and, by the orbit-stabilizer theorem, the conjugacy class of g in $\mathrm{Alt}(\Omega)$ has size

$$\frac{|\mathrm{Alt}(\Omega)|}{\frac{1}{2}|K|} = |C|.$$

In other words C is a conjugacy class of $\mathrm{Alt}(\Omega)$, and the result follows. □

(E4.5) *Let C be a conjugacy class of $\mathrm{Sym}(n)$ of type $1^{a_1}2^{a_2}3^{a_3}\cdots$. Suppose that $g \in C \subset \mathrm{Alt}(n)$. The following are equivalent:*
(1) C is the union of two conjugacy classes of $\mathrm{Alt}(n)$;
(2) $a_i \leq 1$ for all i, with $a_i = 0$ for all even i.

The following exercise will be used shortly.

(E4.6) *Prove that, if $n \geq 5$ and C is a non-trivial conjugacy class of $\mathrm{Alt}(n)$, then $|C| > n$.*

4.2.1. *An extension.* It should be clear that Lemma 4.3 is a special case of a more general result dealing with the following setting: G is a finite group, N is a normal subgroup, and C is a conjugacy class of G that is a subset of N.

(E4.7) *The set C is the union of a number of conjugacy classes, $C_1, \dots, C_k$, of N; the classes $C_1, \dots C_k$ are of equal size; finally*

$$k = \frac{|G : N|}{|C_G(g) : C_N(g)|},$$

where $g \in C$.

In this situation we say that 'the G-conjugacy class C splits into k N-conjugacy classes.'

4.3. **Simplicity.**

Lemma 4.4. $\mathrm{Alt}(5)$ *is simple.*

Proof. The group $\mathrm{Alt}(5)$ contains a single element of type 1^5, 15 of type 1^12^2 (all conjugate), 20 of type 1^12^2 (split into two conjugacy classes) and 24 of type 5^1 (all conjugate).

A normal subgroup of $\mathrm{Alt}(5)$ must be a union of some of these five conjugacy classes, and one of them must be the conjugacy class of size 1 containing the identity. Furthermore such a union must have order dividing 60. A quick check implies that $\mathrm{Alt}(5)$ contains only $\{1\}$ and itself as normal subgroups. □

(E4.8) *Write down the subgroup lattice of $\mathrm{Alt}(4)$. Identity which subgroups are normal and thereby demonstrate that $\mathrm{Alt}(4)$ is not simple. Prove that $\mathrm{Alt}(2)$ and $\mathrm{Alt}(3)$ are simple and abelian.*

Before proving our main result, we need the following.[13]

(E4.9) *Prove that the group $\mathrm{Alt}(n)$ is generated by the set of all 3-cycles (a 3-cycle is an element of cycle type $1^{n-3}3^1$). Show, in fact, that the following set of 3-cycles is sufficient to generate $\mathrm{Alt}(n)$:*

$$\{(1, 2, i) \mid i = 3, \dots, n\}.$$

Theorem 4.5. $\mathrm{Alt}(n)$ *is simple for $n \geq 5$.*

Proof. We proceed by induction on n. We have proved the base case, when $n = 5$. Suppose that the result is true for $\mathrm{Alt}(n)$ and let K be a normal subgroup of $G = \mathrm{Alt}(n+1)$. Then G has a subgroup H of index $n+1$ that is the stabilizer of a point in the natural action of G on $\{1, \dots, n\}$. Clearly $H \cong \mathrm{Alt}(n)$. By induction H is simple, thus $K \cap H$ is either trivial, or equal to H.

Case 1: $K \cap H$ is trivial. In this case $|K| \leq n+1$ and, in particular, $\mathrm{Alt}(n+1)$ contains a non-trivial conjugacy class of order at most $n+1$. This contradicts (E4.6).[14]

Case 2: $K \cap H = H$. Then K contains H and, since K is normal, K contains all conjugates of H. Since all 3-cycles fix a point in the natural action on $\{1, \dots, n\}$, K contains all 3-cycles. Now (E4.9) implies that $K = G$ as required. □

[13] We ask for a proof of a stronger statement ("Show, in fact...") as this will come in handy for a later result.

[14] A reminder: if you are hazy as to why $|K \cap H| \leq n+1$ in this case, then recall the following basic result: If G, H, K are all groups with $H, K \leq G$, then, writing $KH = \{kh \mid k \in K, h \in H\}$, we have $|KH| = \frac{|K|\cdot|H|}{|K \cap H|}$.

4.4. **Semidirect products.** The group $\mathrm{Alt}(n)$ is a normal subgroup of $\mathrm{Sym}(n)$. To understand the relationship between these two groups, we need to discuss semidirect products. These will be useful in many places throughout the course, for instance they are needed for the definition of a wreath product a little later.

Let H and K be groups. Now suppose that H acts on K as an object from **Group**; equivalently (by Lemma 3.2), let $\phi : H \to \mathrm{Aut}(K)$ be a group homomorphism.

Consider the set whose elements are ordered pairs with the first entry from H and the second from K[15]. Define a multiplication operation on this set as follows:

$$(h_1, k_1)(h_2, k_2) = (h_1 \cdot h_2, k_1^{\phi(h_2)} \cdot k_2).$$

Lemma 4.6. *The set and multiplication operation just defined form a group.*

This group is denoted $K \rtimes_\phi H$.

Proof. The multiplication defined above is clearly a well-defined binary operation. Let us check the group axioms in turn:

Associativity: Let $h_1, h_2, h_3 \in H$ and $k_1, k_2, k_3 \in K$. Now observe that

$$\begin{aligned}(h_1, h)2)\left((h_2, k_2)(h_3, k_3)\right) &= (h_1, k_1)(h_2h_3, k_2^{\phi(h_3)}k_3) \\ &= (h_1h_2h_3, k_1^{\phi(h_2h_3)}k_2^{\phi(h_3)}k_3), \text{ while} \\ \left((h_1, k_1)(h_2, k_2)\right)(h_3, k_3) &= (h_1h_2, k_1^{\phi(h_2)} \cdot k_2)(h_3, k_3) \\ &= (h_1h_2h_3, (k_1^{\phi(h_2)}k_2)^{\phi(h_3)}k_3)\end{aligned}$$

and associativity follows.

Identity: The identity element is $(1, 1)$ and observe that for $h \in H, k \in K$

$$(1,1)(h,k) = (h, 1^{\phi(h)}k) = (h,k)$$
$$(h,k)(1,1) = (h, k^{\phi(1)}1) = (h,k).$$

Inverse: One can easily check that, for $h \in H, k \in K$, $(h^{-1}, (k^{-1})^{\phi(h^{-1})})$ is the inverse of (h, k) for the multiplication defined above. We are done. □

(E4.10) *Suppose that the action of H on K is the trivial action. What is $K \rtimes_\phi H$?*

The next lemma lists some basic properties of this construction.

Lemma 4.7. *Let $G = K \rtimes_\phi H$.*

1. *The subset $K_0 := \{(1, k) \mid k \in K\}$ is a normal subgroup of $K \rtimes_\phi H$ that is isomorphic to K;*
2. *The subset $H_0 := \{(h, 1) \mid h \in H\}$ is a subgroup of $K \rtimes_\phi H$ that is isomorphic to K;*
3. *$G/K_0 \cong H$;*
4. *The natural conjugation action of H_0 on K_0 is isomorphic to the action of H on K given by ϕ.*

Proof. Define a function

$$\begin{aligned}\varphi : K \rtimes_\phi H &\to H \\ (h,k) &\mapsto h.\end{aligned}$$

Now, for any $(h_1, k_1), (h_2, k_2) \in G$ observe that

$$\varphi\left((h_1, k_1)(h_2, k_2)\right) = \varphi(h_1h_2, k_1^{\phi(h_2)}k_2) = h_1h_2 = \varphi(h_1, k_1)\varphi(h_2, k_2).$$

Thus φ is a group homomorphism. It is clear that $K_0 = \ker(\varphi)$ thus K_0 is a normal subgroup of G and (1) follows. Now define a function

$$\begin{aligned}\theta : K_0 &\to K \\ (1,k) &\mapsto k.\end{aligned}$$

[15]In other words consider the *set* (not the group) $H \times K$.

It is clear that θ is an isomorphism and (1) is proved. Now the subset H_0 is obviously a subgroup and, moreover, the restriction

$$\varphi|_{H_0} : H_0 \to H$$

is clearly an isomorphism, thus (2) is proved. To see (3), simply note that φ is onto, and apply the first isomorphism theorem.

Finally, to prove (4), observe that the following diagram commutes (note that the conjugation action $H_0 \times K_0 \to K_0$ is labelled γ):

$$\begin{array}{ccc} H_0 \times K_0 & \xrightarrow{\gamma} & K_0 \\ \downarrow {\scriptstyle (\varphi|_{H_0},\theta)} & & \downarrow {\scriptstyle \theta} \\ H \times K & \xrightarrow{\phi} & K \end{array} \qquad \begin{array}{ccc} ((h,1),(1,k)) & \overset{\gamma}{\longmapsto} & (h,1)^{-1}(1,k)(h,1) = (1, k^{\phi(h)}) \\ \downarrow {\scriptstyle (\varphi|_{H_0},\theta)} & & \downarrow {\scriptstyle \theta} \\ (h,k) & \overset{\psi}{\longmapsto} & k^{\phi(h)} \end{array}$$

□

In what follows I will tend to identify the groups K_0 and K, and the groups H_0 and H. This allows me to abuse notation and think of $K \rtimes_\phi H$ as a semi-direct product of two of its *subgroups*, a point of view that is helpful [16] Usually, too, the homomorphism ϕ is obvious from the context, so I will tend to write the semidirect product as $K \rtimes H$.

Suppose that G is a group with normal subgroup K such that $G/K \cong H$. In this case we write $G = K.H$ and call G *an extension of K by H*.[17] A semi-direct product $G := K \rtimes H$ is an example of a group $K.H$, but it is important to note that not all groups $K.H$ can be expressed as a semi-direct product. In the literature, groups $K.H$ that can be expressed as a semi-direct product are called *split extensions* and are sometimes denoted $K : H$; those that can't be expressed as a semi-direct product are called *non-split extensions*.[18] The following exercise allows us to recognise when an extension is split.

> **(E4.11)** *Suppose that K is a normal subgroup of a group G with G/K isomorphic to a group H. The extension $H.K$ is split if and only if G contains a subgroup J such that $G = JK$ and $J \cap K = \{1\}$.*
>
> **(E4.12)** *Prove that, for all integers $n \geq 2$, $\mathrm{Sym}(n) \cong \mathrm{Alt}(n) : C_2$.*
>
> **(E4.13)** *Find an example of a group $G = K.H$ (where K and H are both non-trivial finite groups) which is non-split. Hint: there is precisely one example with $|G| \leq 7$, and it is abelian. The smallest non-abelian examples have $|G| = 8$.*
>
> **(E4.14)** *Write down as many groups G as you can, for which $G = K.H$ where $K \cong A_6$ and $H \cong C_2$. Identify those that can be written as split extensions.*

One final remark: there is an unfortunate notational issue that crops up in this area. For two subgroups H and K of a group G, the following definition of *the product of H and K* is standard:

$$HK := \{hk \mid h \in H, k \in K\}.$$

In general this set is not a group.

> **(E4.15)** *Prove that if $H \leq N_G(K)$, then $HK = KH$, and HK is a group.*

Note that if $H \leq N_G(K)$, then (E4.11) implies that the set $H.K$ is isomorphic to $K \rtimes H$ if and only if $H \cap K = \{1\}$.

---

[16] Writing $G = K \rtimes \phi_H$ where K and H are subgroups of G is sometimes referred to as *an internal direct product of K and H*.

[17] **Warning**: Some authors call this *an extension of H by K*.

[18] If you know about short exact sequences, then this terminology will make sense to you. If you don't, I recommend you look 'em up.

4.5. **Almost simple groups.** We have already seen the conjugation action γ of a group G on itself, γ has associated homomorphism $\gamma^* : G \to \mathrm{Aut}(G)$ with kernel equal to $Z(G)$, the center of G. If $Z(G)$ is trivial, then γ^* yields an embedding of G into its own automorphism group.

Let us consider the special case when $G = S$, a non-abelian finite simple group. The following lemma gives information about the structure of $\mathrm{Aut}(S)$.

Lemma 4.8. *Let S be a non-abelian finite simple group. Then $\mathrm{Aut}(S)$ contains a unique normal subgroup S_0 isomorphic to S and every non-trivial normal subgroup of $\mathrm{Aut}(S)$ contains S_0.*

Proof. We have already observed that $\mathrm{Aut}(S)$ contains a subgroup S_0 isomorphic to S - it is the image of γ^* and is normal in $\mathrm{Aut}(S)$ by Lemma 3.5. One can quickly check that the action of $\mathrm{Aut}(S)$ on S_0 via conjugation is isomorphic to the action of $\mathrm{Aut}(S)$ on S given by the identity embedding $\mathrm{Aut}(S) \to \mathrm{Aut}(S)$.

Suppose that N is a non-trivial normal subgroup of S. Since S is simple, $S \cap N$ is either trivial or equal to S. If the latter, then we conclude that N contains S. Thus, to prove the result, we assume that $S \cap N$ is trivial, and we demonstrate a contradiction.

Let $s \in S, n \in N$ and observe that the commutator $s^{-1}n^{-1}sn$ is an element of both S and N. Thus, by assumption, this commutator is trivial, and we conclude that N centralizes S. But this implies that the conjugation action of N on S is trivial, contradicting the fact that N contains non-trivial automorphisms of S. We are done. □

In what follows we will identify the two groups S and S_0, and think of S as a subgroup of $\mathrm{Aut}(S)$. The lemma implies that we can do this without ambiguity. Now we are able to define the notion of an *almost simple group*: it is a group G such that

$$S \leq G \leq Aut(S).$$

(E4.16) *Prove that a group G is almost simple if and only if the following two conditions hold:*
(1) G contains a normal subgroup S that is non-abelian and simple;
(2) any non-trivial normal subgroup of G contains S.

Clearly, if $n \geq 5$, then $\mathrm{Alt}(n)$ is itself an almost simple group, as is $\mathrm{Sym}(n)$. One consequence of the classification of finite simple groups is that all finite almost simple groups are also classified.

(E4.17) *Prove that $\mathrm{Sym}(n)$ is almost simple for $n \geq 5$.*

(E4.18) *(Hard) How many almost simple groups (up to isomorphism) have a normal subgroup isomorphic to $\mathrm{Alt}(6)$?*

4.6. $\mathrm{Aut}(\mathrm{Alt}(n))$**.** In this section we will classify all of the almost simple groups with a normal subgroup isomorphic to $\mathrm{Alt}(n)$ for some n. Equivalently we will describe the automorphism group of $\mathrm{Alt}(n)$. We know already that $\mathrm{Sym}(n) \leq \mathrm{Aut}(\mathrm{Alt}(n))$, and it turns out that in nearly all cases, the reverse inclusion also holds:

Theorem 4.9. *If $n = 5$ or $n \geq 7$, then $\mathrm{Aut}(\mathrm{Alt}(n)) = \mathrm{Sym}(n)$. If $n = 6$, then $\mathrm{Aut}(\mathrm{Alt}(n))$ contains $\mathrm{Sym}(n)$ as an index 2 subgroup.*

Our proof of Theorem 4.9 proceeds by considering 3-cycles in $\mathrm{Alt}(n)$. Observe first that a product of two 3-cycles can take one of the following four forms (in each case, we assume that all letters are distinct):

$$(a,b,c)(a,b,c) = (a,d)(b,c); \quad (a,b,c)(a,d,b) = (b,c,d);$$
$$(a,b,c)(a,d,e) = (a,b,c,d,e); \quad (a,b,c)(d,e,f).$$

Lemma 4.10. *Let ϕ be an automorphism of $\mathrm{Alt}(n)$ such that for any 3-cycle σ, $\phi(\sigma)$ is a 3-cycle. Then there exists an element $\rho \in \mathrm{Sym}(n)$ such that $\phi(\sigma) = \rho^{-1}\sigma\rho$.*

Proof. Consider the 3-cycles $u_i = (1, 2, i)$ where $i = 3, \ldots, n$. Observe that if $i \neq j$, then the product u_iu_j has order 2. For $i = 3, \ldots, n$ define $v_i = \phi(u_i)$ and observe that (by assumption) v_i is a 3-cycle, and that the order of $v_iv_j = 2$ whenever $i \neq j$. Thus, examining the forms above, observe that $v_1 = (a, b, c)$ and $v_2 = (a, b, d)$.

Consider v_3. If v_3 fixes a, then in order for v_1v_3 (resp. v_2v_3) to have order 2 we must have $v_3 = (b, c, f)$ (resp. (b, d, g)). This is a contradiction, thus we obtain that v_3 does not fix a. A similar analysis for b implies that $v_3 = (a, b, e)$ for some e (distinct from a, b, c and d).

We can iterate this analysis to conclude that there are distinct $a_1, \dots, a_n$ such that

$$\phi(1, 2, i) = (a_1, a_2, a_i).$$

Now let $\rho \in \mathrm{Sym}(n)$ be the permutation for which $i^\rho = a_i$ and we obtain immediately that

$$\rho^{-1}(1, 2, i)\rho = (a_1, a_2, a_i) = \phi(1, 2, i).$$

Then (E4.9) yields the result. □

Lemma 4.11. *If $n \geq 3$ and $n \neq 6$, then any automorphism of $\mathrm{Alt}(n)$ is obtained by a conjugation of an element of $\mathrm{Sym}(n)$. Thus $\mathrm{Aut}(\mathrm{Alt}(n)) = \mathrm{Sym}(n)$.*

Proof. Let ϕ be an automorphism of $G := \mathrm{Alt}(n)$ and let σ be a 3-cycle. The image of $\phi(\sigma)$ has order 3, i.e. it is a product of r distinct 3-cycles for some $r \geq 1$.

Observe that, for $n = 3, 4, 5$ any element of order 3 is a 3-cycle. Thus the supposition of Lemma 4.10 is true by default and the result follows. Assume, from here on, that $n \geq 6$.

One can check easily enough that

$$|C_G(\sigma)| = \frac{3}{2}(n-3)!, \text{ and } |C_G(\phi(\sigma))| = \frac{3^r}{2}r!(n-3r)!$$

Since $C_G(\sigma) \cong C_G(\phi(\sigma))$ we conclude that

$$\frac{3}{2}(n-3)! = \frac{3^r}{2}r!(n-3r)!.$$

A little bit of checking confirms that either $r = 1$ or else $(r, n) = (2, 6)$ and we are done. □

(E4.19) *If $n \geq 3$ and $n \neq 6$, then any automorphism of $\mathrm{Sym}(n)$ is inner. Thus $\mathrm{Aut}(\mathrm{Sym}(n)) = \mathrm{Sym}(n)$.*

The proof of Lemma 4.11 implicitly used the following result (that we have already seen for the case of inner automorphisms). The final part will be needed below.

(E4.20) *Let ϕ be an automorphism of a group G and let $g, h \in G$. Then*
- *g and h have the same order;*
- *$C_G(g) \cong C_G(\phi(g))$;*
- *If g and h are conjugate in G, then $\phi(g)$ and $\phi(h)$ are conjugate in G.*[19]

In light of Lemma 4.11, to prove Theorem 4.9, we need only study Alt(6). We need the following result.

(E4.21) *Suppose that H is a subgroup of a group G and suppose that there exists $g \in G$ such that, for all $h \in G \backslash H$, $gh \in H$. Then $|G : H| \leq 2$.*

Observe that Alt(6) has exactly two conjugacy classes of elements of order 3, thus any automorphism g of Alt(6) either swaps these conjugacy classes or fixes them. Let g be an automorphism that swaps these classes, and consider $h \in \mathrm{Aut}(\mathrm{Alt}(6))$. If h fixes the classes, then, by Lemma 4.10, $h \in \mathrm{Sym}(6)$, if h swaps these classes then gh fixes these classes and, again by Lemma 4.10, $gh \in \mathrm{Sym}(6)$.

Now (E4.21) implies that Aut(Alt(6)) contains Sym(6) as a subgroup of index at most 2 . To prove Theorem 4.9, then, we need to show that there exists an automorphism of Alt(6) that is not contained in Sym(6). This is our task for the rest of the section.

We proceed by studying a particular subgroup H of Alt(6) that is isomorphic to Alt(5). Of course Alt(6) has some obvious subgroups of this form – take the stabilizer of a point in the action on $\{1, \dots, 6\}$. The subgroup we construct is different – it acts *transitively* on $\{1, \dots, 6\}$. The next exercise gets us under way.

(E4.22) *Prove that Alt(5) contains 6 Sylow 5-subgroups.*

[19] In particular this implies that $\mathrm{Aut}(G)$ has a well-defined action on the set of conjugacy classes of G. This is another way of looking at the situation described in §4.2.1.

Let Ω be the set of Sylow 5-subgroups of $\mathrm{Alt}(5)$. By Sylow's theorems $\mathrm{Alt}(5)$ acts transitively by conjugation on Ω. Of course the action is faithful (since $\mathrm{Alt}(5)$ is simple) and hence Lemma 3.1 yields an embedding $\mathrm{Alt}(5) \hookrightarrow \mathrm{Sym}(6)$. Write H for this copy of $\mathrm{Alt}(5)$ in $\mathrm{Sym}(6)$.

(E4.23) *Prove that, in fact, $H \hookrightarrow \mathrm{Alt}(6)$. Prove, moreover, that H has 6 distinct conjugates in $\mathrm{Alt}(6)$.*

Let Γ be the set of 6 conjugates of H in $\mathrm{Alt}(6)$. Now $\mathrm{Alt}(6)$ acts faithfully and transitively on these 6 conjugates and so we obtain an embedding $\mathrm{Alt}(6) \hookrightarrow \mathrm{Sym}(6)$. By the same reasoning as in the previous exercise we conclude that, in fact, $\mathrm{Alt}(6) \hookrightarrow \mathrm{Alt}(6)$ and so, in particular, this embedding is an isomorphism.

(E4.24) *Prove that this isomorphism is not induced by an element of $\mathrm{Sym}(6)$.*

4.7. **A first look at subgroups.** One of the main aims of the first half of the course is to understand the subgroup structure of $\mathrm{Alt}(n)$ and $\mathrm{Sym}(n)$. We begin that process now.

A useful definition: suppose a group G acts on a set Ω, and suppose that Γ is a proper subset of Ω. The *setwise stabilizer* of Γ is

$$G_\Gamma := \{g \in G \mid \gamma^g \in \Gamma \text{ for all } \gamma \in \Gamma\}.$$

If $H \leq G_\Gamma$ we say things like 'H preserves Γ setwise'.

The following two exercises are focused on the same idea, but the second uses categorical language. Note that, by convention, we define $\mathrm{Sym}(\emptyset) = \mathrm{Sym}(0) = \{1\}$.

(E4.25) *Let Ω be a finite set of order n, and let Γ be a subset of Ω with $|\Gamma| = k$.*

1. *There is a unique subgroup G of $\mathrm{Sym}(\Omega)$ that preserves Γ setwise and is isomorphic to $\mathrm{Sym}(k) \times \mathrm{Sym}(n-k)$;*
2. *if $H \leq \mathrm{Sym}(\Omega)$ preserves Γ setwise, then $H \leq G$.*

(E4.26) *Consider a category called **Intrans***

***Objects**: An object is a pair (Γ, Δ) where Γ is a finite set and Δ is a subset of Γ.*

***Arrows**: An arrow $(\Gamma, \Delta) \to (\Gamma', \Delta')$ is a function $f : \Gamma \to \Gamma'$ such that $x \in \Delta \implies f(x) \in \Delta'$.*

1. *Prove that **Intrans** is a category.*
2. *Prove that if X is an object in **Intrans**, then $\mathrm{Aut}(X) \cong \mathrm{Sym}(\Delta) \times \mathrm{Sym}(\Gamma \backslash \Delta)$.*
3. *Prove that if G acts on $X = (\Gamma, \Delta)$ as an object from **Intrans**, then G is a subset of the setwise stabilizer of Δ, and conversely.*

The following proposition is an immediate corollary of either of the previous two exercises.

Proposition 4.12. *Let $H \leq \mathrm{Sym}(\Omega)$ where $|\Omega| < \infty$. One of the following holds:*

1. *H is intransitive and $H \leq \mathrm{Sym}(k) \times \mathrm{Sym}(n-k)$ for some $1 < k < n$;*
2. *H is transitive.*[20]

The following exercise is included as food for thought (i.e. parts of it might be rather hard).

(E4.27) *Let Ω be a subset of order n and let Γ and Δ) be subsets of Ω of order k. Let H (resp. K) be the setwise stabilizer of Γ (resp. Δ) in $\mathrm{Sym}(n)$. For what values of n and k is H maximal? Are H and K conjugate? How many conjugacy classes of subgroups isomorphic to H does $\mathrm{Sym}(n)$ contain?*

(E4.28) *Describe the intersection of $\mathrm{Sym}(k) \times \mathrm{Sym}(n-k)$ with $\mathrm{Alt}(n)$. Is it maximal in $\mathrm{Alt}(n)$? How many conjugacy classes of such subgroups are there?*

[20]Note that, since H is a permutation group, I feel at liberty to write things like 'H is intransitive' when I really mean something like 'the action of H on Ω induced by restricting the action of $\mathrm{Sym}(\Omega)$ on Ω is intransitive'. This sort of terminology will crop up from here on without further comment.