Queen Mary
University of London

MTHM024/MTH714U **Group Theory**

Notes 5 **Autumn 2011**

---

5 Symmetric and alternating groups

In this section we examine the alternating groups A_n (which are simple for $n \geq 5$), prove that A_5 is the unique simple group of its order, and study some further properties, including the remarkable outer automorphism of the symmetric group S_6.

Let us remind ourselves at the start of the test for conjugacy in S_n. The *cycle structure* of permutation is the list of cycle lengths.

Proposition 5.1 *Two elements of S_n are conjugate if and only if they have the same cycle structure.*

Using this, it is possible to calculate the size of any conjugacy class in S_n:

Proposition 5.2 *If a permutation has a_i cycles of length i for $i = 1, 2, \ldots, n$, then the size of its conjugacy class in S_n is*

$$\frac{n!}{1^{a_1} a_1! 2^{a_2} a_2! \cdots n^{a_n} a_n!}.$$

Proof Write down brackets and spaces for a permutation with the given cycle structure. There are $n!$ ways of writing the numbers $1, 2, \ldots, n$ into the gaps. But we get the same permutation if we start any cycle at a different point, or if we rearrange the cycles of the same length in any order. The number of different representations of a permutation is thus the denominator in the above expression.

We saw that every permutation is a product of transpositions; that is, the transpositions generate S_n. Similarly, we have:

Proposition 5.3 *The alternating group A_n is generated by the 3-cycles.*

Proof First, note that 3-cycles are even permutations, so they lie in A_n.

Now take an arbitrary even permutation $g \in A_n$; say

$$g = t_1 t_2 \cdots t_{2k-1} t_{2k}.$$

We have to express g as a product of 3-cycles. Clearly it suffices to write each consecutive pair of transpositions $t_{2i-1}t_{2i}$ in the product in terms of 3-cycles. There are three cases for a product of two transpositions:

- $(a,b)(a,b) = 1$;
- $(a,b)(a,c) = (a,b,c)$;
- $(a,b)(c,d) = (a,b,c)(a,d,c)$.

5.1 The group A_5

Recall that A_n is the group of all even permutations on $\{1,\ldots,n\}$. (A permutation is even if the number of disjoint cycles is congruent to n mod 2, or if it is the product of an even number of transpositions.) It is a group of order $(n!)/2$.

A_2 is the trivial group, and A_3 the cyclic group of order 3. A_4 is a group of order 12. It consists of the identity, three conjugate elements of order 2, and eight elements of order 3 (falling into two conjugacy classes each of size 4). The identity and the three elements of order 2 form a normal subgroup of order 4, the *Klein group* V_4. It is the only non-trivial proper normal subgroup of A_4. (We use "non-trivial" to mean "not the identity subgroup", and "proper" to mean "not the whole group".)

Proposition 5.4 *A_5 is simple.*

There are several ways to prove this theorem. Here are two. They both start by describing the conjugacy classes. First, note that any conjugacy class in S_n must be a union of conjugacy classes in A_n; since the index is 2, either it is a single A_n-class, or it splits into two A_n-classes of equal sizes. We need to know which classes split.

Proposition 5.5 *The following are equivalent for a permutation $g \in A_n$:*

- *the S_n-conjugacy class of g splits into two A_n-classes;*
- *there is no odd permutation which commutes with g;*
- *g has no cycles of even length, and all its cycles have distinct lengths.*

Proof S_n acts transitively by conjugation, and the stabiliser of an element g is its *centraliser* (the set of elements which commute with g). Now if $C(g)$ and $C'(g)$ are the centralisers of g in S_n and A_n, then $C'(g) = C(g) \cap A_n$, so $C'(g) = C(g)$ if condition (b) holds, and $|C'(g)| = |C(g)|/2$ otherwise. Now the sizes of the conjugacy classes in S_n and A_n are $|S_n|/|C(g)|$ and $|A_n|/|C'(g)|$, from which we see that (a) is equivalent to (b).

If g has a cycle of even length, then this cycle is an odd permutation commuting with g; if g has two cycles of equal odd length l, then a permutation interchanging them is a product of l transpositions and commutes with g. On the other hand, if neither possibility holds, then any permutation commuting with g must fix each of its cycles and act on it as a power of the corresponding cycle of g, hence is an even permutation. So (b) and (c) are equivalent.

Using this, we can calculate the conjugacy classes in A_5:

Cycle structure	Class size	Splits in A_5?
$[1,1,1,1,1]$	1	No
$[1,2,2]$	15	No
$[1,1,3]$	20	No
$[5]$	24	Yes

So the class sizes are $1, 15, 20, 12, 12$.

A normal subgroup is a union of conjugacy classes, containing the identity, and having order dividing 60 (the order of A_5). It is easy to see that there is no such divisor.

Here is a rather different proof. We know that A_5 acts doubly transitively, and hence primitively, on $\{1,2,3,4,5\}$. (Alternatively it is primitive because 5 is prime.) So, if N is a non-trivial normal subgroup, then N is transitive. Then $|N| = 5 \cdot |N \cap A_4|$, and $N \cap A_4$ is a normal subgroup of A_4, hence is $\{1\}$, V_4 or A_4. So $|N| = 5, 20$ or 60. We can ignore the last case.

Since 5 divides $|N|$, we see that N contains a Sylow 5-subgroup of A_5. Since they are all conjugate, it contains all six Sylow 5-subgroups. But they contain 24 elements of order 5; these cannot fit into a group of order 5 or 20.

5.2 Simplicity of A_n

Theorem 5.6 *A_n is simple for all $n \geq 5$.*

Proof The proof is by induction, starting at $n = 5$ (the case we have just done). Suppose that N is a non-trivial normal subgroup of A_n. Then N is transitive, so contains a set of coset representatives for the stabiliser A_{n-1}; thus $NA_{n-1} = A_n$. Also, $N \cap A_{n-1}$

is a normal subgroup of A_{n-1}, so by the inductive hypothesis either $N \cap A_{n-1} = A_{n-1}$ (in which case we have

$$A_n/N = NA_{n-1}/N \cong A_{n-1}/N \cap A_{n-1} = \{1\},$$

so that $N = A_n$) or $N \cap A_{n-1} = \{1\}$, in which case N acts regularly and $|N| = n$.

Now there are many ways to proceed. Here are four different proofs. I think that the first is probably the easiest.

- Suppose that h is a non-identity element of N. Choose the numbering such that h maps $1 \mapsto 2$ and $3 \mapsto 4$, where $1,2,3,4$ are all distinct. Now choose an element $g \in A_n$ which maps $1 \mapsto 1$, $2 \mapsto 2$, $3 \mapsto 3$, and $4 \mapsto 5$. (Since $n \geq 6$, there will be such an element.) Then, by the rules for conjugating permutations, $g^{-1}hg$ maps $1 \to 2$ and $3 \mapsto 5$. This contradicts the fact that N is a transitive group of degree n with order n, so contains a unique element mapping 1 to 2.

- We have a formula for the size of conjugacy classes in A_{n-1}. Using this, and some hard labour, it is possible to show that there cannot be a conjugacy class of size $n-1$ or smaller. So the existence of a normal subgroup of order n is impossible.

- Use the analysis of regular normal subgroups we gave in the last chapter of the notes. The action of A_{n-1} on $N \setminus \{1\}$ by conjugation is isomorphic to its action on $\{1,2,\ldots,n-1\}$. This implies

  (a) all non-identity elements of N are conjugate, so all have the same order, necessarily a prime number p;

  (b) now N is a p-group, so $Z(N) \neq \{1\}$; but $Z(N)$ is fixed by conjugation, so $Z(N) = N$, and N is elementary abelian;

  (c) suppose that $p > 2$, and let $a, b \in N$ such that $b \neq a, a^2$; then since A_{n-1} is 2-transitive, there is an element $g \in A_{n-1}$ satisfying $g^{-1}ag = a$ and $g^{-1}a^2g = b$, which is impossible;

  (d) suppose that $p = 2$, and choose $a, b, c \in N$ generating a subgroup of order 8; since N is triply transitive, there is an element $g \in N$ satisfying $g^{-1}ag = 1$, $g^{-1}bg = b$ and $g^{-1}(ab)g = c$, which is impossible.

  The contradiction shows that no normal subgroup of order n can exist.

- We have seen that N is generated by at most $\lfloor \log_2 n \rfloor$ elements. An automorphism is determined by the images of the generators, so $|\operatorname{Aut}(N)| \leq n^{\log_2 n}$. But A_{n-1} acts faithfully on N by conjugation, so $(n-1)! \leq n^{\log_2 n}$. Some easy checking shows that this is impossible for $n \geq 6$.

5.3 Normal subgroups of S_n

Theorem 5.7 *The only normal subgroups of S_n for $n \geq 5$ are $\{1\}$, A_n and S_n.*

Proof Let N be a normal subgroup of S_n. Then $N \cap A_n$ is a normal subgroup of A_n, so $N \cap A_n = \{1\}$ or A_n.

If $N \cap A_n = A_n$, then $N \geq A_n$, so $N = A_n$ or S_n.

if $N \cap A_n = \{1\}$, then

$$N = N/(N \cap A_n) \cong NA_n/A_n = S_n/A_n \text{ or } A_n/A_n,$$

So $|N| = 1$ or 2. But $|N| = 2$ is impossible, since then there would have to be a non-identity element of S_n in a conjugacy class of size 1. So $N = \{1\}$ in this case.

5.4 The uniqueness of A_5

Proposition 5.8 *A simple group of order* 60 *is isomorphic to* A_5.

Proof Let G be a simple group of order 60.

The number of Sylow 5-subgroups of G is congruent to 1 (mod 5) and divides 12, but is not 1 (else the unique Sylow subgroup would be a normal subgroup of G). So there are six Sylow 5-subgroups.

Consider the action of G on the set Ω of six Sylow 5-subgroups by conjugation. By Sylow's Theorem, the action is transitive. Since G is simple, the kernel of the action is $\{1\}$; that is, the action is faithful. So the image of the action is a subgroup of S_6 isomorphic to G; let us call it H.

Now $H \leq A_6$, since otherwise $H \cap A_6$ would be a normal subgroup of H, contradicting the simplicity of H. Also, $|H| = 60$, and $|A_6| = 360$, so H has index 6 in H.

Consider the action of $K = A_6$ on the set $\cos(H,K)$ of six cosets of H. This action is faithful, so K is a subgroup of the symmetric group S on the set $\cos(H,K)$. Clearly K has index 2 in S, and so is a normal subgroup. Thus $K = A_6$ in its usual action on six objects. But then H is the stabiliser of one of these objects, so $H \cong A_5$.

Since $G \cong H$ we have $G \cong A_5$ as required.

5.5 Automorphisms

You may have got lost in the above proof because the group A_6 was acting on a set of six objects which were not the original $\{1,\ldots,6\}$ on which the group is defined. We can put this confusion to constructive use. In the next section we see a remarkable property of the number 6, which is shared by no other positive integer, finite or infinite.

First some definitions. Let G be a group.

- An *automorphism* of G is an isomorphism from G to G.
- An *inner automorphism* is a map of the form $c_g : x \mapsto g^{-1}xg$ from the group G to itself.

In what follows, maps will be composed from left to right, so to avoid confusion, we write a map on the right of its argument.

Theorem 5.9 *Let G be a group.*

(a) The set of automorphisms of G forms a group under the operation of composition. This is the automorphism group *of G, denoted by* $\mathrm{Aut}(G)$.

(b) An inner automorphism of G is an automorphism of G (as the name suggests).

(c) The inner automorphisms comprise a normal subgroup of $\mathrm{Aut}(G)$*, denoted by* $\mathrm{Inn}(G)$*; it is isomorphic to $G/Z(G)$, where $Z(G)$ is the centre of G.*

Proof (a) It is straightforward to show that the composition of automorphisms is an automorphism, and the inverse map of an automorphism is an automorphism.

(b) First, c_g is a bijective map, since it has an inverse, namely $c_{g^{-1}}$. Next,

$$(xy)c_g = g^{-1}(xy)g = g^{-1}xg \cdot g^{-1}yg = (xc_g)(yc_g),$$

so c_g is a homomorphism, and hence an automorphism.

There is a map from G to $\mathrm{Aut}(G)$ given by $g \mapsto c_g$. We show that this map is a homomorphism.

$$\begin{aligned} (xc_g)c_h &= (g^{-1}xg)c_h = h^{-1}(g^{-1}xg)h, \\ xc_{gh} &= (gh)^{-1}x(gh) = (h^{-1}g^{-1})x(gh), \end{aligned}$$

and the right-hand sides are equal.

So the First Isomorphism Theorem tells us that $\mathrm{Inn}(G)$, the image of this map, is a subgroup of $\mathrm{Aut}(G)$. To show that it is normal, let ϕ be any automorphism of G, and calculate the effect of $\phi^{-1}c_g\phi$:

$$\begin{aligned} x(\phi^{-1}c_g\phi) &= ((x\phi^{-1})c_g)\phi \\ &= (g^{-1}(x\phi^{-1})g)\phi \\ &= (g\phi)^{-1}x(g\phi), \end{aligned}$$

where we used the fact that automorphisms map inverses to inverses to say that $(g^{-1})\phi = (g\phi)^{-1}$. So $\phi^{-1}c_g\phi = c_{g\phi}$, an inner automorphism. Thus $\mathrm{Inn}(G)$ is a normal subgroup of $\mathrm{Aut}(G)$.

The kernel of the map $g \mapsto c_g$ is the set

$$\begin{aligned}\{g \in G : c_g = 1\} &= \{g \in G : xc_g = x \text{ for all } x \in G\} \\ &= \{g \in G : g^{-1}xg = x \text{ for all } x \in G\} \\ &= \{g \in G : xg = gx \text{ for all } x \in G\} \\ &= Z(G).\end{aligned}$$

So $G/Z(G) \cong \mathrm{Inn}(G)$.

An automorphism which is not inner is called *outer*. However, by abuse of language, the *outer automorphism group* of G is not the group of outer automorphisms — they do not form a group [WHY?] — but is defined to be the quotient group $\mathrm{Aut}(G)/\mathrm{Inn}(G)$. Thus, the outer automorphism group of G is trivial if and only if G has no outer automorphisms.

5.6 Outer automorphisms of S_6

For $n \geq 3$, $Z(S_n) = \{1\}$, so $\mathrm{Inn}(S_n) \cong S_n$. It turns out that, except for the single value $n = 6$, we actually have $\mathrm{Aut}(S_n) = S_n$, so that S_n has no outer automorphisms. We will not prove that, but will construct outer automorphisms of S_6 in two different ways, and hence show that $|\mathrm{Out}(S_6)| = 2$.

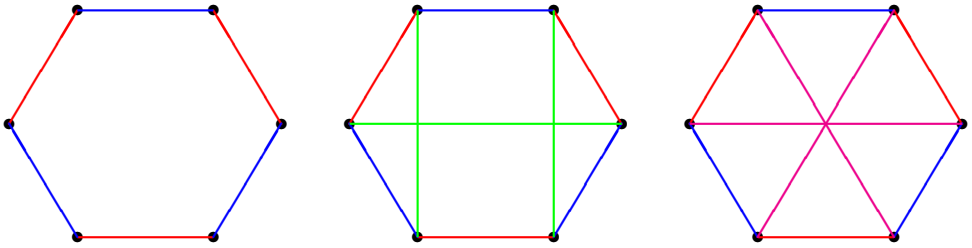
First, we can find such a subgroup directly. Let $G = S_5$. It is easy to check that G has six Sylow 5-subgroups. (The only divisors of 24 which are congruent to 1 (mod 6) are 1 and 6, and we know that S_5 does not have a normal Sylow 5-subgroup.) So S_5 acts faithfully and transitively on the set of six Sylow 5-subgroups by conjugation, giving a transitive subgroup of S_6 isomorphic to S_5 but not conjugate to the stabiliser of a point. By our previous analysis, this shows that there is an outer automorphism.

For the second approach, we follow Sylvester, including his rather odd terminology. Let $A = \{1,2,\ldots,6\}$. A *duad* is a 2-element subset of A; there are $(6 \cdot 5)/2 = 15$ duads. A *syntheme* is a partition of A into three duads. Each duad is contained in three synthemes (the number of ways of partitioning the remaining four points into two duads), so there are $(15 \cdot 3)/3 = 15$ synthemes. Finally, a *synthematic total* is a partition of the 15 duads into five synthemes. It is a little harder to count this; we argue as follows.

Consider two disjoint synthemes; think of them as having two different colours, say red and blue (see the left-hand figure below). The red and blue duads form the edges of a hexagon, and the remaining nine duads are of two types; six "short diagonals" of the hexagon, and three "long diagonals".

It is easy to see that there are two different ways to pick three disjoint duads from these nine: either take the three long diagonals (magenta on the right), or one long

diagonal and the two short diagonals perpendicular to it (green in the middle). So the only way to partition these nine duads into three synthemes is to take the three synthemes of the second type.



Thus, any two disjoint synthemes are contained in a unique synthematic total. There are eight synthemes disjoint from a given one; so the number of synthematic totals is $(15 \cdot 8)/(5 \cdot 4) = 6$. The six synthematic totals are all isomorphic, and so S_6 permutes them transitively. Thus, the stabilisers of synthemes form a conjugacy class of subgroups of index 6, not conjugate to the point stabilisers. Hence we get our outer automorphism.

Using this approach, we can show that the outer automorphism group has order 2: all that is required is to show that any subgroup of index 6 stabilises either a point or a syntheme.

It is an instructive exercise to repeat the construction. Let X be the set of synthemes. Then

- any two synthematic totals share a unique syntheme, so the "duads of X" correspond to synthemes of A;
- three synthemes containing a given duad lie between them in all the synthematic totals, so the "synthemes of X" correspond to duads of A;
- the five duads through a point lie between them in all fifteen synthemes, so the "synthematic totals of X correspond to the points of A.

Thus, the square of our automorphism is the identity.

Exercise: Show that a permutation group which acts primitively on $\{1,\ldots,n\}$ and contains a transposition is the symmetric group S_n.

Exercise: Show that a permutation group which acts primitively on $\{1,\ldots,n\}$ and contains a 3-cycle is the symmetric group S_n or the alternating group A_n.