Queen Mary
University of London

MTH714U **Group theory**

Notes 2 **Autumn 2008**

---

2 Permutation groups

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.

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.

A possibly more convincing proof that the sign of a permutation is well-defined may be obtained by letting S_n act on the set $\{\pm 1\}$ by multiplying by

$$\prod_{i>j} \frac{i^\pi - j^\pi}{i-j},$$

and proving that this does define a group action, with kernel A_n.

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.

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.

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

$$\text{if } H \text{ is primitive, then } H \text{ is transitive.} \tag{1}$$

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

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

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.

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, $H = \{g \in G : a^g = a\}$. Recall (the orbit–stabilizer theorem) that the points of Ω are in natural bijection with the (right) cosets Hg of H in G. This bijection is given by $Hx \leftrightarrow a^x$. 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.

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. □

For example, consider S_n acting on the set $\Omega = \{\{1,2\},\ldots,\{n-1,n\}\}$ of $n(n-1)/2$ unordered pairs from n points. The stabilizer H of $\{1,2\}$ is $S_2 \times S_{n-2}$, and provided $n > 4$ this subgroup is maximal: if $g \notin H$, then there are points $i, j > 2$ such that $i^g \in \{1,2\}$ but j^g is not. Then the transposition (i^g, j^g) is in the subgroup generated by H and g, and therefore so are all the transpositions. It follows that S_n acts primitively on the given $n(n-1)/2$ objects.

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

$$G \times H \quad = \quad \{(g,h) : g \in G, h \in H\} \tag{3}$$

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

$$\begin{aligned} (g_1,h_1)(g_2,h_2) &= (g_1,g_2,h_1h_2) \\ (g,h)^{-1} &= (g^{-1},h^{-1}). \end{aligned} \tag{4}$$

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

$$\begin{aligned} (g_1,h_1)(g_2,h_2) &= (g_1 g_2^{\phi(h_1^{-1})}, h_1h_2) \\ (g,h)^{-1} &= ((g^{-1})^{\phi(h)}, h^{-1}). \end{aligned} \tag{5}$$

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

$$\phi(\pi) \quad : \quad (g_1,\ldots,g_n) \mapsto (g_{1\pi^{-1}},\ldots,g_{n\pi^{-1}}). \tag{6}$$

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 $\mathrm{Sym}(\Omega_1) \wr S_k$.

Iwasawa's Lemma and simplicity The key to proving simplicity of many of the finite simple groups is Iwasawa's Lemma:

THEOREM 2. *If G is a finite perfect group, acting faithfully and primitively on a set Ω, such that the point stabilizer H has a normal abelian subgroup A whose conjugates generate G, then G is simple.*

Proof. For otherwise, there is a normal subgroup K with $1 < K < G$, which does not fix all the points of Ω, so we may choose a point stabilizer H with $K \not\leq H$, and therefore $G = HK$ since H is a maximal subgroup of G. So any $g \in G$ can be written $g = hk$ with $h \in H$ and $k \in K$, and therefore every conjugate of A is of the form $g^{-1}Ag = k^{-1}h^{-1}Ahk = k^{-1}Ak \leq AK$. Therefore $G = AK$ and $G/K = AK/K \cong A/A\cap K$ is abelian, contradicting the assumption that G is perfect. □

To see this in action, let us prove that A_n is simple whenever $n \geq 5$. Let Ω be the set of unordered triples (i.e. subsets of size 3) from the set $\{1,2,\ldots,n\}$. The stabilizer of one of these triples is $A_n \cap (S_3 \times S_{n-3})$, which has a normal subgroup of order 3, cyclically permuting the three points in the triple. These 3-cycles generate the alternating group. Also, provided $n \geq 5$, they are commutators, since $(a,b,c) = (a,b)(d,e)(a,c)(d,e) = [(ac)(de),(bc)(de)]$. Finally, we need to show that the action of A_n on Ω is primitive. We can prove this by showing by brute force that the stabilizer of a triple is maximal. (Actually it isn't maximal if $n = 6$, so we need a different proof in this case.) Then apply Iwasawa's Lemma.

More on automorphisms More generally, if $G \trianglelefteq H$, then each element of H induces an automorphism of G, by conjugation in H. Thus for example if $n \geq 4$ then S_n is (isomorphic to) a subgroup of $\mathrm{Aut}(A_n)$. It turns out that for $n \geq 7$ it is actually the whole of $\mathrm{Aut}(A_n)$. We shall not prove this here.

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 $(1,2,3)$, $(1,2,4)$, …, $(1,2,n)$. 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.

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 ϕ of S_6 we first note that ϕ must map the point stabilizer S_5 to another subgroup $H \cong S_5$. However, H does not fix one of the six points on which S_6 acts. Therefore H is transitive on these six points.

So 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 have a group homomorphism $\phi : S_6 \to \mathrm{Sym}(\{Hg : g \in S_6\}) \cong S_6$. The kernel of ϕ is trivial, since S_6 has no non-trivial normal subgroups of index 6 or more. Hence ϕ is a group isomorphism, i.e. an automorphism of S_6.

But ϕ is not an inner automorphism, because it maps the transitive subgroup H to the stabilizer of the trivial coset H, whereas inner automorphisms preserve transitivity.