Lecture 1: Introduction, and alternating groups

Robert A. Wilson

Queen Mary, University of London

LTCC, 6th October 2008

INTRODUCTION

Simple groups

- A subgroup $H$ of a group $G$ is normal if the left and right cosets are equal, $Hg = gH$ for all $g \in G$.

- A group $G$ is simple if it has exactly two normal subgroups, 1 and $G$.

- The abelian simple groups are exactly the cyclic groups of prime order, $C_p$.

- The non-abelian simple groups are much harder to classify: 50 years of hard work by many people, c. 1955–2005, led to

- CFSG: the Classification Theorem for Finite Simple Groups.

CFSG

Every non-abelian finite simple group is one of the following

- an alternating group $A_n$, $n \geq 5$: the set of even permutations on $n$ points;

- a classical group over a finite field: six families (linear, unitary, symplectic, and three families of orthogonal groups);

- an exceptional group of Lie type: ten families;

- 26 sporadic simple groups, ranging in size from $M_{11}$ of order 7920 to the Monster of order nearly $10^{54}$.

Our aim is to understand the statement of this theorem in more detail.
Practicalities

▶ The course web-site is accessible from the LTCC site http://www.ltcc.ac.uk/, or directly at http://www.maths.qmul.ac.uk/~raw/FSG/. It will contain lecture notes, exercises, solutions, links to background reading, further reading, etc.
▶ You are encouraged to print off and read the lecture notes, which are more detailed than the lectures themselves.

ALTERNATING GROUPS

Permutations

▶ A permutation on a set $\Omega$ is a bijection from $\Omega$ to itself.
▶ The set of permutations on $\Omega$ forms a group, called the symmetric group on $\Omega$.
▶ A transposition is a permutation which swaps two points and fixes all the rest.
▶ Every permutation can be written as a product of transpositions.
▶ The identity element cannot be written as the product of an odd number of transpositions.
▶ Hence no element can be written both as an even product and an odd product.

Even permutations

▶ A permutation is even if it can be written as a product of an even number of transpositions, and odd otherwise.
▶ The even permutations form a subgroup called the alternating group, and the odd permutations form a coset of this subgroup.
▶ In particular, the alternating group has index 2 in the symmetric group.
▶ So if $\Omega$ has $n$ points, the symmetric group $S_n$ has order $n!$, and the alternating group has order $n!/2$. 
Transitivity

- Write $a^\pi$ for the image of $a \in \Omega$ under the permutation $\pi$.
- The orbit of $a \in \Omega$ under the group $H$ is $\{a^\pi \mid \pi \in H\}$.
- The orbits under $H$ form a partition of $\Omega$.
- If there is only one orbit (the entire set $\Omega$ itself), then $H$ is transitive.
- For $k \geq 1$, a group $H$ is $k$-transitive if for every set of $k$ distinct elements $a_1, \ldots, a_k \in \Omega$ and every set of $k$ distinct elements $b_1, \ldots, b_k \in \Omega$, there is a permutation $\pi \in H$ with $a_i^\pi = b_i$ for all $i$.

Primitivity

- A block system for $H$ is a partition of $\Omega$ preserved by $H$.
- The partitions $\{\Omega\}$ and $\{\{a\} \mid a \in \Omega\}$ are trivial block systems.
- If $H$ preserves a non-trivial block system (called a system of imprimitivity), then $H$ is called imprimitive.
- Otherwise $H$ is primitive.
- If $H$ is primitive, then $H$ is transitive. Why?
- If $H$ is 2-transitive, then $H$ is primitive. Why?

Group actions

Suppose $G$ is a subgroup of $S_n$, acting on $\Omega = \{1, 2, \ldots, n\}$.
- The stabilizer of $a \in \Omega$ in $G$ is $H := \{g \in G \mid a^g = a\}$.
- The set $\{g \in G \mid a^g = b\}$ is equal to the coset $Hx$, where $x$ is any element with $a^x = b$.
- In other words $a^x \mapsto Hx$ is a bijection between $\Omega$ and the set of right cosets of $H$.
- Hence the orbit-stabilizer theorem: $|H| \cdot |\Omega| = |G|$.
- Conversely, the action of $G$ on $\Omega$ is the same as the action on cosets of $H$ given by $g : Hx \mapsto Hxg$.

Maximal subgroups

- This gives a very useful correspondence between transitive group actions and subgroups.
- primitive group actions correspond to maximal subgroups:
  - The block of imprimitivity containing $a$, say $B$, corresponds to the cosets $Hx$ such that $a^x \in B$.
  - The union of these cosets is a subgroup $K$ with $H < K < G$, so $H$ is not maximal.
- ... and conversely.
**Simplicity of Alternating Groups**

- Every element in $S_n$ can be written as a product of disjoint cycles.
- Conjugation by $g \in S_n$ is the map $x \mapsto g^{-1}xg$. It maps a cycle $(a_1, \ldots, a_k)$ to $(a_1^g, \ldots, a_k^g)$.
- Hence two elements of $S_n$ are conjugate if and only if they have the same cycle type.
- Conjugacy in $A_n$ is a little more subtle: if there is a cycle of even length, or two cycles of the same odd length, then we get the same answer.
- But if the cycles have distinct odd lengths then the conjugacy class in $S_n$ splits into two classes of equal size in $A_n$.

**Simplicity of $A_5$**

- The conjugacy classes in $A_5$ are:
  - One identity element;
  - 15 elements of shape $(a, b)(c, d)$;
  - 20 elements of shape $(a, b, c)$;
  - 24 elements of shape $(a, b, c, d, e)$, consisting of two conjugacy class of 12 elements each.
- No proper non-trivial union of conjugacy classes, containing the identity element, has size dividing 60, so there is no proper non-trivial normal subgroup.

**Simplicity of $A_n$**

- Assume $N$ is a normal subgroup of $A_n$.
- Then $N \cap A_{n-1}$ is normal in $A_{n-1}$, so by induction is either 1 or $A_{n-1}$.
- In the first case, $N$ has at most $n$ elements, but there is no conjugacy class small enough to be in $N$.
- In the second case, $N$ contains a 3-cycle, so contains all 3-cycles, so is $A_n$. 
Intransitive subgroups

We work in $S_n$ rather than $A_n$ (as it is easier), and consider only maximal subgroups.

- If a subgroup has more than two orbits, it cannot be maximal.
- If a subgroup has two orbits, of lengths $k$ and $n - k$, then it is contained in $S_k \times S_{n-k}$.
- This is maximal if $k \neq n - k$. Why?
- If $k = n - k$ we can adjoin an element swapping the two orbits, giving a larger group $(S_k \times S_k).2$ which is maximal.
- The intransitive maximal subgroups of $S_n$ are, up to conjugacy, $S_k \times S_{n-k}$ for $1 \leq k < n/2$.

Transitive imprimitive subgroups

- If $n = km$, then you can split $\Omega$ into $k$ subsets of size $m$.
- The stabilizer of this partition contains $S_m \times S_m \times \cdots \times S_m$, the direct product of $k$ copies of $S_m$.
- It also contains $S_k$ permuting the $k$ blocks.
- Together these form the wreath product of $S_m$ with $S_k$, written $S_m \wr S_k$.
- These subgroups are usually (always?) maximal in $S_n$. 
Primitive wreath products

- If $n = m^k$, we can label the $n$ points of $\Omega$ by $k$-tuples $(a_1, \ldots, a_k)$ of elements $a_i$ from a set $A$ of size $m$.
- Then $S_m \times S_m \times \cdots \times S_m$ can act on this set by getting each copy of $S_m$ to act on one of the $k$ coordinates.
- Also $S_k$ can act by permuting the $k$ coordinates.
- This gives an action of $S_m \wr S_k$ on the set of $m^k$ points.
- This is called the product action to distinguish it from the imprimitive action we have just seen.

Affine groups

- If $n = p^d$, where $p$ is prime, then we can label the $n$ points of $\Omega$ by the vectors of a $d$-dimensional vector space over $\mathbb{Z}/p\mathbb{Z}$.
- The translations $x \mapsto x + v$ act on this vector space.
- The linear transformations $x \mapsto xM$ (where $M$ is an invertible matrix) also act.
- These generate a group $AGL_d(p)$ which we shall study in more detail next week.
- Usually (but not always) these groups are maximal in either $S_n$ or $A_n$.

Subgroups of diagonal type

These are harder to describe.
- Let $T$ be a non-abelian simple group, and let $H$ be the wreath product $T \wr S_m$ for some $m \geq 2$.
- This contains a ‘diagonal’ subgroup $D \cong T$ consisting of all the ‘diagonal’ elements $(t, t, \ldots, t) \in T \times T \times \cdots \times T$.
- $H$ contains a subgroup $D \times S_m$ of index $|T|^{m-1}$.
- Let $H$ act on the $n = |T|^{m-1}$ cosets of this subgroup.
- Then $H$ is nearly maximal in $S_n$: we just need to adjoin the automorphisms of $T$, acting the same way on all the $m$ copies of $T$.

Almost simple groups

- A group $G$ is almost simple if there is a simple group $T$ such that $T \leq G \leq \text{Aut } T$.
- If $M$ is a maximal subgroup of $G$, then $G$ acts primitively on the $|G| / |M|$ cosets of $M$.
- Hence $G$ is a subgroup of $S_n$, where $n = |G| / |M|$.
- Often such a group $G$ is maximal in $S_n$ or $A_n$.
- For a reasonable value of $n$ these are straightforward to classify.
- But classifying these groups $G$ for all $n$ is a hopeless task.
The O’Nan–Scott Theorem

says that every maximal subgroup of $A_n$ or $S_n$ is of one of these types.
If $H$ is any proper subgroup of $S_n$ other than $A_n$, then $H$ is a subgroup of (at least) one of the following:

- (intransitive) $S_k \times S_{n-k}$, for $k < n/2$;
- (transitive imprimitive) $S_k : S_m$, for $n = km$, $1 < k < n$;
- (product action) $S_k \rtimes S_m$, for $n = km$, $k \geq 5$;
- (affine) $AGL_d(p)$, for $n = p^d$, $p$ prime;
- (diagonal) $T^m.(\text{Out}(T) \times S_m)$, where $T$ is non-abelian simple, and $n = |T|^{m-1}$;
- (almost simple) an almost simple group $G$ acting on the $n$ cosets of a maximal subgroup $M$. 

THE END