NZMRI Summer School
Introduction to the finite simple groups

Colva Roney-Dougal
colva.roney-dougal@st-andrews.ac.uk

School of Mathematics and Statistics, University of St Andrews

Nelson, 8 January 2018

University
of
St Andrews

Simple groups and maximal subgroups

Defn: A proper subgroup $M < G$ is a maximal subgroup of G if $M < H \leq G \Rightarrow H = G$.

Defn: A group G is simple if G is nontrivial and G has no proper non-trivial normal subgroups.

Example 1

G – abelian simple group of order n.
$1 \neq g \in G$, $a := |g|$.
If $a \neq n$ then $1 < \langle g \rangle < G$. Then G abelian $\Rightarrow \langle g \rangle$ is a proper non-trivial normal subgp of G.
So each non-identity element of G has order n, and so n is prime and G is cyclic.

The maximal subgroups of C_n are $C_{n/p}$ for each prime $p \mid n$.

The Jordan–Hölder Theorem

Theorem 2 (Jordan–Hölder Thm)

G – finite group. Then $\exists$ subgps $G_1, \ldots, G_n$ of G s.t.
$G = G_0 > G_1 > G_2 > \cdots > G_n = 1$ and $\forall i$

1. $G_i \trianglelefteq G_{i-1}$
2. *G_{i-1}/G_i is simple.*

Let $G = H_0 > H_1 > H_2 > \cdots > H_p = 1$ satisfy the same two condns.
Then $n = p$ and $\exists$ bijection $\phi : \{1, \ldots, n\} \to \{1, \ldots, p\}$ s.t. $\forall i$

$$\frac{G_{i-1}}{G_i} \cong \frac{H_{\phi(i)-1}}{H_{\phi(i)}}.$$

Moral: Every finite group is made up of simple groups in an essentially unique way.

These simple gps are the composition factors of G.

Introducing $\mathrm{PSL}_d(q)$

Let $d \geq 2$, q be a prime power, $\mathbb{F}_q$ be the field of order q, $V = \mathbb{F}_q^d$.

Defn: $\mathrm{GL}_d(q) = \{$invertible $d \times d$ matrices over $\mathbb{F}_q\}$, the general linear group.

The determinant map is a homom from $\mathrm{GL}_d(q)$ to $\mathbb{F}_q^*$, the multiplicative group of $\mathbb{F}_q$.
The kernel is the determinant 1 matrices: $\mathrm{SL}_d(q)$, the special linear group.

Lemma 3
The center of $\mathrm{GL}_d(q)$ is $Z(\mathrm{GL}_d(q)) = \{\lambda I_d \ : \ \lambda \in \mathbb{F}_q^*\}$.

Defn: The projective special linear group is
$\mathrm{PSL}_d(q) := \frac{\mathrm{SL}_d(q)}{\mathrm{SL}_d(q) \cap Z(\mathrm{GL}_d(q))}$.

Theorem 4
$\mathrm{PSL}_d(q)$ is simple if $d > 2$ or $q > 3$.

The classification of finite simple groups

S – finite simple group. Then S is one of the following:

1. C_p for some prime p.
2. A_n for $n \geq 5$.
3. A classical group: $\mathrm{PSL}_d(q)$, $\mathrm{PSU}_d(q)$, $\mathrm{PSp}_d(q)$, $\mathrm{P\Omega}_d^\varepsilon(q)$, $\varepsilon \in \{+, -, \circ\}$.
4. An exceptional group: $\mathrm{E}_n(q)$ $n \in \{6, 7, 8\}$, $\mathrm{F}_4(q)$, $\mathrm{G}_2(q)$, ${}^2\mathrm{B}_2(q)$, ${}^3\mathrm{D}_4(q)$, ${}^2\mathrm{E}_6(q)$, ${}^2\mathrm{F}_4(q)$, ${}^2\mathrm{G}_2(q)$, ${}^2\mathrm{F}_4(2)'$.
5. One of 26 sporadic simple groups.

Cases 3 and 4 are the groups of Lie type:

- q is a prime power;
- some restrictions on d and q for existence and simplicity;
- constructions are related to, but fiddlier than, $\mathrm{PSL}_d(q)$.

Not all of these groups are pairwise non-isomorphic; e.g. $\mathrm{PSL}_2(9) \cong \mathrm{A}_6$.

Groups of automorphisms

Defn: An automorphism of a group G is an isomorphism $\phi : G \to G$.
$\mathrm{Aut}(G)$ is the set of all automorphisms of G.

Lemma 5
$\mathrm{Aut}(G)$ *forms a group under composition of maps.*

Proof.
$\mathrm{Aut}(G) \subset \mathrm{Sym}(G)$; only need to prove is a subgroup.

Products: Let $\alpha, \beta \in \mathrm{Aut}(G)$. Then
$(gh)(\alpha\beta) = ((gh)\alpha)\beta = ((g\alpha)(h\alpha))\beta = (g(\alpha\beta))(h(\alpha\beta))$, so
$\alpha\beta \in \mathrm{Aut}(G)$.

Inverses: Inverse of an isom is an isom. $\square$

Example 6
Let $G = C_p$. Then $\mathrm{Aut}(G) \cong C_{p-1}$.

Types of automorphisms, and almost simple groups

Defn: Let $g \in G$. The map $c_g : G \to G$, $x \mapsto g^{-1}xg$ is an inner automorphism of G.

Lemma 7

1. $\mathrm{Inn}(G) := \{c_g : g \in G\} \trianglelefteq \mathrm{Aut}(G)$.
2. $\mathrm{Inn}(G) \cong G/Z(G)$.

Corollary 8

If G is nonabelian simple, then $G \cong \mathrm{Inn}(G)$.

Defn: G is almost simple if there exists a nonabelian simple group S s.t. $S \cong \mathrm{Inn}(S) \trianglelefteq G \leq \mathrm{Aut}(S)$. S is the socle of G.

Defn: The outer automorphism group of G is $\mathrm{Out}(G) := \mathrm{Aut}(G)/\mathrm{Inn}(G)$.

Health warnings: (a) Elts of $\mathrm{Out}(G)$ are not automorphisms!
(b) Often refer to elts of $\mathrm{Aut}(G) \setminus \mathrm{Inn}(G)$ as outer automorphisms.

Extensions and semi-direct products

G – group, $1 < N \lhd G$. If $G/N \cong H$ then G is an extension of N by H. Write $G = N.H$.

Internal semi-direct product

G – group s.t. $\exists\ 1 < N \lhd G$ and $1 < H < G$ s.t.

- $N \cap H = 1$
- $HN = G$.

Then G is a semi-direct product or split extension of N by H.
Write $G = N : H$
Notice: $n_1 h_1 \cdot n_2 h_2 = n_1 h_1 n_2 h_1^{-1} h_1 h_2 = n_1 n_2^{h_1^{-1}} h_1 h_2$.

External construction

N, H – groups. $\phi : H \to \mathrm{Aut}(N)$ homom.The semi-direct product of N by H w.r.t. ϕ is $\{(n, h)\ :\ n \in N, h \in H\}$ with product $(n_1, h_1)(n_2, h_2) = (n_1(n_2(h_1^{-1}\phi)), h_1 h_2)$.

If $1 < N \lhd G$ and $G/N \cong H$ but $\nexists K \leq G$ with $K \cong H$ and $K \cap N = 1$ then G is a non-split extension of N by H.

Maximal subgroups

Theorem 9 (Ashbacher-Scott, very roughly)

To describe the maximal subgroups of a finite group G, it suffices to know:

1. *The maximal subgps of the almost simple gps whose socles are composition factors of G.*
2. *The solution to the extension problem for various gps occurring in G: given gps N and H, determine all extensions of N by H.*

Group actions and permutation groups

Defn: An action of a gp G on a nonempty set Ω is a function $\Omega \times G \to \Omega$, $(\alpha, g) \mapsto \alpha^g$ s.t. for all $\alpha \in \Omega$, $g, h \in G$
(A1) $\alpha^{(gh)} = (\alpha^g)^h$; and
(A2) $\alpha^{1_G} = \alpha$.
Usually denote gp actions by conjugation.

Example 10

The symmetric gp S_n naturally acts on $\underline{n} = \{1, \ldots, n\}$.
Any gp G acts on itself by conjugation: $x^g = g^{-1}xg$.

Defn: A permutation representation is a homomorphism $\theta : G \to \mathrm{Sym}(\Omega)$ for some Ω. A permutation group is a subgp of S_n for some n.

Example 11

The map $G \to \mathrm{Inn}(G) \leq \mathrm{Sym}(G)$, $g \mapsto c_g$ is a perm rep.

Equivalence of actions and perm reps

Lemma 12

Group actions are in natural bijection with perm reps.

Proof.

Given $\theta : G \to \mathrm{Sym}(\Omega)$, define an action of G on Ω by $\alpha^g = \alpha^{(g\theta)}$.
(A1) $\alpha^{(gh)} = \alpha^{((gh)\theta)} = \alpha^{(g\theta)(h\theta)} = (\alpha^{g\theta})^{h\theta} = (\alpha^g)^h$.
(A2) $\alpha^{1_G} = \alpha^{1\theta} = \alpha^{1_{\mathrm{Sym}(\Omega)}} = \alpha$.

Conversely, given an action of G on Ω, define $\theta : G \to \mathrm{Sym}(\Omega)$ by $\alpha^{g\theta} = \alpha^g$ for all $\alpha \in \Omega$.

These two operations are mutually inverse. $\square$

Defn: An action/perm rep of G is faithful if the only elt of G to fix all points of Ω is 1_G.

Example 13

The action of S_n on $\{\{\alpha, \beta\} : \ \alpha, \beta \in \underline{n}\}$ is faithful if $n > 2$.
The conjugation action of G on itself has kernel $Z(G)$. So action is not faithful iff $Z(G) \neq 1 \neq G$.

Orbits

These defns apply to actions, perm reps and perm gps.

Defn: The orbit of $\alpha \in \Omega$ under G is $\alpha^G = \{\alpha^g \ : \ g \in G\}$.

Lemma 14

Let $\beta, \gamma \in \alpha^G$. Then $\exists\, x \in G$ s.t. $\beta^x = \gamma$. Hence orbits partition Ω.

Proof.

$\exists\, g, h \in G$ s.t. $\alpha^g = \beta$, $\alpha^h = \gamma$. Then
$\beta^{g^{-1}h} = (\beta^{g^{-1}})^h = ((\alpha^g)^{g^{-1}})^h = (\alpha^{gg^{-1}})^h = \alpha^h = \gamma$. $\square$

Defn: If G has a single orbit on Ω then G is transitive; otherwise G is intransitive.

Example 15

If $n \geq 3$ then for $1 \leq k \leq n$, A_n is transitive on k-subsets of $\underline{n}$.
Gp G with conjugation action is intransitive iff $G \neq 1$: orbits are conjugacy classes.

Stabilisers

Defn: Let G act on Ω and $\alpha \in \Omega$. The stabiliser in G of α is

$$G_\alpha = \{g \in G \ : \ \alpha^g = \alpha\}.$$

Exercise

(i) G_α is a subgp of G. (ii) Let $\beta = \alpha^g$. Then $G_\beta = G_\alpha^g$. Hence if G is transitive then all point stabilisers are conjugate in G.

Let $H \leq G$, with $H = Hg_1, Hg_2, \ldots, Hg_n$ the right cosets of H in G. The right coset action of G on H is

$$(Hg_i)^g = Hg_i g.$$

Lemma 16

The right coset action of G on H is transitive, with point stabilisers $\{H^g \ : \ g \in G\}$. The kernel of the action is $\cap_{g \in G} H^g$.

Hence there is a natural correspondence between transitive actions and conjugacy classes of subgps.

The orbit-stabiliser theorem

Theorem 17 (The orbit-stabiliser thm)

Let $G \leq \mathrm{Sym}(\Omega)$, $\alpha \in \Omega$. *Then* $|\alpha^G| = |G : G_\alpha|$.
So G *transitive* $\Rightarrow |G : G_\alpha| = |\Omega|$.

Proof.

$\alpha^x = \alpha^y$ iff $\alpha^{xy^{-1}} = \alpha$ iff $xy^{-1} \in G_\alpha$ iff $G_\alpha x = G_\alpha y$.
Hence there is a natural bijection $\alpha^G \leftrightarrow \{G_\alpha g \ : \ g \in G\}$. □

Defn: G is regular if G is transitive and $G_\alpha = 1$.

Corollary 18

If $G \leq \mathrm{Sym}(\Omega)$ *is regular then* $|G| = |\Omega|$.

Lemma 19

If $G \leq \mathrm{Sym}(\Omega)$ *and* $N \trianglelefteq G$ *then* G *permutes the orbits of* N.

Proof.

Let $\beta \in \alpha^N$. Then $\exists\ n \in N$ s.t. $\beta = \alpha^n$. Then $\beta^g = (\alpha^n)^g$
$= \alpha^{gn_1} \in (\alpha^g)^N$, so $(\alpha^N)^g \subseteq (\alpha^g)^N$. Converse similar. □

Maximal subgroups of almost simple groups

G – almost simple, socle T. Let $M \leq_{\max} G$.

One of the following occurs:

1. $T \cap M = T$. Trivial maximal.
2. $T \cap M \leq_{\max} T$. Ordinary maximal.
3. $T \cap M \leq_{\text{non}-\max} T$. Novelty maximal.

The trivial maximals of G can be found by calculating the maximal subgps of G/T.

Theorem 20

Let $M \leq_{\max} G$. Then $M \cap T \neq 1$.

Hence M – ordinary or novelty maximal of G, $H := T \cap M \neq 1$.
Then $H \trianglelefteq M$ and by Thm 20 H is not normal in G, so
$M = N_G(H)$.
Also, $M \leq_{max} G \Rightarrow TM = G \Rightarrow M/(M \cap T) \cong \cong TM/TG/T$.

How to determine maximal subgroups

Work is to find ordinary and novelty maximals: $M \leq_{\max} G$ s.t. $M = N_G(M \cap T)$ and $M/(M \cap T) \cong G/T \leq \mathrm{Out}(T)$.

- Classify (possibly only roughly) all subgps of some gp S closely related to T.
  (S chosen to be as easy to work with as possible).
- Deduce information about all conjugacy classes of subgps in T.
- $\mathrm{Out}(T)$ acts on conjugacy classes of subgps of T.
- Stabiliser in $\mathrm{Out}(T)$ of a conjugacy class of subgps corresponds to normaliser in $\mathrm{Aut}(T)$ of a subgp in that class.
- Deduce ordinary and novelty maximal subgps of G.

Centralisers in the symmetric group

Theorem 21

$G \leq \mathrm{Sym}(\Omega)$, transitive. $C := C_{\mathrm{Sym}(\Omega)}(G)$. Then $C_\alpha = 1$ for all $\alpha \in \Omega$, and $C \cong N_G(G_\alpha)/G_\alpha$.

Proof.

Identify Ω with $\{G_\alpha g \ : \ g \in G\}$, let $H := G_\alpha$.
Let $K = N_G(H)$. Define action λ of K on Ω by $(Hg)^{k\lambda} = Hk^{-1}g$.

$\ker(\lambda) = H$, $\mathrm{im}(K) \cong K/H$. Because $Hk^{-1}g = Hg$ for some $g \in G$ iff $k^{-1} \in H$ iff $Hk^{-1}g = Hg \ \forall g \in G$.

$K\lambda \leq C$. Let $x \in G$, $y \in K$. Then for all $Hg \in \Omega$
$Hg^{x(y\lambda)} = Hy^{-1}gx = Hg^{(y\lambda)x}$.

$C \leq K\lambda$. Let $c \in C$, pick $z \in G$ s.t. $\alpha^c = \alpha^z$. Then $H^c = Hz$. Then for all $Hg \in \Omega$, $(Hg)^c = H^{gc} = H^{cg} = Hzg$. If $g \in H$ then $Hz = H^c = (Hg)^c = Hzg$. So $zgz^{-1} \in H$, so $z \in N_G(H)$, and $c = (z^{-1})\lambda$. □

Exercises on Lecture 1

1. Find a nonabelian gp with two different composition series.
2. Prove that $Z(\mathrm{GL}_d(q))$ is the set of scalar matrices.
3. Show that the following hold: (i) $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$.
(ii) $\mathrm{Inn}(G) \cong G/Z(G)$.
4. Show that $\mathrm{S}_n \cong \mathrm{A}_n : C_2$, and that $\mathrm{A}_4 \cong V_4 : C_3$. Show that Q_8 is not a split extension.
5. Finish the proof of Lemma 12: check $g\theta \in \mathrm{Sym}(\Omega)$ and that θ is a homom.
6. Let $G \leq \mathrm{Sym}(\Omega)$ and $\alpha \in \Omega$. Show that (i) G_α is a subgp of G. (ii) Let $\beta = \alpha^g$. Then $G_\beta = G_\alpha^g$. (iii) If G is transitive then the point stabilisers form a complete conjugacy class of subgps of G.
7. Let G act on the set of its subgps by conjugation. What is the stabiliser of $H \leq G$? Deduce that $|\{H^g : x \in G\}| \mid |G|$.
8. Let $\alpha \in \mathrm{Aut}(G)$, and let C be a conjugacy class of elements of G or of subgps of G. Show that (i) C^α is a conjugacy class of (elements or subgps of) G. (ii) If $C^\alpha = C$ and $X \in C$ then there exists $g \in G$ s.t. $X^{\alpha c_g} = X$.