# NZMRI Summer School
# The symmetric and alternating groups

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

School of Mathematics and Statistics, University of St Andrews

Nelson, 9 January 2018

University of St Andrews

# Introduction

Theorem 22

*The alternating group $\mathrm{A}_n$ is nonabelian simple iff $n \geq 5$.*

This lecture: Understand the subgp structure of the almost simple gps with socle $\mathrm{A}_n$.

- Determine $\mathrm{Out}(\mathrm{A}_n)$.
- Then for each $G$ s.t. $\mathrm{A}_n \trianglelefteq G \leq \mathrm{Aut}(\mathrm{A}_n)$, find maximal subgps of $G$.

# Low-index subgroups

## Lemma 23

*Let $n \geq 5$ and $1 < k < n$. Then $\mathrm{A}_n$ has no subgp of index $k$.*

## Proof.

Suppose $\exists\ H < \mathrm{A}_n$, index $k$.
The right coset action of $\mathrm{A}_n$ on $H$ is a transitive action on $k$ points, so induces a homom $\Psi : \mathrm{A}_n \to \mathrm{S}_k$.
$n > 2 \Rightarrow |\mathrm{A}_n| = n!/2 > k!$, so $\Psi$ not an isom.
Thm 22: $\mathrm{A}_n$ is simple. So $\ker\Psi = \mathrm{A}_n$, a contradiction. □

## Theorem 24

*Let $n \geq 4$. Then* $\mathrm{Aut}(\mathrm{A}_n) \cong \mathrm{S}_n$*, except* $\mathrm{Aut}(\mathrm{A}_6) \cong \mathrm{A}_6.2^2$.

We first prove:

## Lemma 25

*Let $n \geq 9$. If $H \leq \mathrm{A}_n$ and $\theta : \mathrm{A}_{n-1} \to H$ is an isom, then $H = (\mathrm{A}_n)_\alpha$ for some $\alpha \in \underline{n}$.*

## $n \geq 9$, $H \leq \mathrm{A}_n$, $H \cong \mathrm{A}_{n-1} \Rightarrow H = (\mathrm{A}_n)_\alpha$

$n > 4$, so Lemma 23 $\Rightarrow$ $H$ has no nontriv orbit length $< n-1$.
So if $H$ is *not* a point stab, then $H$ is transitive.

Claim: $\theta$ maps 3-cycles to 3-cycles Let $g \in H$ s.t. $g = (1\ 2\ 3)\theta$.
Then $g$ centralises a subgp $K$ of $H$ s.t. $K \cong \mathrm{A}_{n-4}$.
$n - 4 \geq 5 \Rightarrow K$ has an orbit $\alpha^K$ s.t. $|\alpha^K| = m \geq n - 4$.

$|K : K_\alpha| = m$, so if $N_K(K_\alpha) \neq K_\alpha$ then $K$ has a subgp of index $\leq m/2 \leq n/2 < n - 4$, a contradiction. Hence $N_K(K_\alpha) = K_\alpha$.

Thm 21: $G \leq \mathrm{Sym}(\Omega)$, transitive. $C_{\mathrm{Sym}(\Omega)}(G) \cong N_G(G_\alpha)/G_\alpha$.

So $C_{\mathrm{Sym}(\alpha^K)}(K) = 1$. Hence $g$ moves $\leq 4$ points in $\underline{n}$.
Also, $|g| = 3$ so $g = (a\ b\ c)$ is a 3-cycle.

Claim: $H$ generated by 3-cycles with a common fixed point
Let $X = \{(1, 2, i) \ : \ 3 \leq i \leq n-1\} \subseteq \mathrm{A}_{n-1}$. Let $x, y \in X$. Then $\langle x, y \rangle \cong \mathrm{A}_4 \cong \langle x\theta, y\theta \rangle$. So each 3-cycle in $X\theta$ is $(a, b, j)$, for distinct $j$.

$\langle X \rangle = \mathrm{A}_{n-1}$, so $H = \langle X\theta \rangle$ fixes exactly one point in $\underline{n}$. $\square$

# Aut($\mathrm{A}_n$), ctd

**Proof of Theorem 24, $n \geq 9$**

Let $\phi \in \mathrm{Aut}(\mathrm{A}_n)$.
Then $\phi$ acts on $\mathcal{S} = \{H \leq \mathrm{A}_n \ : \ H \cong \mathrm{A}_{n-1}\}$.
By Lemma 25, each such $H$ is a point stabiliser in the natural action, so $|\mathcal{S}| = n$.
Hence $\phi$ induces $\sigma \in \mathrm{S}_n$. But $\sigma$ completely determines the action of $\phi$ on $\mathrm{A}_n$, so $\phi \in \mathrm{S}_n$. □

- $n = 4, 5, 7, 8$: Exercise.
- $\mathrm{A}_6 \cong \mathrm{PSL}_2(9)$, easier to understand automorphisms that way: Lecture 3.

# Intransitive groups

Let $H \leq \mathrm{S}_n$, $n \geq 5$.
Is $H$ transitive?
If not, let $\Delta = \alpha^H \subset \underline{n}$, and $k := |\Delta| < n$.

## Lemma 26

*Up to $\mathrm{A}_n$-conjugacy $H \leq \mathrm{S}_k \times \mathrm{S}_{n-k}$ with orbits $\underline{k}$ and $X := \{k+1, \ldots, n\}$.*

## Proof.

Example 15: $\mathrm{A}_n$ is transitive on $k$-subsets of $\underline{n}$.
So $\exists\ \tau \in \mathrm{A}_n$ s.t. $\Delta^\tau = \underline{k}$. Then
$\underline{k}^{H^\tau} = \underline{k}^{\tau^{-1}H\tau} = \Delta^{H\tau} = \Delta^\tau = \underline{k}$. □

## Corollary 27

*If an intransitive subgp of $X = \mathrm{A}_n$ or $\mathrm{S}_n$ is maximal, it is of the form $X \cap (\mathrm{S}_k \times \mathrm{S}_{n-k})$.*

# Intransitive maximal subgroups

**Theorem 28**

*The intransitive maximal subgroups of* $\mathrm{S}_n$, $n \geq 5$, *are* $\mathrm{S}_k \times \mathrm{S}_{n-k}$ *for* $1 \leq k < n/2$.

**Proof.**

Let $H = \mathrm{S}_k \times \mathrm{S}_{n-k}$ for $k < n/2$.

Let $g \in \mathrm{S}_n \setminus H$, and $G = \langle H, g \rangle$. We show $G = \mathrm{S}_n$.

$g \notin H$ so $X^g \cap \underline{k} \neq \emptyset$. Since $k < n/2$, $X^g \neq \underline{k}$.

Let $i, j \in X$ s.t. $i^g \in \underline{k}$, $j^g \in X$.
Then $(i\ j) \in H$, so $\sigma := (i\ j)^g = (i^g, j^g) \in G$.

$I := \{\sigma^\tau \ : \ \tau \in \mathrm{S}_k\} = \{(z\ j^g) \ : \ 1 \leq z \leq k\} \subset G$.
$\{\mu^\tau \ : \ \mu \in I,\ \tau \in \mathrm{S}_{n-k}\} = \{(a\ b) \ : \ a \in \underline{k}, b \in X\} \subset G$.
So $(a\ b) \in G$ for all $a, b \in \underline{n}$, and $G = \mathrm{S}_n$. □

# Imprimitivity

Defn: $H \le \mathrm{S}_n$, transitive. If $\exists\ \Delta \subset \underline{n}$ with $1 < |\Delta| < n$ s.t. for each $h \in H$ either $\Delta^h = \Delta$ or $\Delta^h \cap \Delta = \emptyset$ then $\Delta$ is a block for $H$, and $H$ is imprimitive.

$\{\Delta^h\ :\ h \in H\}$ is a system of imprimitivity. Each $\Delta^h$ is a block, and $\cup_{h\in H}\Delta^h = \underline{n}$, so blocks partition $\underline{n}$ into equal size parts.

If $G$ is transitive and not imprimitive then $G$ is primitive.

## Example 29

$C_6 = \langle(1\ 2\ \ldots\ 6)\rangle$. One system of imprimitivity is $\{\{1,4\},\{2,5\},\{3,6\}\}$, so $C_6$ is imprimitive.
Another is $\{\{1,3,5\},\{2,4,6\}\}$: systems of imprimitivity are not unique.

Consider $C_p$ acting on $p$ points, some prime $p$. Then size of a block divides $|\Omega| \Rightarrow C_p$ is primitive.

# Imprimitive wreath products

Defn: $H$ – group, $G \leq \mathrm{S}_d$. The wreath product $H \wr G$ is the semidirect product $H^d : G$, where $(h_1, \ldots, h_d)^{g^{-1}} = (h_{1^g}, \ldots, h_{d^g})$. That is

$(h_{11}, \ldots, h_{1d})g_1(h_{21}, \ldots, h_{2d})g_2 = (h_{11}h_{21^{g_1}}, \ldots, h_{1d}h_{2d^{g_1}})g_1g_2$.

Theorem 30

*$H \leq \mathrm{Sym}(\Delta)$, $G \leq \mathrm{S}_d$ both transitive. There is an imprimitive action of $H \wr G$ on $\Delta \times \underline{d}$:* $(\alpha, i)^{(h_1,\ldots,h_d)g} = (\alpha^{h_i}, i^g)$.

Proof.

A1 $((\alpha, i)^{(h_{11},\ldots,h_{1d})g_1})^{(h_{21},\ldots,h_{2d})g_2} = (\alpha^{h_{1i}}, i^{g_1})^{(h_{21},\ldots,h_{2d})g_2}$

$= (\alpha^{h_{1i}h_{2i^{g_1}}}, i^{g_1g_2}) = (\alpha, i)^{(h_{11}h_{21^{g_1}},\ldots,h_{1d}h_{2d^{g_1}})g_1g_2}$

A2 $(\alpha, i)^{(1_H,\ldots,1_H)1_G} = (\alpha^{1_H}, i^{1_G}) = (\alpha, i)$.

Transitive: Let $\alpha, \beta \in \Delta$, $i, j \in \underline{d}$. Then $\exists h \in H$ s.t. $\alpha^h = \beta$ and $\exists g \in G$ s.t. $i^g = j$. Then $(\alpha, i)^{(h,h,\ldots,h)g} = (\alpha^h, i^g) = (\beta, j)$.

Blocks are $\{(\alpha, i) \ : \ \alpha \in \Delta\}$, for $i \in \underline{d}$. □

# Maximal imprimitive subgroups

## Lemma 31

*$G \leq \mathrm{S}_n$ imprimitive, blocks size $k$.*
*Up to $\mathrm{A}_n$-conjugacy $G \leq \mathrm{S}_k \wr \mathrm{S}_{n/k}$ with blocks*
*$B_a := \{(a-1)k+1, \ldots, ak\}$ for $1 \leq a \leq n/k$.*

## Proof.

Can conjugate $G$ in $\mathrm{A}_n$ to yield blocks $B_1, \ldots, B_{n/k}$.
If $\sigma \in \mathrm{S}_n$ preserves $\{B_1, \ldots, B_{n/k}\}$, can write $\sigma = \mu\tau_1 \ldots \tau_{n/k}$,
where $\mu$ permutes the subscripts on the $B_i$ but sends
$i_1k + j \mapsto i_2k + j$, for all $i_1, j$, and $\tau_i \in \mathrm{Sym}(B_i)$. $\mu \leftrightarrow \mu' \in \mathrm{S}_{n/k}$,
$\mathrm{Sym}(B_i) \cong \mathrm{S}_k$, so $\sigma \in \mathrm{S}_k \wr \mathrm{S}_{n/k}$. □

## Theorem 32

*$\mathrm{S}_k \wr \mathrm{S}_{n/k}$ is a maximal subgp of $\mathrm{S}_n$ for all proper nontrivial divisors $k$ of $n$.*

# Point stabilisers of primitive groups

$G$ – primitive. Then $G$ is not contained in any intransitive or imprimitive group.

### Lemma 33

*$G \leq \mathrm{S}_n$ – transitive. The gp $G$ is primitive iff $G_\alpha \leq_{\max} G$.*

### Proof.

$G$ imp $\Rightarrow$ $G_\alpha$ not maximal

$\Delta$ – block for $G$, s.t. $\alpha \in \Delta$. Let $H = \{g \in G \ : \ \Delta^g = \Delta\}$. Then $H \leq G$ and $H \neq G$. Also, if $g \in G_\alpha$ then $\alpha \in \Delta \cap \Delta^g$ so $\Delta = \Delta^g$ and $g \in H$. So $G_\alpha \leq H$. Let $\beta \in \Delta$, $\beta \neq \alpha$. Then $\exists\ g \in G$ with $\alpha^g = \beta$. Hence $\Delta^g = \Delta$, so $g \in H$. Hence $G_\alpha < H < G$.

$G_\alpha$ not maximal $\Rightarrow$ $G$ imprimitive.

Let $G_\alpha < H < G$. Then $|H : G_\alpha| < |G : G_\alpha| = |\Omega|$, so $H$ is intransitive. Let $\Delta = \alpha^H$, and let $g \in G$. If $g \in H$ then $\Delta^g = \Delta$. If $\Delta^g \cap \Delta \neq \emptyset$, then $\exists u, v \in H$ s.t. $\alpha^{ug} = \alpha^v$. Then $ugv^{-1} \in G_\alpha$, so $g \in u^{-1}G_\alpha v \subset H$. Hence $\Delta^g \cap \Delta \neq \emptyset \Rightarrow \Delta^g = \Delta$. □

# Primitive groups of affine type

$p$ – prime, $V = \mathbb{F}_p^d$.

Defn: The affine general linear group $\mathrm{AGL}_d(p)$ is $V : \mathrm{GL}_d(p) = \{(h, v) \ : \ v \in V, h \in \mathrm{GL}_d(p)\}$ with multiplication $(h_1, v_1)(h_2, v_2) = (h_1 h_2, v_1^{h_2} + v_2)$.

$\mathrm{AGL}_d(p)$ acts on $V$ via $v^{(h,w)} = vh + w$. Action is faithful, so $\mathrm{AGL}_d(p) \leq \mathrm{Sym}(V)$.
With this action, $V \cong \{(1, v) \ : \ v \in V\} \trianglelefteq \mathrm{AGL}_d(p)$ is regular.
$\mathrm{GL}_d(p)$ is the stabiliser of $\underline{0} \in V$.

Defn: A group of affine type is $G \leq \mathrm{S}_{p^d}$ s.t. $V \trianglelefteq G \leq \mathrm{AGL}_d(p)$.

**Lemma 34**

*$G$ – gp of affine type. $G$ is primitive iff $G_0$ is an irreducible subgroup of $\mathrm{GL}(V)$.*

**Example 35**

If $C_p \trianglelefteq G \leq \mathrm{AGL}_1(p) \cong C_p : C_{p-1} \leq \mathrm{S}_p$ then $G$ is primitive.

# Product action primitive groups

Let $H \leq \mathrm{Sym}(\Delta)$, $K \leq \mathrm{S}_d$. The product action of $G = H \wr K$ on $\Omega = \Delta^d = \{(\delta_1, \ldots, \delta_d) \;:\; \delta_i \in \Delta\}$ is:

$$\begin{aligned}(\delta_1, \ldots, \delta_d)^{(h_1, \ldots, h_d)k} &= (\delta_1^{h_1}, \ldots, \delta_d^{h_d})^k \\ &= (\delta_{1^{k^{-1}}}^{h_{1^{k^{-1}}}}, \ldots, \delta_{d^{k^{-1}}}^{h_{d^{k^{-1}}}})\end{aligned}$$

If $H$ is transitive then $H \wr K$ is transitive.
$(\alpha_1, \ldots, \alpha_d), (\beta_1, \ldots, \beta_d) \in \underline{k}^d$. Then $\forall i \; \exists \; h_i \in H$ s.t. $\alpha_i^{h_i} = \beta_i$.
Hence $(\alpha_1, \ldots, \alpha_d)^{(h_1, \ldots, h_d)1_K} = (\beta_1, \ldots, \beta_k)$.

### Theorem 36

*$G$ is primitive iff (i) $H$ is primitive and not regular on $\Delta$ and (ii) $K$ is transitive on $\underline{d}$.*

### Corollary 37

*$\mathrm{S}_k \wr \mathrm{S}_d$ is primitive in the product action on $\underline{k}^d$ for all $k \geq 3$.*

# Diagonal type groups

$T$ – nonabelian simple, $k \geq 2$.
$D = \{(t, t, \ldots, t) : t \in T\} \cong T \leq T^k$ – diagonal subgroup.
Right coset action of $T^k$ on $D$:
$\Omega = \{D(t_1, \ldots, t_k) = D(1, t_1^{-1}t_2, \ldots, t_1^{-1}t_k) \ : t_i \in T\}$.
Hence $n := |\Omega| = |T|^{k-1}$.
$k > 2 \Rightarrow D$ not maximal $\Rightarrow T^k$ not primitive.

**Theorem 38**
$N_{\mathrm{S}_n}(T^k) = T^k.(\mathrm{Out}(T) \times \mathrm{S}_k) \cong (T \wr \mathrm{S}_k).\mathrm{Out}(T) = \{(s_1, \ldots, s_k)\sigma \ : \ s_i \in \mathrm{Aut}(T), \sigma \in \mathrm{S}_k, \mathrm{Inn}(T)s_i = \mathrm{Inn}(T)s_j \ \forall i, j\}$.

**Defn:** If $G \leq \mathrm{S}_{|T|^{k-1}}$ with $T^k \trianglelefteq G \leq T^k.(\mathrm{Out}(T) \times \mathrm{S}_k)$ and $\mathrm{Inn}(T) \leq G_\alpha \leq \mathrm{Aut}(T) \times \mathrm{S}_k$ then $G$ is a group of diagonal type.

**Theorem 39**
*$G$ is primitive iff either $k = 2$ or $k > 2$ and the action of $G$ by conjugation on direct factors $\{T_1, \ldots, T_k\}$ of $T^k$ is primitive.*

# The maximal subgroups of $\mathrm{A}_n$ and $\mathrm{S}_n$

Theorem 40 (O'Nan–Scott + Liebeck–Praeger–Saxl)

*$H < X = \mathrm{A}_n$ or $\mathrm{S}_n$, $n \geq 5$. Up to $\mathrm{S}_n$-conjugacy, $H$ is a subgp of one of the following groups $G < X$.*

1. *$G = (\mathrm{S}_k \times \mathrm{S}_{n-k}) \cap X$ with $k \neq n/2$. $G \leq_{\max} X$.*
2. *$G = \mathrm{S}_k \wr \mathrm{S}_{n/k} \cap X$, with $1 < k < n$. $G \leq_{\max} X$ except when $X = \mathrm{A}_8$, $k = 2$.*
3. *$G = \mathrm{AGL}_k(p) \cap X$. $G \leq_{\max} \mathrm{A}_n G$, except when $X = \mathrm{A}_n$ and $n \in \{7, 11, 17, 23\}$.*
4. *$G = (T^k.(\mathrm{Out}(T) \times \mathrm{S}_k)) \cap X$ , with $n = |T|^{k-1}$. $G \leq_{\max} \mathrm{A}_n G$.*
5. *$G = (\mathrm{S}_m \wr \mathrm{S}_k) \cap X$, with $m \geq 5$, $k \geq 2$, product action. $G \leq_{\max} \mathrm{A}_n G$ except when $X = \mathrm{A}_n$ and $G$ is imprimitive.*
6. *$S \trianglelefteq H \leq G \leq \mathrm{Aut}(S)$ is a primitive almost simple group.*

# The almost simple maximals of $\mathrm{A}_n$ and $\mathrm{S}_n$

Liebeck, Praeger and Saxl classified the non-maximal cases when $G$ is almost simple.

To determine the explicit list of maximals for a given $n$:

- For the gps $G$ on the previous slide, determine which exist.
- If $\mathrm{A}_n G = \mathrm{S}_n$ then get one class of $G$ in $\mathrm{S}_n$, and one class of $G \cap \mathrm{A}_n$ in $\mathrm{A}_n$.
- If $N_{\mathrm{S}_n}(G) < \mathrm{A}_n$ then get two classes of $G$ in $\mathrm{A}_n$.
- Find the almost simple primitive groups $G \leq \mathrm{S}_n$.
- Sort them by their socles $S$. Eliminate the non-maximals by LPS. Determine conjugacy as above.

**Theorem 41 (CMRD 05)**

*The maximal subgps of $\mathrm{A}_n$ and $\mathrm{S}_n$ are known for $n \leq 2500$.*

**Theorem 42 (Coutts, Quick & CMRD 2011)**

*The primitive gps of degree less than 4095 are known.*

# An example: $A_8$ and $S_8$

**Maximal subgroups**

| Order | Index | Structure | | G.2 |
|---|---|---|---|---|
| 2520 | 8 | $A_7$ | : | $S_7$ |
| 1344 | 15 | $2^3{:}L_3(2)$ | ⎤ | $2^4{:}S_4$, |
| 1344 | 15 | $2^3{:}L_3(2)$ | ⎦ | $L_3(2){:}2$ |
| 720 | 28 | $S_6$ | : | $S_6 \times 2$ |
| 576 | 35 | $2^4{:}(S_3 \times S_3)$ | : | $(S_4 \times S_4){:}2$ |
| 360 | 56 | $(A_5 \times 3){:}2$ | : | $S_5 \times S_3$ |

# Exercises on Lecture 2

1. Prove that $\mathrm{A}_n$ is simple for $n \geq 5$:
   1.1 Show that $\mathrm{A}_n$ is generated by the set of all 3-cycles.
   1.2 Show that any normal subgroup $1 \neq N \trianglelefteq \mathrm{A}_n$ contains a 3-cycle.
   1.3 Show that if $N$ contains one 3-cycle then $N$ contains all 3-cycles.
2. Prove Lemma 24 for $n = 7$ (easy), and $n = 8$ (a bit trickier). Hence prove Theorem 25 for $n \neq 6$.
3. Prove that if $n = 2m$ then the natural intransitive action of $\mathrm{S}_m \times \mathrm{S}_m$ is not a maximal subgroup of $\mathrm{S}_n$.
4. Show that $\mathrm{S}_k \wr \mathrm{S}_m$ is maximal in $\mathrm{S}_{km}$ for all $k, m \geq 2$. [Hint: consider $m = 2$ first. Mimic proof of Thm 28].
5. Verify that the given action of $\mathrm{AGL}_d(p)$ is an action, and that $V$ is a regular normal subgroup.
6. Verify that the product action of a wreath product is an action.
7. Verify that the group $T^k.(\mathrm{Out}(T) \times \mathrm{S}_k)$ is primitive.