8th PhD Summer School in Discrete Maths
Finite Permutation Groups
Lecture 4: The O'Nan–Scott Theorem & Applications

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

Rogla, 5 July 2018

University
of

§9: Primitive groups with non-regular socles

Product action wreath products

Theorem 20

Let $G = B \wr A$, where B acts on Δ, with $|\Delta| < \infty$, and A acts on $\underline{n}$. Then G acts on $\Delta^n = \{(\delta_1, \ldots, \delta_n) \ : \ \delta_i \in \Delta\}$ via

$$\begin{aligned}(\delta_1, \ldots, \delta_n)^{(b_1, \ldots, b_n)a} &= (\delta_1^{b_1}, \ldots, \delta_n^{b_n})^a \\ &= (\delta_{1^{a^{-1}}}^{b_{1^{a^{-1}}}}, \ldots, \delta_{n^{a^{-1}}}^{b_{n^{a^{-1}}}})\end{aligned}$$

Defn: This action of $B \wr A$ is the product action.

Theorem 21

Let $G = B \wr A$, with the product action.

1. *G is faithful iff the actions of A and B are both faithful.*
2. *G is primitive iff B is primitive and not regular, and A is transitive.*

The diagonal action

Let T be a non-abelian finite simple group, let $m \geq 2$.

Defn: The diagonal subgroup $D \leq T^m$ is $\{(t, \ldots, t) \; : \; t \in T\}$.

The right coset action of T^m on $D \cong T$ gives a permutation representation $\rho_D : T^m \to \mathrm{Sym}(T^{m-1})$.
Denote $D(t_1, \ldots, t_n)$ by $[t_1, \ldots, t_n] = [t_n^{-1} t_1, \ldots, t_n^{-1} t_{n-1}, 1]$.

Lemma 22
ρ_D is faithful and transitive.

Theorem 23
Let $H = T^m \rho_D \leq \mathrm{Sym}(T^{m-1})$. Let $N = N_{\mathrm{Sym}(T^{m-1})}(H)$. Then

(i) *there exists $W \trianglelefteq N$ with $W \cong T \wr \mathrm{S}_m$;*

(ii) *$N/W \cong \mathrm{Aut}(T)/\mathrm{Inn}(T) = \mathrm{Out}(T)$.*

Primitive groups of diagonal type

Defn: $G \leq \mathrm{Sym}(\Omega)$ is a group of diagonal type if there exists a non-abelian simple T, and an integer $m \geq 2$, s.t.

- up to perm isom, $G \leq (T \wr \mathrm{S}_m).(\mathrm{Aut}(T)/\mathrm{Inn}(T))$, with $\Omega = \{[t_1, \ldots, t_n] \ : \ t_i \in T\}$;
- the base group $T^m \trianglelefteq G$.

Theorem 24

A group G of diagonal type is primitive iff either

(i) $m = 2$; *or*

(ii) $m \geq 3$ *and the conjugation action of G on the set $\{T_1, \ldots, T_m\}$ of minimal normal subgroups of T^m is primitive.*

§10: The O'Nan–Scott Theorem

The O'Nan-Scott Theorem

Let G be a primitive group of degree n, with socle H. Then $H \cong T^m$ for some simple T and $m \geq 1$. The group G is perm isom to one of the following groups U.

1. H is regular and one of the following happens:
   1.1 T is abelian. Then $H \cong (\mathbb{F}_p^m, +)$, $n = p^m$, $U \leq \mathrm{AGL}_d(p)$. Affine type
   1.2 T is non-abelian. Then $m \geq 6$. Twisted wreath
2. H is not regular. Then T is non-abelian and one of the following happens:
   2.1 $H = T$, so $m = 1$, and $T \trianglelefteq U \leq \mathrm{Aut}(T)$, with U_α any maximal subgroup of U. Almost simple
   2.2 $m \geq 2$, $n = |T|^{m-1}$ and $T^m \trianglelefteq U \leq T^m.(\mathrm{S}_m \times \mathrm{Out}(T))$ with the diagonal action. Diagonal type
   2.3 $m = rs$ with $s > 1$, $n = d^s$, and there exists a primitive group K of degree d s.t. $T^m \trianglelefteq U \leq K \wr \mathrm{S}_s$ with the product action. The group K is almost simple or of diagonal type. Product action type

An example: S_8

Let $H \leq \mathrm{S}_8$. Then H can be:

- intransitive: stabilise a k-set for $1 \leq k \leq 3$;
- imprimitive: blocks size 2 or 4;
- $8 = 2^3$, so G can be an affine type subgroup of $\mathrm{AGL}_3(2)$.
- Almost simple: $\mathrm{PSL}_2(7)$, $\mathrm{PGL}_2(7)$, A_8, 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	$(A_5 \times 3){:}2$	: $S_5 \times S_3$

Application: Classifying primitive permutation groups

Two main tasks

1. Find the irreducible subgroups of $\mathrm{GL}_d(p)$, for the groups of affine type.
2. Find the almost simple primitive groups.

Theorem 25 (Bray, Holt, CMRD 13)

Let G be an almost simple group such that $Z.G$ has a faithful representation as a subgroup of $\mathrm{GL}_d(q)$ for $d \leq 12$, with Z being mapped to a subgroup of $Z(\mathrm{GL}_d(q))$. Then the maximal subgroups of G are known.

Theorem 26 (CMRD 05; Coutts, Quick & CMRD 11)

The primitive groups of degree up to 4095 are known.

Application: Random generation

Let x, y be chosen uniformly at random from A_n. What is the probability that $H = \langle x, y \rangle = \mathrm{A}_n$?

- If $H \neq \mathrm{A}_n$, then $\exists\, M \leq_{\max} \mathrm{A}_n$ s.t. $H \leq M$.
- $\mathbb{P}(x, y \in M) = 1/|\mathrm{A}_n : M|^2$.
- Hence
$$\mathbb{P}(H \neq \mathrm{A}_n) \leq \sum_{M \leq_{max} \mathrm{A}_n} \frac{1}{|\mathrm{A}_n : M|^2}.$$

Maximal subgroups of A_n: intransitive, transitive or primitive.

Theorem 27 (Liebeck 84)

Let $G \leq \mathrm{S}_n$ be primitive and almost simple. Then either $|G| < n^9$ or G is one of two specified families of permutation groups.

Can also bound the number of almost simple subgroups.

Theorem 28 (Morgan & CMRD '15)

$$1 - \frac{1}{n} - \frac{8.8}{n^2} \leq \mathbb{P}(H = \mathrm{A}_n) \leq 1 - \frac{1}{n} - \frac{0.93}{n^2}$$

§11: Some simple primitive groups

Some almost simple primitive groups

Theorem 29

A_n is simple for all $n \geq 5$.

Corollary 30

For $n \geq 5$, the action of A_n or S_n on the cosets of any maximal subgroup is an almost simple primitive group.

Defn: $\mathrm{SL}_d(q) \trianglelefteq \mathrm{GL}_d(q)$ is all matrices of determinant 1.

$\mathrm{GL}_d(q)$ and $\mathrm{SL}_d(q)$ act faithfully on vectors in $\mathbb{F}_q^d$.

- This action is intransitive: $0g = 0$ for all $g \in \mathrm{GL}_d(q)$.

$\mathrm{GL}_d(q)$ and $\mathrm{SL}_d(q)$ act transitively on all nonzero vectors in $\mathbb{F}_q^d$.

- If $q > 2$ then this action is imprimitive: let $v \in \mathbb{F}_q^d \setminus \{0\}$, and let $\lambda \in \mathbb{F}_q^*$. Then $(\lambda v)g = \lambda(vg)$, so $\langle v \rangle$ is a block.

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

Let $\Omega = \{\langle v \rangle \ : \ v \in \mathbb{F}_q^d \setminus \{0\}\}$ be the system of imprimitivity for this action of $\mathrm{GL}_d(q)$.
Then $\mathrm{GL}_d(q)$ and $\mathrm{SL}_d(q)$ act on Ω.

Lemma 31

1. $|\Omega| = (q^d - 1)/(q - 1)$.
2. *The kernel of the action of* $\mathrm{GL}_d(q)$ *is* $\{\lambda I_d \ : \ \lambda \in \mathbb{F}_q^*\} = Z(\mathrm{GL}_d(q))$.
3. *The action of* $\mathrm{SL}_d(q)$ *is* 2*-transitive, and hence primitive.*

Defn: $\mathrm{PSL}_d(q)$ is the image of $\mathrm{SL}_d(q)$ repn, so $\mathrm{PSL}_d(q) \leq \mathrm{Sym}(\Omega)$. $\mathrm{PGL}_d(q)$ is image of $\mathrm{GL}_d(q)$.

Theorem 32

The groups $\mathrm{PSL}_d(q)$ *are simple, except for* $\mathrm{PSL}_2(2) \cong \mathrm{S}_3$ *and* $\mathrm{PSL}_2(3) \cong \mathrm{A}_4$. $\mathrm{PSL}_d(q) \trianglelefteq \mathrm{PGL}_d(q)$.

Pairwise non-isomorphism

Theorem 33

The simple groups $\mathrm{PSL}_d(q)$ *are pairwise non-isomorphic, and are not isomorphic to the alternating groups, except for*

$$\begin{array}{c} \mathrm{PSL}_2(4) \cong \mathrm{PSL}_2(5) \cong \mathrm{A}_5, \\ \mathrm{PSL}_2(7) \cong \mathrm{PSL}_3(2), \\ \mathrm{PSL}_2(9) \cong \mathrm{A}_6, \quad \mathrm{PSL}_4(2) \cong \mathrm{A}_8 \end{array}.$$

Lemma 34

Let (a, b) *denote the greatest common divisor of* a *and* b*. Then*

$$|\mathrm{PSL}_d(q)| = \frac{1}{(q-1,d)} q^{d(d-1)/2} \prod_{i=2}^{d} (q^i - 1).$$

A faithful linear representation of $\mathrm{PSL}_2(7)$

Defn: Let $G \leq \mathrm{S}_n$. Then there is a faithful linear representation of G via permutation matrices; i.e. a homom $\rho_p : G \to \mathrm{GL}_n(q)$, $g \mapsto m$, where:

1. $m_{ij} \in \{0, 1\}$ for all i, j;
2. $m_{ij} = 1 \Leftrightarrow i^g = j$.

$\mathrm{SL}_2(7) = \langle a := \begin{pmatrix} 3 & 0 \\ 0 & 5 \end{pmatrix}, b := \begin{pmatrix} 6 & 1 \\ 6 & 0 \end{pmatrix} \rangle$.

Label the 1-dim subspaces of $\mathbb{F}_7^2$ by

$$\infty = \langle (0, 1) \rangle, i = \langle (1, i) \rangle \text{ for } 0 \leq i \leq 6.$$

$\mathrm{SL}_2(7)$ acts on $\Omega = \{\infty, 0, \ldots, 7\}$.
$\mathrm{PSL}_2(7) = \langle \overline{a} = (1\ 4\ 2)(3\ 5\ 6), \overline{b} = (\infty\ 6\ 0)(1\ 3\ 5) \rangle \leq \mathrm{Sym}(\Omega)$.

$v_\infty, v_0, v_1, \ldots, v_6$ – standard basis of $V = \mathbb{F}_2^8$.
Let $\rho_p : \mathrm{SL}_2(7) \to \mathrm{GL}_8(2)$ be rep via permutation matrices, then $\mathrm{Im}(\rho_p) = \mathrm{PSL}_2(7)$.

$\mathrm{PSL}_2(7) \cong \mathrm{PSL}_3(2)$

Let $v = (1, 1, \ldots, 1) \in V = \mathbb{F}_2^8$.
Let $U = \langle v, u_1 = \sum_{i=\infty,0,1,3} v_i, u_2 = \sum_{i=\infty,1,2,4} v_i,$
$u_3 = \sum_{i=\infty,2,3,5} v_i \rangle \leq V$.

Lemma 35
$v^{\mathrm{PSL}_2(7)} = v$ and $U^{\mathrm{PSL}_2(7)} = U$.

Proof.
Use $\mathrm{PSL}_2(7) = \langle (1\ 4\ 2)(3\ 5\ 6), (\infty\ 6\ 0)(1\ 3\ 5) \rangle$. $\square$

- So $\mathrm{PSL}_2(7)$ acts on $U/\langle v \rangle = \{u + \langle v \rangle \ : u \in U\}$, dimension 3.
- $\mathrm{PSL}_2(7)$ is simple and action is nontrivial so action is faithful.
- So $\mathrm{PSL}_2(7) \leq \mathrm{GL}_3(2) \cong \mathrm{PSL}_3(2)$.
- But $|\mathrm{PSL}_2(7)| = 168 = |\mathrm{PSL}_3(2)|$.
- So $\mathrm{PSL}_2(7) \cong \mathrm{PSL}_3(2)$.