8th PhD Summer School in Discrete Maths
Finite Permutation Groups
Lecture 1: Group actions

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

Rogla, 2 July 2018

University of St Andrews

§1: The symmetric group

Permutations

Let Ω be a nonempty set.

Defn: A permutation of Ω is a bijection from Ω to Ω.

Defn: We multiply two permutations x and y on Ω by composition of functions:

$$(\alpha)(xy) = (\alpha x)y$$

for all $\alpha \in \Omega$.

Defn: The symmetric group on Ω, written $\mathrm{Sym}(\Omega)$, is the set of all permutations of Ω, under composition of functions.

Defn: Let $\underline{n} = \{1, \ldots, n\}$. Write S_n for $\mathrm{Sym}(\underline{n})$.

Theorem 1

Let $|\Omega| = n$. Then $\mathrm{Sym}(\Omega)$ is a group of order $n!$.

Disjoint cycles

Ω – finite.

Defn: An *r-cycle*, written $c = (a_1\, a_2\, \ldots\, a_r)$, is the permutation

$$\begin{aligned} a_1 &\mapsto a_2 \\ a_2 &\mapsto a_3 \\ &\vdots \\ a_{r-1} &\mapsto a_r \\ a_r &\mapsto a_1 \end{aligned}$$

and fixing $\Omega \setminus \{a_1, \ldots, a_r\}$.

Defn: Cycles c_1 and c_2 are disjoint if no point moved by c_1 is moved by c_2.

Lemma 2

Let c_1 and c_2 be disjoint cycles on Ω. Then $c_1 c_2 = c_2 c_1$.

Theorem 3

Every $\sigma \in \mathrm{Sym}(\Omega)$ can be written as a product of disjoint cycles. This product is unique up to the order of the cycles.

Transpositions

Ω – finite.

Defn: A transposition is a 2-cycle.

Lemma 4

Every $\sigma \in \mathrm{Sym}(\Omega)$ *can be written as a product of transpositions.*

Proof.

$c = (a_1\ a_2\ \dots a_r)$ – an r-cycle. Then

$$c = (a_{r-1}\ a_r)(a_{r-2}a_{r-1}) \cdots (a_2\ a_3)(a_1\ a_2).$$

Result now follows from Theorem 3. □

Warning! The decomposition of a cycle into transpositions is not unique: $(1\ 2\ 3) = (2\ 3)(1\ 2) = (1\ 3)(2\ 3)$.

Even and odd permutations

Ω – finite.

Defn: A permutation σ is even if σ can be written as a product of an even number of transpositions.
σ is odd if σ can be written as a product of an odd number of transpositions.

Theorem 5
Every permutation $\sigma \in \mathrm{Sym}(\Omega)$ is either even or odd, but not both.

Defn: $\mathrm{Alt}(\Omega) = \{\sigma \in \mathrm{Sym}(\Omega) \ : \ \sigma \text{ is even}\}$.

Theorem 6
$\mathrm{Alt}(\Omega) \trianglelefteq \mathrm{Sym}(\Omega)$. *The index* $|\mathrm{Sym}(\Omega) : \mathrm{Alt}(\Omega)| = 2$.

Defn: $\mathrm{Alt}(\Omega)$ is the alternating group.

§2: Actions and representations

Actions

Defn: A permutation group is any $H \leq \mathrm{Sym}(\Omega)$, where $\Omega \neq \emptyset$.

Definition 7

An action of a gp G on a nonempty set Ω is a function $\mu : \Omega \times G \to \Omega$, $(\alpha, g) \mapsto \alpha^g$ s.t. for all $\alpha \in \Omega$, $g, h \in G$

(A1) $\alpha^{1_G} = \alpha$; and
(A2) $\alpha^{(gh)} = (\alpha^g)^h$.

Say that G acts on Ω.

Example 8

1. $\mathrm{Sym}(\Omega)$ acts on Ω by $\alpha^\sigma = \alpha\sigma$.
   So every perm group on Ω acts on Ω: the natural action.
2. G – group. G acts on itself by right multiplication: $(\alpha, g)\mu = \alpha^g := \alpha g$. The right regular action.
3. G – group. $H \leq G$. Let $\Omega = \{Ha : a \in G\}$. Then G acts on Ω by $(Ha, g)\mu_H = (Ha)^g = Hag$. The right coset action.

Permutation representations

G – group. Ω – nonempty set.

Defn: A permutation representation (perm rep) of G on Ω is a homom $\rho : G \to \mathrm{Sym}(\Omega)$.

Theorem 9

Let G act on Ω via $\mu : \Omega \times G \to \Omega$, $(\alpha, g) \mapsto \alpha^g$. For each $g \in G$, let

$$\rho_g : \alpha \mapsto \alpha^g.$$

Then the map $\rho_\mu : G \to \mathrm{Sym}(\Omega)$, $g \mapsto \rho_g$ is a perm rep.

Theorem 10

Let ρ be a perm rep of G on Ω. Then $\mu_\rho : \Omega \times G \to G$, $(\alpha, g) \mapsto \alpha(g\rho)$ is an action.

Theorem 11

The operations of Theorems 9 and 10 are mutually inverse: there is a natural bijection between actions of G on Ω and perm reps of G on Ω.

Properties of actions

Defn: The kernel of an action is the kernel of the corresponding perm rep.

Defn: The degree of an action of G on Ω, or of a permutation group on Ω, or of a perm rep $\rho : G \to \mathrm{Sym}(\Omega)$ is $|\Omega|$.

Defn: An action or representation is faithful if the kernel is trivial.

Theorem 12

If a perm rep ρ is faithful then $\mathrm{Im}\rho \cong G$. If G is finite and $\mathrm{Im}\rho \cong G$ then ρ is faithful.

Proof.

First isomorphism theorem. □

Examples of representations

1. Recall the natural action of a perm group $G \leq \mathrm{Sym}(\Omega)$ (Example 8.1). The corresponding perm rep is the identity map ι embedding G in $\mathrm{Sym}(\Omega)$.
   ι is faithful, and has degree $|\Omega|$.
2. The right regular action $(g, h)\mu = gh$ corresponds to the Cayley rep or the right regular rep.
   It has degree $|G|$.
   Cayley's Theorem Every gp G is isomorphic to a perm gp.
3. Let $H \trianglelefteq G$. The conjugation action of G on H is $\mu : H \times G \to H$, $(h, g) \mapsto g^{-1}hg$.
   The kernel of this action is $C_G(H) = \{g \in G \mid hg = gh \text{ for all } h \in H\}$, the centraliser of H in G.

§3: Orbits and stabilisers

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 13

Let $\alpha, \beta \in \Omega$. Then either $\alpha^G = \beta^G$ or $\alpha^G \cap \beta^G = \emptyset$.
That is, the set of all orbits of G forms a partition of Ω.

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

Example 14

1. Let $H \leq G$; μ_H – right coset action of G on H.
   This action is transitive, of degree $|G : H|$.
2. If $n \geq 3$ then A_n is transitive on k-subsets of $\underline{n}$ for $1 \leq k \leq n$.
3. Let G act on itself by conjugation. The orbits of G are the conjugacy classes: the sets $\{x^{-1}gx \ : \ x \in G\}$.
   If $G \neq 1$ then this action is intransitive.

Stabilisers and the Orbit-Stabiliser Theorem

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

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

Theorem 15

1. $G_\alpha \leq G$.
2. *Let* $\beta = \alpha^g$. *Then* $G_\beta = G_\alpha^g$.
3. $\alpha^g = \alpha^h$ *if and only if* $G_\alpha g = G_\alpha h$.
4. *The orbit-stabiliser theorem:* $|\alpha^G| = |G : G_\alpha|$.

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

Corollary 16

Let G act transitively on Ω, let $\alpha \in \Omega$.

1. $\{G_\omega : \omega \in \Omega\} = \{G_\alpha^g \ : \ g \in G\}$.
2. *The kernel of the action is* $\cap_{g \in G} G_\alpha^g$ *– the core of* G_α *in* G.
3. *If G is finite then: G is regular if and only if* $|G| = |\Omega|$.