35003 MODERN ALGEBRA

Prof Murray Elder, UTS
Week 5: group actions; Sylow theorems

Lauritzen 2.10

SYLOW p-SUBGROUP

Let p be a prime, and assume G is a finite group of order $p^r m$ where $\gcd(p, m) = 1, r \in \mathbb{N}_+$.

A subgroup of G of order p^r is called a *Sylow p-subgroup*.

By Lagrange, all subgroups of G must have order dividing $p^r m$, but there is no obvious reason why you should expect to see a subgroup of all possible orders (eg A_5).

Assume $|G| = p^r m$ where $\gcd(p, m) = 1, r \in \mathbb{N}_+$ and p is prime.

Sylow Theorem 1: G has a Sylow p-subgroup.

Sylow Theorem 2: If P, Q are two Sylow p-subgroups, then they are conjugate: there exists $g \in G$ with

$$gPg^{-1} = Q.$$

Furthermore, any subgroup of order p^i (for $1 \leqslant i < r$) is contained in a Sylow p-subgroup.

Sylow Theorem 3: Let $\mathrm{Syl}_p(G)$ denote the set of all Sylow p-subgroups. Then

(i) $|\mathrm{Syl}_p(G)|$ divides m
(ii) $|\mathrm{Syl}_p(G)| \equiv 1 \mod p$

We can immediately show how to use them.

Application: Prove that there is only one group of order 143.

Sylow Theorem 3: Let $\mathrm{Syl}_p(G)$ denote the set of all Sylow p-subgroups. Then

(i) $|\mathrm{Syl}_p(G)|$ divides m
(ii) $|\mathrm{Syl}_p(G)| \equiv 1 \mod p$

How many subgroups of size $13, 11$ does G have?

Sylow Theorem 2: for all $g \in G, gHg^{-1} = ?$ (a subgroup of size $|H|$)

So we have two normal subgroups P, Q with intersection ?

and $PQ = ?$

To prove them, we will use the idea of a *group action*.

We have seen examples of groups acting on (metric spaces) like $\mathbb{R}^2$, on sets $\{1, 2, \ldots, n\}$, and we can define interesting groups as subgroups of the automorphism group of a graph (eg infinite rooted binary tree).

Today we will just think about groups acting on *sets* without extra structure (preserving edges, distance, etc).

Definition

Let $G = (G, *)$ be a group and S a set.

G acts on S (from the left) if there is a map $\alpha\colon G \times S \to S$ denoted $\alpha(g, s) = g \cdot s$ which satisfies

1. $e \cdot s = s$ for all $s \in S$
2. $(g * h) \cdot s = g \cdot (h \cdot s)$ for all $g, h \in G, s \in S$.

When it is clear from context we will not write the dot.

Eg:

- G acts on itself by left mult $\alpha(x, y) := xy$ (think Sudoku proof)
- S_n acts on M_n
- D_{2n} acts on $\mathbb{R}^2$
- $H \leqslant G$ acts on G by $\alpha(h, g) := gh^{-1}$
- G acts on itself by conjugation: $\alpha(x, y) := xyx^{-1}$

DEFINITION 2.10.2

Let $\alpha\colon G \times S \to S$ be a group action of G on S, $X \subseteq S$, $s \in S$.

1. $G \cdot s = Gs = \{g \cdot s \mid g \in G\}$ is the *orbit* of the point s under the action of G (follow s around)
2. S/G is the set of orbits $\{Gs \mid s \in S\}$
3. Let $g \cdot X = gX = \{g \cdot x \mid x \in X\}$, then $G_X = \{g \in G \mid gX = X\}$ is the *stabiliser* of X under the action of G.
4. If $X = \{x\}$ we write $G_{\{x\}} = G_x$ for the stabiliser of a single point.
5. A point $s \in S$ is called a *fixed point* for the action of G on S if $g \cdot s = s$ for all $g \in G$.
6. The set of all fixed points of S is denoted S^G.

Let the group be the symmetric group S_n and the set be M_n.

Action: $\sigma \in S_n, i \in M_n$, $\sigma \cdot i := \sigma(i)$.

$(S_n)_i$ perms which fix the number i.

Fix $\tau \in S_n$ and define a new action of $\langle \tau \rangle$ on S_n:

$$\alpha(\tau^j, i) := \tau^j(i)$$

The orbits of this action are:

Let G be a group, H a subgroup. Define an action of G on G/H (left cosets) by

$$\alpha(x, yH) := (xy)H$$

Orbits?

Stabiliser of a point? eg. point$= H$.

PROPOSITION 2.10.5

Let $\alpha\colon G \times S \to S$ be an action, $X \subseteq S$ and $x \in S$.

(i) G_X is a subgroup of G.

(ii) $S = \bigcup_{s \in S} Gs$
and $Gs \neq G_t$ implies $Gs \cap G_t = \emptyset$ (the orbits are a partition of S)

(iii) The map $\tilde{f}\colon G/G_x \to Gx$ (cosets of G_x to orbits of x) defined by

$$\tilde{f}(gG_x) = gx$$

is a well-defined and bijective map.

(iii) The map $\tilde{f}: G/G_x \to Gx$ defined by $\tilde{f}(gG_x) = gx$ is a well-defined and bijective map.

Proof: Let $g_1, g_2 \in G$. Then

$$\begin{aligned} & g_1 x = g_2 x & \\ \text{iff} \quad & x = g_1^{-1} g_2 x & \text{by defn of action} \\ \text{iff} \quad & g_1^{-1} g_2 \in G_x & \text{by defn of stabiliser} \\ \text{iff} \quad & g_1 G_x = g_2 G_x & \text{by Lemma 2.2.6} \end{aligned}$$

Well-defined: if a coset are represented in two different ways, *i.e.* $g_1 G_x = g_2 G_x$, then $\tilde{f}(g_1 G_x) = g_1 x = g_2 x = \tilde{f}(g_2 G_x)$ so map is well defined.

Injective: if $\tilde{f}(g_1 G_x) = \tilde{f}(g_2 G_x)$ then $g_1 x = g_2 x$ implies $g_1 G_x = g_2 G_x$.

COROLLARY

Let $\alpha\colon G \times S \to S$ be an action where S is finite.

Let B be the set of $x \in S$ such that the orbit Gx has more than one element.

Then

$$|S| = \left|S^G\right| + \sum_{x \in B} |G/G_x|$$

where the summation is done by picking out an element x from each orbit with more than one element.

Proof: Count $|S|$ by first counting the elements which lie in an orbit of size 1

then those that lies in an orbit of size 2 or more. Propn2.10.5(iii) says G/G_x is in bijection with G_x. $\square$

Lemma (Burnside*)

Let $G \times S \to S$ be an action where G, S are finite.

Then

$$|S/G| = \frac{\sum_{g \in G} |S^g|}{|G|}$$

where $S^g = S^{\{g\}} = \{x \in S \mid gx = x\}$.

Proof: count the same thing in two different ways (usual Combinatorics trick).

Thing: let $T = \{(g, x) \in G \times S \mid gx = x\}$.

See Lauritzen.

Also see Lauritzen for an argument to describe the group of linear isometries of $\mathbb{R}^2$ which preserve an octagon centered at $(0, 0)$ using the ideas in proposition 2.10.5.

Recall that G acts on itself by conjugation: $\alpha(x, y) := xyx^{-1}$

The orbit

$$G \cdot y = \{gyg^{-1} \mid g \in G\} \quad := C(y)$$

is the *conjugacy class* of y.

The stabiliser of a point y is called the *centraliser* of y:

$$G_y = \{g \mid gyg^{-1} = y\}$$

and is denoted $Z(y)$. It is the set of elements of G with which y commutes.

What is the set of fixed points for the action?

The stabiliser of a subgroup $H \leqslant G$ with respect to the conjugacy actionis

$$G_H = \{g \in G \mid gHg^{-1} = H\}$$

which would be the whole group if H is normal (what about when H is not normal?)

Denote this by $N_G(H)$, called the *normaliser* of H in G. (is it called that because $N_G(H)$ is a normal subgroup? So it "makes H normal")

Corollary 2.10.7: the size of the set acted on (G) is equal to the size of the fixed points ($Z(G)$) plus the size of the orbits/quotients $G/Z(h)$ where h is chosen from each orbit (conjugacy class) with more than one element.

$$|G| = |Z(G)| + \sum_{h \in G} |G/Z(h)| \text{ where } h \ldots$$

Let p be a prime and $r \in \mathbb{N}$. A group of order p^r is called a *p-group.*

Proposition (2.10.13)

Let G be a non-trivial p-group acting on a set finite S. Then

$$|S| \equiv |S^G| \mod p$$

Proof: Corollary which counts the set breaking up between fixed points and orbits/cosets of stabilisers G/G_x:

$$|S| = |S^G| + \sum_{x \in B} |G/G_x|$$

where x is picked from each orbit of size > 1 (B is all orbits of size > 1)

So we just need to show that each $|G/G_x|$ is a multiple of p.

x is not a fixed point so G_x is not all of G.

And G_x is more than just $\{e\}$ since the orbit Gx has size > 1 and is in bijection with G/G_x.

Lagrange: $|G| = p^r = |G_r|[G : G_r] = |G_r| \cdot |G/G_x|$

so $|G/G_x| = p^i$ for $1 \leqslant i < r$, and we have proved the result. $\square$

If the action is the conjugacy action ($S = G, S^G = Z(G)$), then this proposition says

$$|G| \equiv |Z(G)| \mod p$$

Then from this we have $|Z(G)| > 1$ because if $Z(G) = \{e\}$ then $p^r \equiv 1 \mod p$ but p is not a divisor of $p^r - 1$ ‡

GROUPS OF ORDER p^2

Corollary (2.10.15)

If G has order p^2 for a prime p then G is abelian.

Proof: from the previous slide we know $|Z(G)| > 1$ and is $\equiv p^2 \mod p$ so it is either size p or p^2 (the whole group).

Suppose for contradiction $|Z(G)| = p$.

Then $G/Z(G)$ is order p and a group (since $Z(G)$ is normal) so $G/Z(G)$ must be cyclic.

Let $x(G)$ be a generator. Then every element of G is of the form $x^i a$ where $a \in Z(G)$.

Then $(x^i a)(x^j b) = x^{i+j} ab = x^j b x^i a$ so every element commutes, contradiction. □

The previous proof gives us a glimpse into the method for proving the Sylow Theorems (at the start of the lecture).

We find a good action to use (which means choosing a set, a group (may not be the original group but maybe a subgroup), then exploit the orbit-stabiliser proposition to count.

Lauritzen says: extending this proof a bit further, you can prove that the only two groups possible are $\mathbb{Z}/p^2\mathbb{Z}$ and $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ (we know this is true if $p = 2$). Good exercise to try this (see workshop sheet 4).

Extending this even further, you can *classify* all finite abelian groups. See Exercise 2.11.57 (HOF)

NEXT:

Friday: Worksheet on proving Sylow theorems, and applying them (Lauritzen 2.10 pages 102-103 and problems from 2.11)

Next Wednesday:

- Free groups and group presentations (special topic not in Lauritzen, notes will be provided)