

# 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  $\gcd(p, m) = 1$ ,  $r \in \mathbb{N}_+$ .

# 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*.

# 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  $A_5$ ).

$$30 \quad \nearrow \quad 5! / 2 \quad 60$$

# SYLOW THEOREMS

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 THEOREMS

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. <sup>order,</sup>  
 $p$

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  $1 \leq i < r$ ) is contained in a Sylow  $p$ -subgroup.

# SYLOW THEOREMS

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  $1 \leq i < r$ ) is contained in a Sylow  $p$ -subgroup.

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

(i)  $|\text{Syl}_p(G)|$  divides  $m$  .

(ii)  $|\text{Syl}_p(G)| \equiv 1 \pmod{p}$

congruent.

# HOW TO USE

$$g h_1 g^{-1} = g h_2 g^{-1}$$

We can immediately show how to use them.

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

$$2 \cdot 143 \cdot 2$$

Sylow Theorem 3: Let Syl<sub>p</sub>(G) denote the set of all Sylow  $p$ -subgroups. Then

- (i)  $|Syl_p(G)|$  divides  $m$
- (ii)  $|Syl_p(G)| \equiv 1 \pmod{p}$

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

$Syl_{13}(G) = \{H\}$

$\forall g \in G$

$g H g^{-1}$

1. Subgroup of  $G$ ?
2. size?

$|Syl_{13}(G)|$  divide ~~13~~ 11

either 1, 11

also  $|Syl_{13}(G)| \equiv 1 \pmod{13}$

HOW TO USE  $P \times Q$   $PQ$   $P$  size 11  $Q$  size 13

2  
3  
4 →  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59  
60  
61  
62  
63  
64  
65  
66  
67  
68  
69  
70  
71  
72  
73  
74  
75  
76  
77  
78  
79  
80  
81  
82  
83  
84  
85  
86  
87  
88  
89  
90  
91  
92  
93  
94  
95  
96  
97  
98  
99  
100

We can immediately show how to use them.

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

Sylow Theorem 3: Let  $Syl_p(G)$  denote the set of all Sylow  $p$ -subgroups. Then

- (i)  $|Syl_p(G)|$  divides  $m$
- (ii)  $|Syl_p(G)| \equiv 1 \pmod{p}$

$$gkg^{-1} = k$$

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

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

So we have two normal subgroups  $P, Q$  with intersection  $= \{e\}$ .

$|Syl_{11}(G)|$  — divide 13 → 1, 13  
 $\equiv 1 \pmod{11}$   
 $\equiv 2 \pmod{11}$

## HOW TO USE

We can immediately show how to use them.

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

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

(i)  $|\text{Syl}_p(G)|$  divides  $m$

(ii)  $|\text{Syl}_p(G)| \equiv 1 \pmod{p}$

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

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

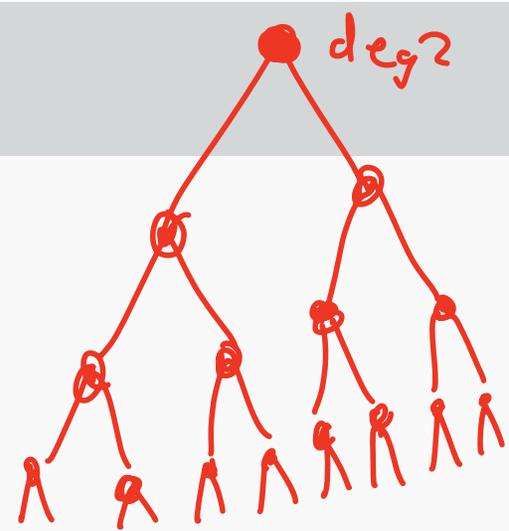
So we have two normal subgroups  $P, Q$  with intersection ?

and  $PQ = ?$

## HOW TO PROVE

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

# HOW TO PROVE



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  $\{1, 2, \dots, n\}$ , 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).



# GROUP ACTION

## Definition

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

$G$  acts on  $S$  (from the left) if there is a map  $\alpha: G \times S \rightarrow S$  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:

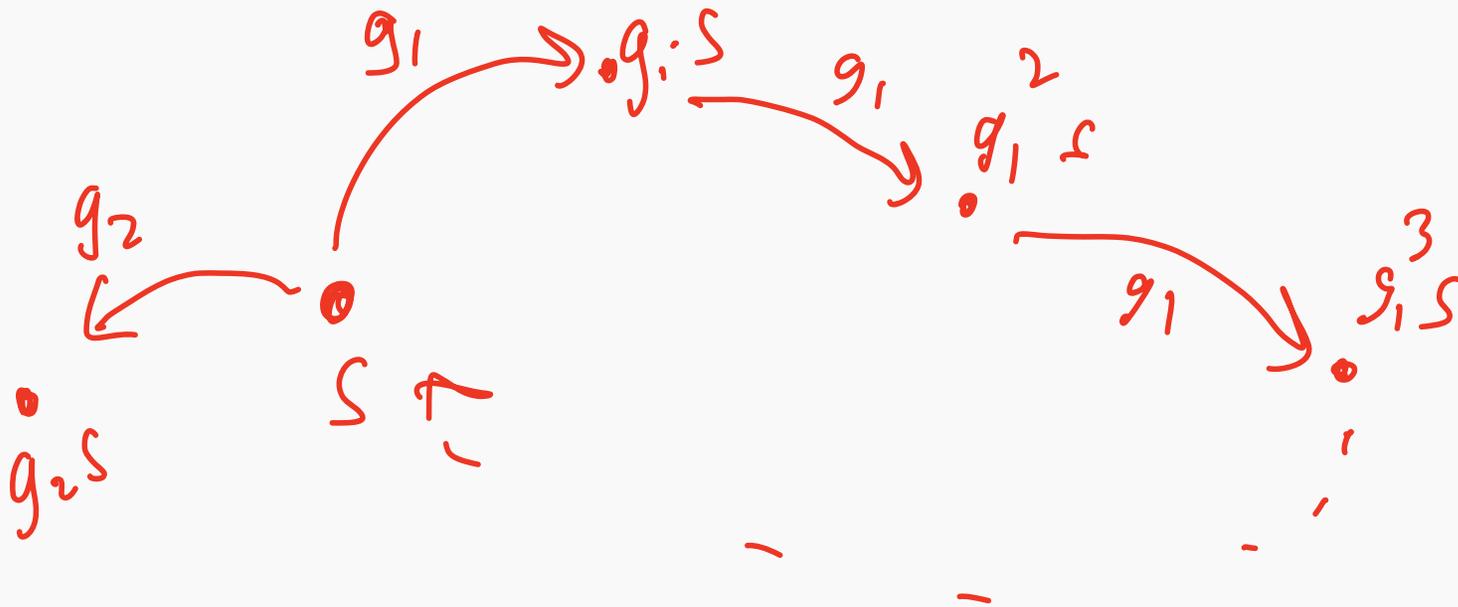
- $G$  acts on itself by left mult  $\alpha(x, y) := xy$  (think Sudoku proof)
- $S_n$  acts on  $M_n = \{1, \dots, n\}$
- $D_{2n}$  acts on  $\mathbb{R}^2$  self H-group.
- subgroup  $H \leq G$  acts on  $G$  by  $\alpha(h, g) := gh^{-1}$
- $G$  acts on itself by conjugation:  $\alpha(x, y) := xyx^{-1}$

## DEFINITION 2.10.2

Let  $\alpha: G \times S \rightarrow S$  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)

$$Gs \subseteq S$$



## DEFINITION 2.10.2

Let  $\alpha: G \times S \rightarrow S$  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  $\{Gs \mid s \in S\}$

## DEFINITION 2.10.2

Let  $\alpha: G \times S \rightarrow S$  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  $G$ .

one element is  $e$

Fix X

$$G_X \subseteq G$$

## DEFINITION 2.10.2

Let  $\alpha: G \times S \rightarrow S$  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.

## DEFINITION 2.10.2

Let  $\alpha: G \times S \rightarrow S$  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  $g \in G$ .

$\underbrace{\hspace{1cm}} \quad \underbrace{\hspace{1cm}}$

eg

$$\begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

$\Rightarrow$  a fixed point

for  $GL(2, \mathbb{R})$  on  $\mathbb{R}^2$

$D_8$

## DEFINITION 2.10.2

Let  $\alpha: G \times S \rightarrow S$  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  $S^G$ .

# EXAMPLES

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

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

# EXAMPLES

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  $i$ .

$$(S_n)_i$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ & 4 & 2 & 3 \end{pmatrix}$$

fixes 1.

# EXAMPLES

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  $i$ .

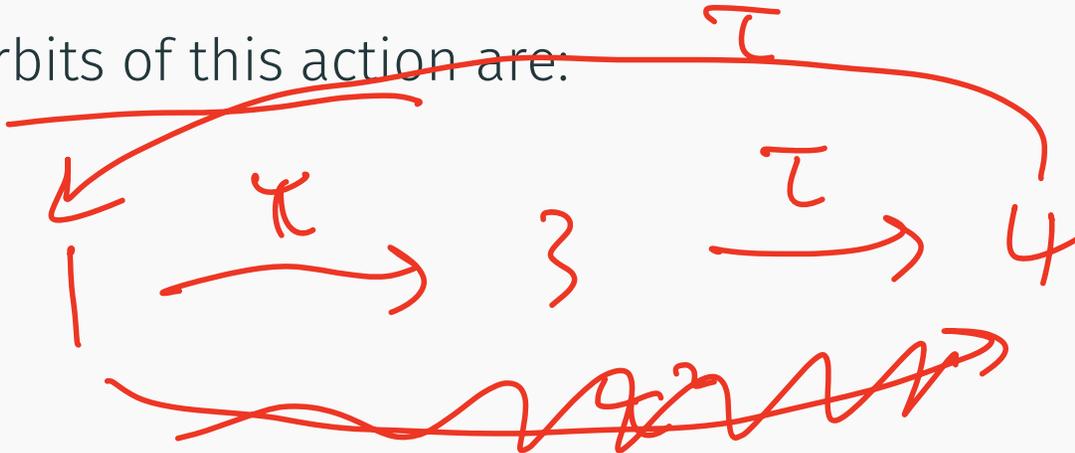
$$\{e, \tau, \tau^2, \dots\}$$

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

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

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$$

The orbits of this action are:



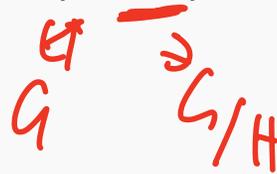
1, 3, 4

# EXAMPLES

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?



# EXAMPLES

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 =  $H$ .

$$gH = H$$

iff  $g \in H$

# PROPOSITION 2.10.5

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

(i)  $G_x$  is a subgroup of  $G$ .

$$\overline{\{g \in G \mid \underline{g \cdot X} = X\}}.$$

$$g, h \in G_x,$$

$$(g \circ h) \circ X$$

$$\begin{aligned} &= g \circ (h \circ X) \\ &= g \circ X = X. \end{aligned}$$

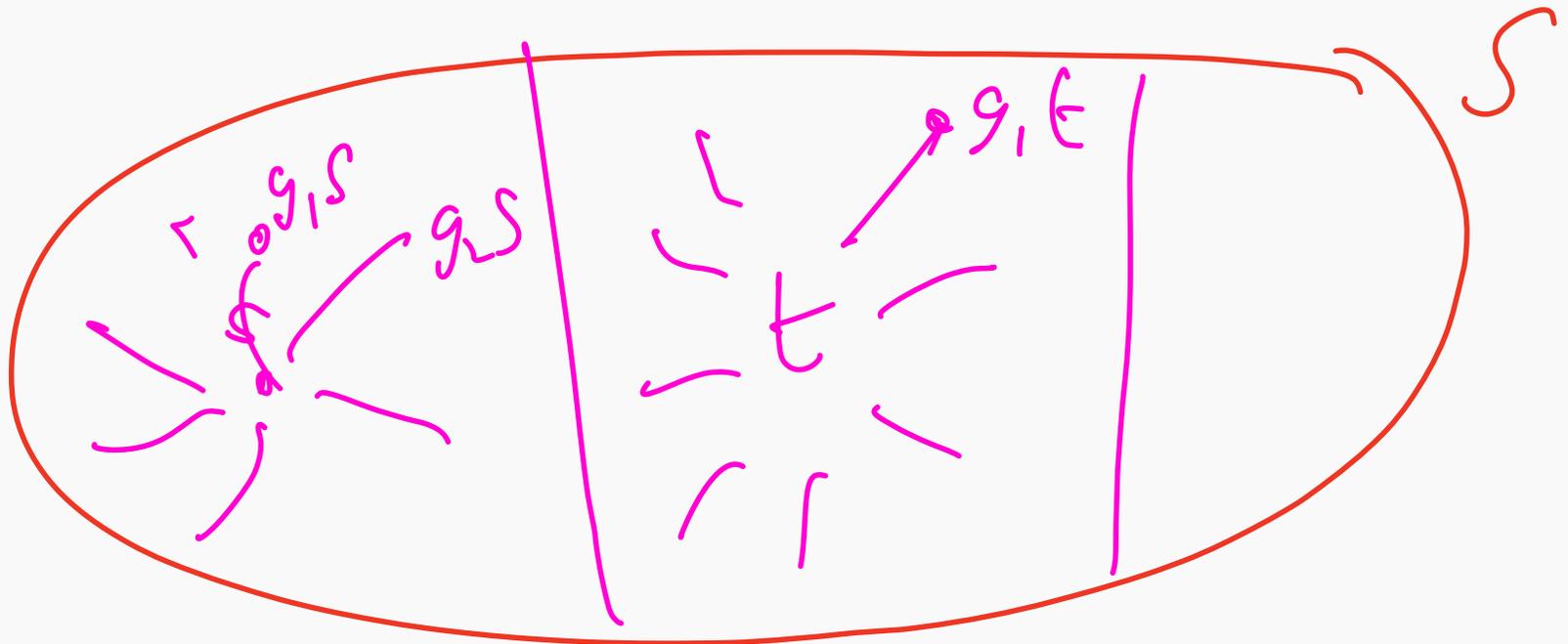
Check: inverse.

# PROPOSITION 2.10.5

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

(i)  $G_x$  is a subgroup of  $G$ .

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



# PROPOSITION 2.10.5

Let  $\alpha: G \times S \rightarrow S$  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  $Gs \neq Gt$  implies  $Gs \cap Gt = \emptyset$  (the orbits are a partition of  $S$ )

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

$x \in S$

left cosets

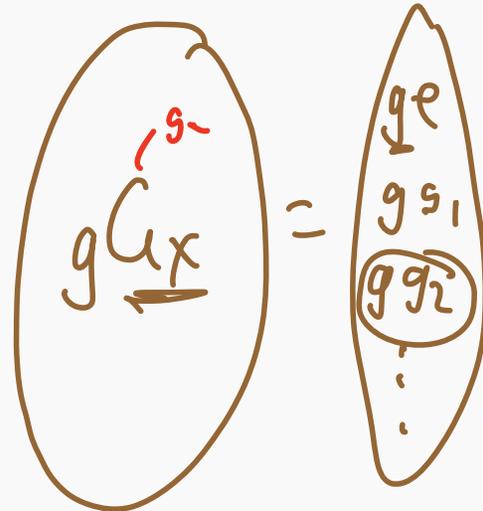
$$\tilde{f}(gG_x) = gx$$

is a well-defined and bijective map.  $\rightarrow$  1-1  $\rightarrow$  onto.



doesn't depend on choice of  $g$

$$g(x) \parallel g(g_x x) = gx$$



## PROOF OF PROPOSITION 2.10.5(iii)

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

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

$$\begin{aligned} & g_1x = g_2x \\ \text{iff } & x = g_1^{-1}g_2x \quad \text{by defn of action} \\ \text{iff } & g_1^{-1}g_2 \in G_x \quad \text{by defn of stabiliser} \\ \text{iff } & g_1G_x = g_2G_x \quad \text{by Lemma 2.2.6} \end{aligned}$$

## PROOF OF PROPOSITION 2.10.5(iii)

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

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

$$\begin{aligned} & g_1x = g_2x \\ \text{iff } & x = g_1^{-1}g_2x \quad \text{by defn of action} \\ \text{iff } & g_1^{-1}g_2 \in G_x \quad \text{by defn of stabiliser} \\ \text{iff } & g_1G_x = g_2G_x \quad \text{by Lemma 2.2.6} \end{aligned}$$

Well-defined: if a coset are represented in two different ways, *i.e.*  $\underline{g_1G_x} = \underline{g_2G_x}$ , then  $\underline{\tilde{f}(g_1G_x)} = \underline{g_1x} = \underline{g_2x} = \underline{\tilde{f}(g_2G_x)}$  so map is well defined.

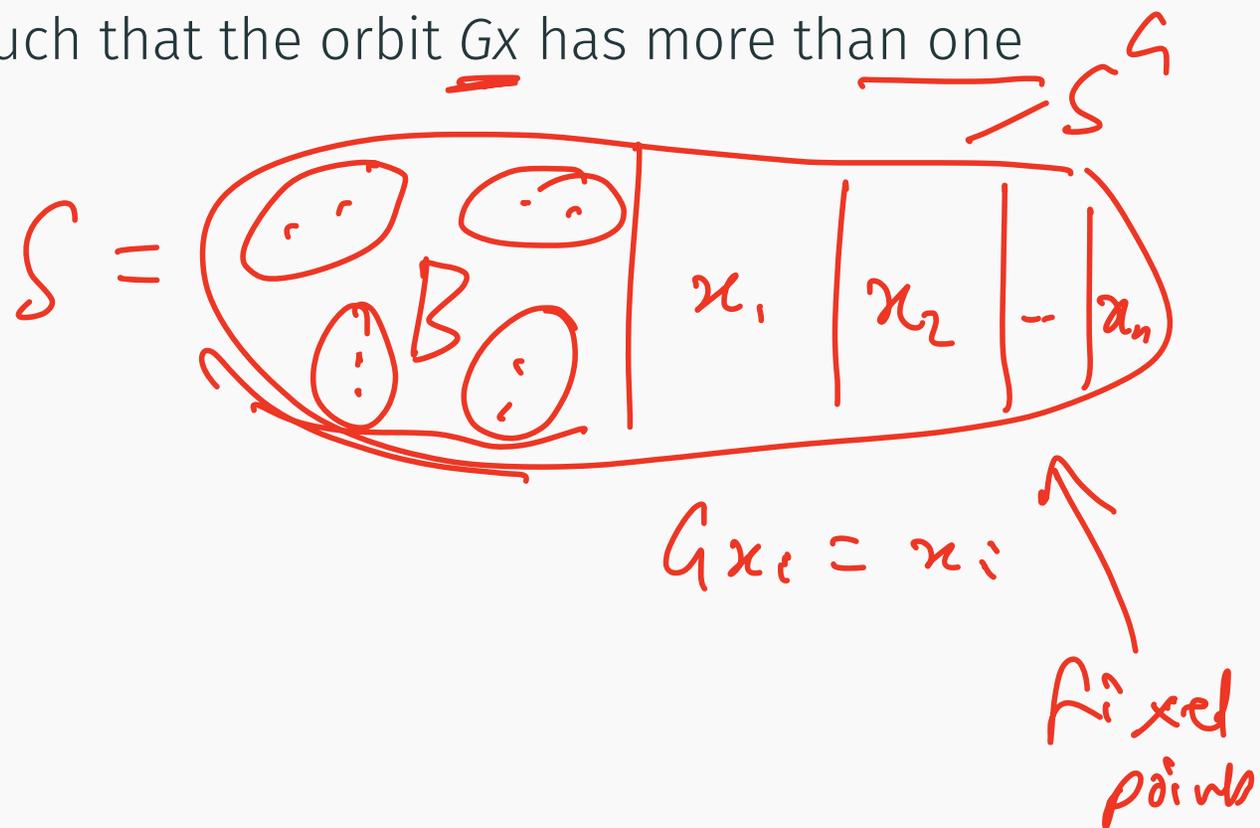
Injective: if  $\underline{\tilde{f}(g_1G_x)} = \underline{\tilde{f}(g_2G_x)}$  then  $\underline{g_1x} = \underline{g_2x}$  implies  $\underline{g_1G_x} = \underline{g_2G_x}$ .

Surjective: Exercise

# COROLLARY

Let  $\alpha: G \times S \rightarrow S$  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.



# COROLLARY

Let  $\alpha: G \times S \rightarrow S$  be an action where  $S$  is finite.

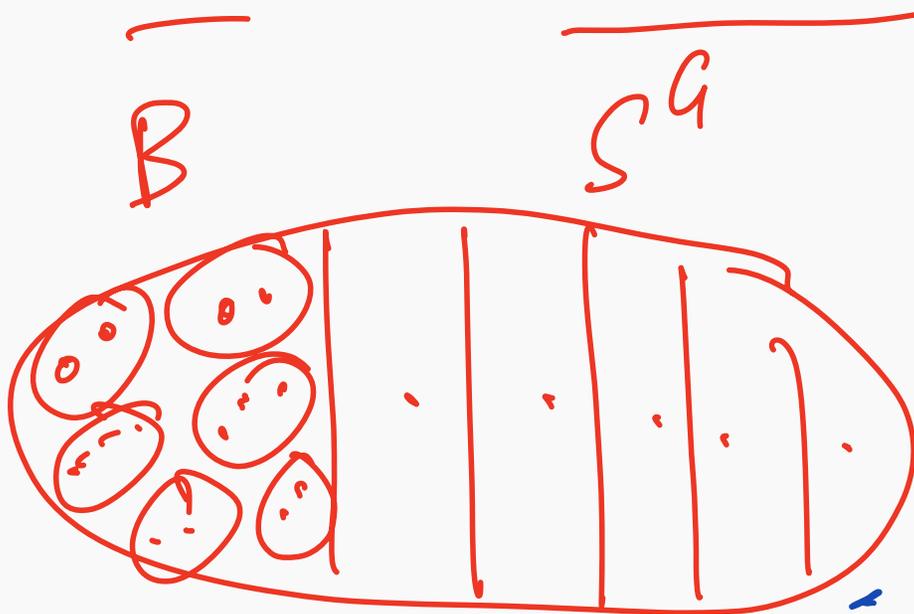
Let  $B$  be the set of  $x \in S$  such that the orbit  $Gx$  has more than one element.

Then

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

*left cosets.*

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



Bijection  $G/G_x$   
with  $G_x$

## COROLLARY

Let  $\alpha: G \times S \rightarrow S$  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

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

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

## COROLLARY 2.10.7

Let  $\alpha: G \times S \rightarrow S$  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

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

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 lie in an orbit of size 2 or more. Propn 2.10.5(iii) says  $G/G_x$  is in bijection with  $G_x$ .  $\square$

## Lemma (Burnside\*)

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

Then

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

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

## Lemma (Burnside\*)

Let  $G \times S \rightarrow S$  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).

*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.

# CONJUGACY ACTION

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

# CONJUGACY ACTION

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

The orbit

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

is the conjugacy class of  $y$ .

# CONJUGACY ACTION

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

The orbit

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

is the *conjugacy class* of  $y$ .

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

$$\underline{G}_y = \{g \mid \underline{gyg^{-1}} = y\} = \{g \in G \mid gy = yg\}$$

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

# CONJUGACY ACTION

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

The orbit

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

is the *conjugacy class* of  $y$ .

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

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

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?

$e$ , anything that commutes with ALL elts of  $G$

Center:

$$Z(G) = \left\{ g \in G \mid \begin{array}{l} gh = hg \\ \forall h \in G \end{array} \right\}$$

commutes

## CONJUGACY ACTION CONTINUED

The stabiliser of a subgroup  $H \leq G$  with respect to the conjugacy action is

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

which would be the whole group if  $\underline{H}$  is normal (what about when  $H$  is not normal?)

Note  $H \subseteq G_H$

## CONJUGACY ACTION CONTINUED

The stabiliser of a subgroup  $H \leq G$  with respect to the conjugacy action is

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

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”)

## CONJUGACY ACTION CONTINUED

The stabiliser of a subgroup  $H \leq G$  with respect to the conjugacy action is

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

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.

$$|G| = |Z(G)| + \sum_{\substack{\text{size} \\ \geq 2}} (|G/Z(h)|)$$

$\underbrace{\hspace{10em}}_{S^G} \quad \underbrace{\hspace{10em}}_{\sum_{x \in B} \quad \downarrow \quad \underline{h}}$

## CONJUGACY ACTION CONTINUED

The stabiliser of a subgroup  $H \leq G$  with respect to the conjugacy action is

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

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.

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

is such that  
 $G_h$  size  
 $\geq 2$

## $p$ -GROUPS

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

# $p$ -GROUPS

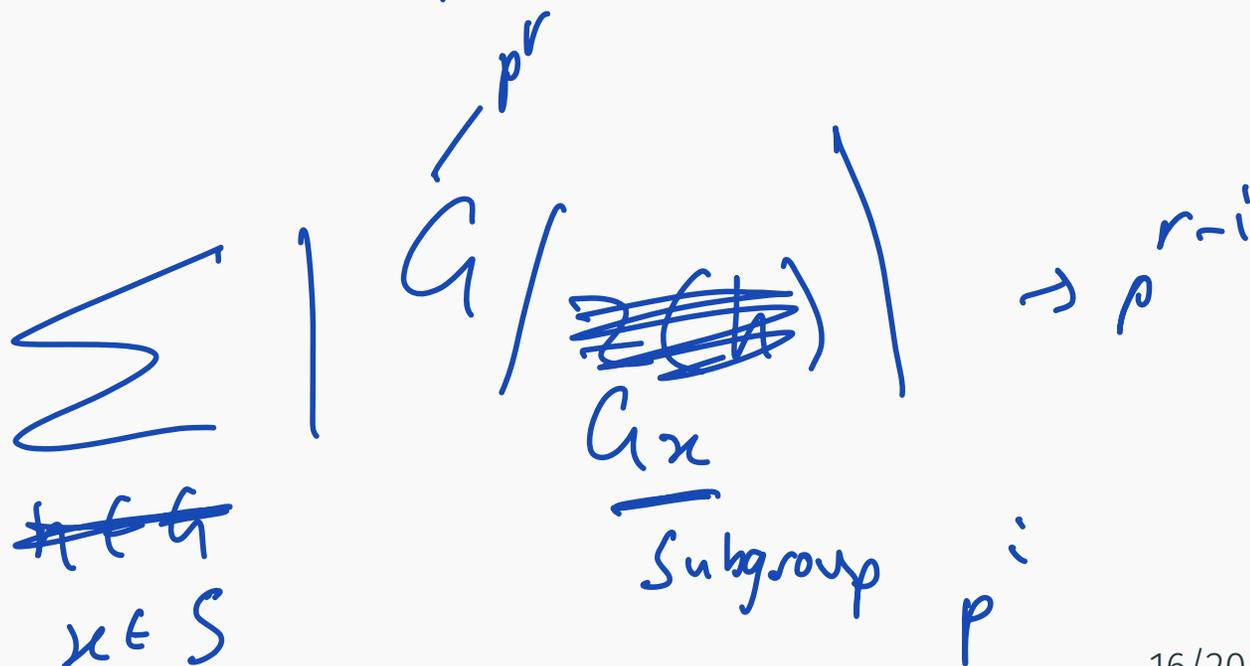
Let  $p$  be a prime and  $r \in \mathbb{N}$ . A group of order  $p^r$  is called a  $p$ -group.

## Proposition (2.10.13)

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

$$\underline{|S|} \equiv \underline{|S^G|} \pmod{p}$$

fixed points.



## $p$ -GROUPS

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

$$|S| \equiv |S^G| \pmod{p}$$

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

2.10.7

# $p$ -GROUPS

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

$$|S| \equiv |S^G| \pmod{p}$$

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  $p$ .

## PROOF CONTINUED

$x$  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  $1 \leq i < r$ , and we have proved the result. □

## PROOF CONTINUED

$x$  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  $1 \leq i < r$ , and we have proved the result.  $\square$

---

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

$$|G| \equiv |Z(G)| \pmod{p}$$

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

$$Z(G) = \{g \in G : gh = hg \ \forall h \in G\}.$$

Applic  
 $|G|=p$

# GROUPS OF ORDER $p^2$

order 4:  $\mathbb{Z}/4\mathbb{Z}$

$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

$\mathbb{Z}/p\mathbb{Z}$

$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$

## 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  $\equiv p^2 \pmod{p}$  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  $x \in G \setminus Z(G)$  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. □

since

$a, b \in Z(G)$

they commute with all elts of  $G$ .

## SUMMARY

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.

Corollary.  
2 · 10 · 7

## SUMMARY

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).

# SUMMARY

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)

$$\mathbb{Z}/p_1\mathbb{Z} \times \mathbb{Z}/p_2\mathbb{Z} \times \dots \times \mathbb{Z}/p_k\mathbb{Z}$$

Handwritten notes in blue ink:

- A circled expression:  $\mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/13\mathbb{Z}$
- Three question marks:  $???$
- A circled expression:  $\mathbb{Z}/143\mathbb{Z}$

## 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)