Group Theory - Weeks 4,5 & 6 - Group Actions & the Sylow Theorems

Antonio León Villares

October 2022

Contents

Based on the notes by Susan J. Sierra, Chapter 4

1 Group Actions

1.1 Definition: Action of a Group

Let G be a group, and X a set.
*An **action** of G on X is the function:*

$$G \times X \to X$$

$$(g, x) \mapsto g \cdot x$$

satisfying:

1. ***Trivial Identity**:*
$$\forall x \in X, \qquad e \cdot x = x$$
2. ***"Associativity"**:*
$$g \cdot (h \cdot x) = (gh) \cdot x$$

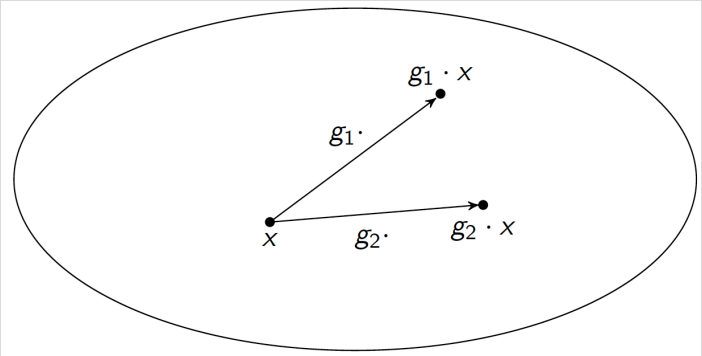
1.1.1 Examples: Group Actions

- the **symmetric group** S_n acts on $\{1, 2, \ldots, n\}$ in a natural way:
$$\sigma \cdot i = \sigma(i)$$
- the **dihedral group** D_n acts on $\{T, B\}$ (the "top" and "bottom" faces of the polygon) in the following way. If g denotes a reflection, and h denotes a rotation:
$$g \cdot T = B \qquad g \cdot B = T \qquad h \cdot T = T \qquad h \cdot B = B$$
- the **dihedral group** D_n acts on $\{1, 2, \ldots, n\}$ in a natural way, if we use the set to label the vertices of the polygon.
- the **trivial action** is defined for any set X. Given any group G, we can define:
$$\forall x \in X, \forall g \in G, g \cdot x = x$$
- let $\mathbb{F}$ be a field, $n \in \mathbb{N}$, and define the group of $n \times n$, matrices $G = GL(\mathbb{F}; n)$. G acts on the set $\mathbb{F}^n$ via matrix multiplication:
$$A \cdot v = Av$$

1.2 Definition: The Orbit

Let G be a group, and X a set.
*The **orbit** of $x \in X$ is the **subset** of X containing all elements which can be mapped to via a **group action**:*

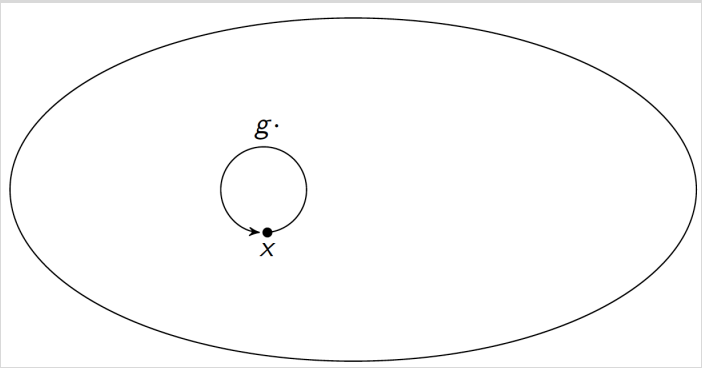
$$Orb_G(x) = G \cdot x = \{g \cdot x \mid g \in G\} \subseteq X$$



1.3 Definition: The Stabilizer

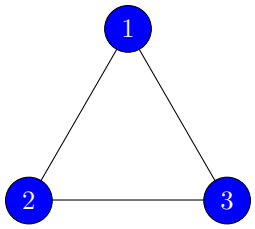
Let G be a group, and X a set.
*The **stabilizer** of $x \in X$ is the **subset** of G containing all group elements which fix $x \in X$ via a **group action**:*

$$Stab_G(x) = \{g \mid g \cdot x = x, g \in G\} \subseteq G$$



1.3.1 Example: Orbit and Stabilizer for D_3

Consider the group D_3 of symmetries of a triangle:



Consider D_3 acting on the vertices $\{1, 2, 3\}$. Then:

$$Orb_G(1) = \{1, 2, 3\}$$

since applying the rotations allow us to map a vertex to every other vertex.
Moreover:

$$Stab_G(1) = \{e, g\}$$

where g denotes a reflection about the vertex 1. All other elements of the groups are rotations (which clearly map 1 to some other vertex) or reflections about other vertices.

1.4 Lemma: Orbits as Equivalence Classes

Let G be a group acting on a set X.

1. *The following is an **equivalence relation**:*

$$x \sim y \iff \exists g \in G \ : \ g \cdot x = y$$

2. *The **equivalence classes** are **orbits**:*

$$cl(x) = Orb_G(x)$$

3. *Orbits **partition** X.*

(Lemma 4.2.2)

Proof. 1. **Equivalence Relation**

(1) **Reflexivity**

Clearly $x \sim x$, since $e \cdot x = x$ by properties of group actions.

(2) **Symmetry**

Assume that $x \sim y$. That is:

$$\exists g \in G \ : \ g \cdot x = y$$

But then:

$$g^{-1} \cdot y = g^{-1} \cdot (g \cdot x) = (gg^{-1}) \cdot x = x$$

so $y \sim x$.

(3) **Transitivity**

Assume $x \sim y$ and $y \sim z$. Then:

$$\exists g_1, g_2 \in G \ : \ g_1 \cdot x = y, g_2 \cdot y = z$$

Thus:

$$(g_2 g_1) \cdot x = g_2 \cdot (g_1 \cdot x) = g_2 \cdot y = z$$

so $x \sim z$.

Hence, $\sim$ is an equivalence relation on X, as required.

2. **Orbits as Equivalence Classes**
   By definition, the equivalence class of $x \in X$ is:

$$cl(x) = \{y \mid g \cdot x = y, g \in G\} = \{g \cdot x \mid g \in X\} = Orb_G(x)$$

3. **Orbits Partition**
   Since orbits are equivalence classes, and equivalence classes partition a set, the orbits must partition the set.

□

1.5 Lemma: Stabilizers as Subgroups

Let G be a group acting on X.
Then:

$$\forall x \in X, \qquad Stab_G(x) \leq G$$

(Lemma 4.2.3)

Proof. Firstly, the stabilizer is non-empty, since $e \cdot x = x$, so:

$$e \in Stab_G(x)$$

To show that $Stab_G(x)$ is a subgroup, let $g, h \in Stab_G(x)$. We now show that $gh^{-1} \in Stab_G(x)$:

$$\begin{aligned}(gh^{-1}) \cdot x &= (gh^{-1}) \cdot (h \cdot x) \\ &= g \cdot ((hh^{-1}) \cdot x) \\ &= g \cdot x \\ &= x\end{aligned}$$

so $gh^{-1} \in Stab_G(x)$ as required.

□

1.6 Definition: Transitive Actions

*G acts **transitively** on X if:*

$$\forall x, y \in X, \exists g \in G \ : \ y = g \cdot x$$

*In other words, there is an element $x \in X$, such that when G acts on x, it generates X (so X is in a single **orbit**).*
For example, D_n acts transitively on the set of vertices $\{1, 2, \ldots, n\}$, since n rotations allow us to map any vertex to every other vertex.

1.7 Definition: Faithful Actions

*G acts **faithfully** on X if the only element which fixes everything is e:*

$$\forall x \in X, g \cdot x = x \implies g = e$$

Alternatively:

$$\forall x \in X, Stab_G(x) = \{e\}$$

*Alternatively, if **kernel** of an action:*

$$N = \{g \mid g \cdot x = x, \forall x \in X, g \in G\} = \bigcap_{x \in X} Stab_G(x)$$

is trivial:

$$N = \{e\}$$

1.8 Theorem: The Orbit-Stabilizer Theorem

*Let G be a **finite group** acting on X. Then:*

$$\forall x \in X, \qquad |G| = |Stab_G(x)||Orb_G(x)|$$

Proof. We exploit Lagrange's Theorem, which tells us that if $H \leq G$:

$$|G| = |H||G/H|$$

For some $x \in X$, define:

$$H = Stab_G(x)$$

We claim there exists a bijection:

$$\phi : Orb_G(x) \to G/H$$

Indeed, let $y \in Orb_G(x)$. Then:

$$\exists g \in G : g \cdot x = y$$

Define:

$$\phi(y) = gH$$

This mapping is **surjective**. Let $g_1 H \in G/H$. Then, define:

$$y = g_1 \cdot x$$

Thus:

$$\phi(y) = g_1 H$$

so ϕ is surjective.

This mapping is **injective**. Assume that:

$$\phi(y_1) = \phi(y_2) \implies g_1 H = g_2 H$$

where:

$$y_1 = g_1 \cdot x \qquad y_2 = g_2 \cdot x$$

Since $g_1 H = g_2 H$, then $\exists h \in H$ such that:

$$g_1 h = g_2$$

But then:

$$y_2 = g_2 \cdot x = (g_1 h) \cdot x = g_1 \cdot (h \cdot x) = g_1 \cdot x = y_1$$

where we have used the fact that $h \in Stab_G(x)$, so $h \cdot x = x$. Hence, we have shown that:

$$\phi(y_1) = \phi(y_2) \implies y_1 = y_2$$

so ϕ is injective.

Thus, ϕ is a bijection, so $|G/H| = |Orb_G(x)|$, and by Lagrange's Theorem:

$$|G| = |H||G/H| = |Stab_G(x)||Orb_G(x)|$$

as required.

□

1.8.1 Example: Verifying Orbit-Stabilizer for Permutations

Consider the group S_n acting on $X = \{1, \ldots, n\}$. Let $x \in X$. Then, it is clear that:

$$Orb_G(x) = X$$

(that is, S_n acts transitively). This is because the transposition $\sigma = (i\ x)$ maps x to any $i \in [1, n]$.

The stabilizer is the set of all permutations which fix x. That is, all the permutations which don't include x in the cycle. But this is just the set of permutations of $n - 1$ elements:

$$Stab_G(x) = S_{n-1}$$

Hence:

$$|Stab_G(x)||Orb_G(x)| = |S_{n-1}||X| = (n-1)!n = n! = |S_n|$$

as expected.

1.9 Groups Act on Themselves

- **How can a group act on itself?**
  - groups are sets, so they can act on themselves
  - there are 3 "natural" definitions for group actions when they act on themselves. Let $g, h \in G$. Consider:
    1. **Left Action**:
    $$g \cdot h = gh$$
    2. **Right Action**:
    $$g \cdot h = hg^{-1}$$
    3. **Conjugate Action**:
    $$g \cdot h = ghg^{-1}$$

We verify that the conjugate action is indeed a group action. Let $a, g, h \in G$. Then:

(1)

$$e \cdot a = eae^{-1} = h$$

(2)

$$g \cdot (h \cdot a) = g \cdot (hah^{-1}) = g(hah^{-1})g^{-1} = (gh)a(gh)^{-1} = (gh) \cdot a$$

1.9.1 Definition: Conjugacy Classes

*Let G be a group. The **conjugacy class** of $a \in G$ is the **orbit** of a:*

$$Cl(a) = Orb_G(a) = \{gag^{-1} \mid g \in G\}$$

1.9.2 Definition: Centraliser

*Let G be a group. The **centralizer** of $a \in G$ is the **stabilizer** of a:*

$$C_G(a) = Stab_G(a) = \{g \mid gag^{-1} = a, g \in G\} = \{g \mid ga = ag, g \in G\}$$

*That is, the **centralizer** of a is the set of all elements in G which **commute** with a.*

1.9.3 Lemma: Orbit-Stabilizer for Conjugate Action

Let G be a finite group. By the Orbit-Stabilizer Theorem:

$$\forall a \in G, \qquad |G| = |C_G(a)||Cl(a)|$$

(Lemma 4.2.7)

1.9.4 Theorem: The Class Equation

Let G be a group, and consider a set of representatives $a_1, \ldots, a_n \in G$. Then:

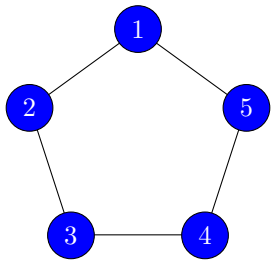
$$G = Cl(a_1) \sqcup \ldots \sqcup Cl(a_n)$$

*where $\sqcup$ is the **disjoint union**. This just says that the **conjugacy classes** partition a group (since they are **orbits**).*
This means that:

$$|G| = \sum_{i=1}^{n} |Cl(a_i)|$$

1.9.5 Example: Conjugate Actions and the Dihedral Group

Consider D_5 acting on its vertices:



We fix notation: let g be the reflection through the vertical line bisecting vertex 1; let h be the anticlockwise rotation by $\frac{2\pi}{5}$ radians.

What is the centralizer of h? This is the set of all elements in D_5 which commute with h. This clearly includes all powers of h:

$$h^n h = h^{n+1} = hh^n$$

so:

$$\{e, h, h^2, h^3, h^4\} \subseteq C_G(h)$$

Moreover, $g \notin C_G(h)$. This is because gh^n represents a reflection, so:

$$(gh^k)^2 = e \implies gh^k gh^k = e \implies gh^k = h^{n-k}g$$

In particular, we must have:

$$gh = h^4 g = h^{-1} g \neq hg$$

so g doesn't commute with h.
But since $|C_G(h)|$ divides $|G|$ by the Theorem above, $|C_G(h)| = 5$ or $|C_G(h)| = 10$ (since it contains at least 5 elements). Since $g \notin C_G(h)$ it can **only** contain 5 elements, so:

$$\{e, h, h^2, h^3, h^4\} = C_G(h)$$

What about the conjugacy classes? Which elements are generated by conjugating with h?

$$aha^{-1}$$

By the theorem above, we must have 2 elements. If $a = e$, then we generate h:

$$ehe^{-1} = h$$

In fact, since rotations commute, they will always generate h:

$$h^k(h)h^{-k} = h(h^k h^{-k}) = h$$

What about reflection?

$$ghg^{-1} = h^{-1} = h^4$$

(here we use $gh^k g = h^{-k}$).
Hence:

$$Cl(h) = \{h, h^4\}$$

1.10 The Centre of Prime Groups

1.10.1 Definition: p-group

*A **p-group** is a group in which each element has an order of a **power** of p, where p is **prime**.*

1.10.2 Lemma: Finite p-group

*Let G be **finite**, then:*

$$G \text{ is a p-group} \iff \exists n \in \mathbb{N} \ : \ |G| = p^n$$

Proof.

- ($\implies$): assume G is a finite p-group, and that every element has an order of the form p^k, for some $k \in \mathbb{N}$. Now, assume there is a prime q which divides $|G|$. By Cauchy's Theorem, this implies that there exists an element $g \in G$ with order q. But all elements in G have orders of the form p^k, so $q = p^k$. Hence, any divisor of $|G|$ must be a power of p, so $|G|$ is a power of p.
- ($\impliedby$): assume that $|G| = p^n$. All the elements of G must have an order which divides $|G|$ by Lagrange's Theorem, so every element must be a power of p.

□

1.10.3 Definition: Centre of a Group

*The **centre** of a group G is the set of all $g \in G$ which commute with every element of G:*

$$Z(G) = \{g \mid \forall h \in G, gh = hg, g \in G\}$$

1.10.4 Theorem: p-groups Have Non-Trivial Centres

*Let G be a **non-trivial, finite p-group**. Then:*

$$Z(G) \neq \{e\}$$

*That is, the **centre** is **non-trivial**.*
(Theorem 4.2.12)

We will use the **class equation**, which tells us that there are representatives $a_i \in G$ such that:

$$|G| = \sum_{i=1}^{n} |Cl(a_i)|$$

. Notice, by Lagrange's Theorem:

$$|G| = |C_G(a_i)||Cl(a_i)|$$

Since G is a p-group, $|G| = p^k$, and it must be the case that:

$$p \mid |Cl(a_i)| \implies \exists r_i \ : \ |Cl(a_i)| = p^{r_i}$$

Now, notice that if $a \in Z(G)$, a commutes with every element of G, so:

$$Cl(a) = \{gag^{-1} \mid g \in G\} = \{a(gg^{-1}) \mid g \in G\} = \{a\}$$

Similarly, if $Cl(a) = \{a\}$, then:

$$\forall g \in G, \ gag^{-1} = a \implies ga = ag$$

so a commutes with every element in G.

Hence, we have that:

$$a \in Z(G) \iff Cl(a) = \{a\}$$

But then, we can rewrite the class equation as:

$$|G| = p^k = \sum_{a_i \in Z(G)} |Cl(a_i)| + \sum_{a_i \notin Z(G)} |Cl(a_i)| = |Z(G)| + \sum_{a_i \notin Z(G)} |Cl(a_i)|$$

But $|Cl(a_i)| = p^{r_i} > 1$ (since a_i isn't in the centraliser, so the conjugacy class contains more than 1 element), and $|G| = p^k$, so p divides their difference; in other words:

$$p \mid |Z(G)|$$

Hence, $|Z(G)| \geq 2$, so $Z(G)$ is non-trivial.

1.10.5 Revision Exercises

1. **Show that if G is a group with $|G| = p^2$, where p is prime, then G is abelian.**

2 The Sylow Theorems

2.1 Motivation for the Sylow Theorems

The Sylow Theorems can be thought of as generalising Cauchy's Theorem to powers of p. They are particularly useful in the study of **normal subgroups**. Normal subgroups are very important, because they help define **simple groups**, which in turn can be used to "decompose" all finite group. So understanding simple groups is fundamental to understanding the structure of all finite groups. To study simple groups, we require the tools provided by the Sylow Theorems.

2.2 Definition: p-Subgroups

*Let G be a **finite group**. A **p-subgroup** is **subgroup** of G which is a **p-group** (so its order is a power of p, where p is **prime**).*

2.3 Definition: Sylow p-Subgroups

*Let G be a **finite group**. A **Sylow p-subgroup** is a **p-subgroup** whose order is the **highest** power of p which divides $|G|$.*
*If p **doesn't** divide $|G|$, then $\{e\}$ is the unique Sylow p-subgroup, known as the **trivial Sylow p-subgroup**.*

2.4 Theorem: Sylow I

The First Sylow Theorem states that non-trivial Sylow p-subgroups always exist.

---

*Let $|G| = n$ and suppose that p is a **prime** such that:*

$$p \mid n$$

We can thus write:

$$|G| = n = p^m r, \qquad p \nmid r$$

*Then, there exists **at least** one **Sylow p-subgroup**, which will be a **subgroup** of order p^m.*
(Theorem 4.1.2)

2.5 Theorem: Sylow II

*The Second Sylow Theorem states that **all** Sylow p-subgroups are **conjugate**.*

*Let $|G| = n$ and suppose that p is a **prime** such that:*

$$p \mid n$$

We can thus write:

$$|G| = n = p^m r, \qquad p \nmid r$$

*Suppose that P is a **Sylow p-subgroup** and that:*

$$H \leq G$$

*is **any** p-subgroup of G.*
Then:

$$\exists x \in G \ : \ H \subseteq xPx^{-1}$$

*In particular, if P, P' are **Sylow p-subgroups**, since:*

$$|xPx^{-1}| = |P|$$

and:

$$|P| = |P'|$$

it follows that: this means that:

$$\exists x \in G \ : \ P' \subseteq xPx^{-1} \implies \exists x \in G \ : \ P' = xPx^{-1}$$

*Hence, **any** 2 **Sylow p-subgroups** of G are **conjugate** in G.*
(Theorem 4.1.3)

2.5.1 Corollary: Normal Subgroups and Unique Sylow p-Subgroups

Let $|G| = p^m r$ where p doesn't divide r.
Let P be a Sylow p-subgroup of G.
Then:

$$P \triangleleft G \iff P \text{ is the unique Sylow p-subgroup}$$

*That is, a Sylow p-subgroup is normal **if and only if** it is the **unique** Sylow p-subgroup:*

$$P \triangleleft G \iff n_p = 1$$

(Lemma 4.19 & Corollary 4.3.2)

Proof.

- ($\implies$) Assume that $P \triangleleft G$. By Sylow II, all Sylow p-subgroups are conjugate to P. n_p is the number of Sylow p-subgroups, so in particular, it is the number of Sylow p-subgroups which are conjugate to P. But by definition, a subgroup is normal **if and only if** it has a unique conjugate, so $n_p = 1$, and thus, P must be a normal subgroup.
- ($\impliedby$) Let P the unique Sylow p-subgroup. Then for any $g \in G$, gPg^{-1} is a subgroup of order $|P|$. Since P is the only such subgroup:

$$\forall g \in G, gPg^{-1} = P$$

so P will be a normal subgroup.

□

2.6 Theorem: Sylow III

*The Third Sylow Theorem gives us information about the **number** of Sylow p-subgroups.*

*Let $|G| = n$ and suppose that p is a **prime** such that:*

$$p \mid n$$

We can thus write:

$$|G| = n = p^m r, \qquad p \nmid r$$

*Let n_p be the number of **distinct Sylow p-subgroups** of G. Then:*

$$n_p \mid r \qquad n_p \equiv 1 \ (mod\ p)$$

(Theorem 4.1.4)

2.7 Applications/Examples of Sylow Theorems

2.7.1 Example: Verifying Sylow on S_3

We have that:

$$|S_3| = 6 = 3 \times 2$$

So Sylow I predicts subgroups of order 2 and 3.

Since the transpositions are their own inverses, they certainly form subgroups with themselves and the identity:

$$\{e, (1\ 2)\} \qquad \{e, (1\ 3)\} \qquad \{e, (2\ 3)\}$$

so $n_2 = 3$, and indeed, $3 \mid 3$ and $3 \equiv 1\ (mod\ 2)$, as predicted by Sylow III. It can also be shown that the transpositions are conjugate (this is a property of transpositions in S_n).

There is only one subgroups of order 3:

$$\{e, (1\ 2\ 3), (1\ 3\ 2)\}$$

which is trivially conjugate to itself, and $1 \mid 3$, $1 \equiv 1\ (mod\ 3)$ as required.

2.7.2 Example: Verifying Sylow on D_6

We have:

$$|D_6| = 12 = 4 \times 3 = 3 \times 4$$

so Sylow I predicts subgroups of order 3 and 4. Moreover:

$$n_2 \mid 3 \qquad n_2 \equiv 1 \ (mod\ 2)$$

(so there are 1 or 3 subgroups of order 4)

$$n_3 \mid 4 \qquad n_3 \equiv 1 \ (mod\ 3)$$

(so there are 1 or 4 subgroups of order 3)

Let g be reflections, and h be rotations by $\pi/3$ anticlockwise. Notice, the subgroups of order 3 must be cylic. h^2 generates a cylic subgroup of order 3. Moreover, any element of D_6 which isn't a power of h will be a reflection:

$$(gh^k)(gh^k) = (gh^k g)h^k = h^{-k}h^k = e$$

Since reflections have order 2, they can't generate a subgroup or order 3, so $\langle h^2 \rangle$ is the only Sylow 3-subgroup.

Now, lets consider the Sylow 2-subgroups. Notice, the gh^k are reflections, so theya re their own inverses. We can consider the sets in which each element are their own inverses:

$$\{e, g, h^3, gh^3\} \qquad \{e, gh, h^3, gh^4\} \qquad \{e, gh^2, h^3, gh^5\}$$

These are clearly closed, and inverses exist by construction, so these are all subgroups. There are 3 of them, as predicted by Sylow III (these groups are isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$)

> *D_6 has no element of order 4, so the Sylow 2-subgroups couldn't have been isomorphic to $\mathbb{Z}_4$. The only remaining group of order 4 is $\mathbb{Z}_2 \times \mathbb{Z}_2$.*

2.7.3 Proposition: Normal Subgroups in Groups of Order 30

> *Any group of order 30 has a **non-trivial normal subgroup**. (Proposition 4.1.7)*

Let G be a group of order 30. We can decompose it into prime factors:

$$|G| = 30 = 2 \times 3 \times 5$$

Sylow I thus predicts the existence of Sylow 2-subgroups, Sylow 3-subgroups and Sylow 5-subgroups. It is sufficient to prove that one of the Sylow 3-subgroups or Sylow 5-subgroups is normal.

By Sylow III, we know the following:

$$n_5 \mid 6 \qquad n_5 \equiv 1 \ (mod\ 5)$$

Since $n_5 \leq 6$, it must thus be the case that $n_5 = 1$ (so there is a unique Sylow 5-subgroup) or $n_5 = 6$ (so there are 6 Sylow 5-subgroups).

Similarly:

$$n_3 \mid 10 \qquad n_3 \equiv 1 \ (mod\ 3)$$

Since $n_3 \leq 10$, it must thus be the case that $n_3 = 1$ (so there is a unique Sylow 3-subgroup) or $n_3 = 10$ (so there are 10 Sylow 3-subgroups).

We now claim that at least one of n_3, n_5 must be 1. We proceed by contradiction: assume neither is 1. Then:

$$n_3 = 10 \qquad n_5 = 6$$

Let $P_i, i \in [1, 6]$ be the 6 Sylow 5-subgroups. Since $|P_i| = 5$ is prime, P_i will be cyclic, by Lagrange's Theorem. Since the 6 Sylow 5-subgroups are **distinct** and **cyclic**, they can't share elements in common (except the identity), so:

$$\forall i, j \in [1, 6], i \neq j \implies P_i \cap P_j = \{e\}$$

Similarly, if $Q_i, i \in [1, 10]$ are the 10 Sylow 3-subgroups, we have $|Q_i| = 3$, so the Q_i will also be cyclic, and:

$$\forall i, j \in [1, 10], i \neq j \implies Q_i \cap Q_j = \{e\}$$

But now, lets consider how many elements are in these Sylow subgroups. For the Sylow 5-subgroups, exploiting their disjoint nature tells us:

$$\bigcup_{i=1}^{6} |P_i| = 1 + (5 - 1) \times 6 = 25$$

For the Sylow 3-subgroups:

$$\bigcup_{u=1}^{10} |Q_i| = 1 + (3 - 1) \times 10 = 21$$

But since these are subgroups, this implies that:

$$|G| = 30 \geq 25 + 21 = 46$$

which is a contradiction.

Hence, we must have $n_3 = 1$ or $n_5 = 1$.

Lets assume that $n_3 = 1$. Then, G has a unique subgroup of order 3 (namely the Sylow 3-subgroup). Call it P. But now, for any $g \in G$:

$$gPg^{-1} \leq G$$

(conjugation always produces subgroups). But $|gPg^{-1}| = |P| = 3$, so gPg^{-1} must be a subgroup of order 3. Since P is the only such subgroup:

$$\forall g \in G, gPg^{-1} = P$$

so P must be a normal subgroup.

The same argument applies when $n_5 = 1$.

Notice, the intersection of Sylow p-subgroups isn't always trivial: the above arguments relied on the fact that the subgroups had prime order. For instance, as we showed above, the Sylow 2-subgroups of D_6 all contain h^3.

2.8 Simple Groups

2.8.1 Definition: Simple Groups

*A group G is **simple** if the **only** normal subgroups of G are trivial:*

$$\{e\} \qquad G$$

3 Proving the Sylow Theorems

3.1 Sylow I

3.1.1 Theorem: Sylow I

*Let $|G| = n$ and suppose that p is a **prime** such that:*

$$p \mid n$$

We can thus write:

$$|G| = n = p^m r, \qquad p \nmid r$$

*Then, there exists **at least** one **Sylow p-subgroup**, which will be a **subgroup** of order p^m.*
(Theorem 4.1.2)

Proof. We shall exploit group actions. Define the following set:

$$X = \{A \mid A \subseteq G, |A| = p^m\}$$

that is, X is the set of all **subsets** of G with cardinality p^m.

Now, for any $g \in G$:

$$|gA| = |A|, \qquad A \in X$$

since the mapping:

$$A \to gA \qquad a \mapsto ga$$

is a bijection (the inverse is just $ga \mapsto g^1(ga) = a$).

Now, we claim that there exists an orbit when G acts on X, such that the orbit has a cardinality which

isn't divisble by p. X is obtained by choosing p^m elements from a set of $p^m r$ elements, so:

$$\begin{aligned}
|X| &= \binom{p^m r}{p^m} \\
&= \frac{(p^m r)!}{(p^m)!(p^m r - p^m)!} \\
&= \frac{p^m r(p^m r - 1)(p^m r - 2)\dots(p^m r - (p^m - 1))}{(p^m)!} \\
&= \frac{p^m r(p^m r - 1)(p^m r - 2)\dots(p^m r - (p^m - 1))}{p^m(p^m - 1)(p^m - 2)\dots(p^m - (p^m - 1))}
\end{aligned}$$

Now, if we let $s \in [1, p^m]$, let k be the highest power of p dividing both:

$$p^m r - s \qquad p^m - s$$

Clearly, p^k divides both $p^m r$ and p^m, so if it divides both, k must be the highest power of p dividing s. Hence, the numerator and denominator of $|X|$ have as a common factor a power of p. These cancel out, meaning that p doesn't divide X. But recall, by the class equation we can partition X into its orbits, such that $\exists A_1, A_2, \dots, A_n$:

$$|X| = \sum_{i=1}^{n} |Orb_G(A_i)|$$

But since p doesn't divide $|X|$, there must be at least one $Orb_G(A_*)$ such that p doesn't divide $Orb_G(A_*)$.

Now, we apply the Orbit-Stabilizer Theorem to this element $A_* \in X$:

$$|G| = p^m r = |Stab_G(A_*)||Orb_G(A_*)|$$

Since p doesn't divide $|Orb_G(A_*)|$, we must then have that:

$$p^m \mid |Stab_G(A^*)|$$

(we can't immediately conclude that $|Stab_G(A^*)| = p^m$, since if r is composite and $r = ab$, then it can be the case that $|Stab_G(A^*)| = ap^m$).

But now, select some $a \in A_*$. Then:

$$(Stab_G(A_*)) \cdot a \subseteq A_*$$

since $Stab_G(A_*)$ is the set of all $g \in G$ which fix A_*:

$$g \cdot A_* = A_* \implies ga \in A_*, \qquad \forall a \in A_*$$

Hence, we have:

$$|(Stab_G(A_*)) \cdot a| = |Stab_G(A_*)| \leq |A_*| = p^m$$

Since $p^m \mid |Stab_G(A^*)|$ but $|Stab_G(A_*)| \leq p^m$, it can only be the case that:

$$|Stab_G(A_*)| = p^m$$

But recall, a property of the stabilizer is that it is a subgroup of G. Hence, we have found a subgroup of g of order p^m, as required for Sylow I.

□

3.2 Sylow II

3.2.1 Theorem: Sylow II

*Let $|G| = n$ and suppose that p is a **prime** such that:*

$$p \mid n$$

We can thus write:

$$|G| = n = p^m r, \qquad p \nmid r$$

*Suppose that P is a **Sylow p-subgroup** and that:*

$$H \leq G$$

*is **any** p-subgroup of G.*
Then:

$$\exists x \in G \ : \ H \subseteq xPx^{-1}$$

*In particular, if P, P' are **Sylow p-subgroups**, since:*

$$|xPx^{-1}| = |P|$$

and:

$$|P| = |P'|$$

it follows that:

$$\exists x \in G \ : \ P' \subseteq xPx^{-1} \implies \exists x \in G \ : \ P' = xPx^{-1}$$

*Hence, **any** 2 **Sylow p-subgroups** of G are **conjugate** in G.*
(Theorem 4.1.3)

Proof. We begin by proving the following Lemma:

*Let p be prime, and let G be a **finite p-group**, acting on a **finite** set X.*
*Then, if X_0 is the set of **fixed points** of X under G:*

$$|X_0| \equiv |X| \ (mod\ p)$$

(Lemma 4.3.1)

Consider the **representatives** of all the orbits of X, which aren't fixed points: $x_1, \ldots, x_n \in X \setminus X_0$. Since x_i is not a fixed point, $|Stab_G(x_i)| < |G|$, so $Stab_G(x_i)$ must be a proper subgroup of G, so by the Orbit-Stabilizer Theorem:

$$|Orb_G(x_i)| > 1$$

and $|Orb_G(x_i)|$ must divide $|G|$. Since G is a finite p-group, we must have that $|G| = p^n$, so $|Orb_G(x_i)|$ must be some power of p, $p^k, k > 0$.

Finally, the orbits partition X, so we can write:

$$X = X_0 \sqcup Orb_G(x_1) \sqcup \ldots \sqcup Orb_G(x_n)$$

so

$$|X| = |X_0| + \sum_{i=1}^{n} |Orb_G(x_i)| \implies |X_0| \equiv |X| \ (mod\ p)$$

where we use the fact that $\forall i \in [1, n], p \mid |Orb_G(x_i)|$.

We can now prove Sylow II.

We consider:

- P to be a Sylow p-subgroup, such that $|P| = p^m$
- H to be any other p-subgroup
- the **action** of H on the set of cosets G/P via:

$$h \cdot (gP) = (hg)P$$

Now, since P is a Sylow p-subgroup, $|P| = p^m$, so by Lagrange's Theorem:

$$|G/P| = r$$

and p doesn't divide r.

By the Lemma we just proved, if X_0 is the set of fixed points of G/P, then:

$$|X_0| \equiv |G/P| \ (mod\ p)$$

Hence, $|X_0| \equiv\ r \ (mod\ p)$, so in particular $|X_0| > 0$, so the action of H on G/P has at least one fixed point.

Suppose that $xP \in X_0$. Then by definition of a fixed point:

$$\forall h \in H \qquad h(xP) = (hx)P = xP$$

which is true **if and only if**:

$$\forall h \in H, \qquad x^{-1}hx \in P$$

Thus, it follows that:

$$x^{-1}Hx \subseteq P \iff H \subseteq xPx^{-1}$$

as required.

If H is a Sylow p-subgroup, then:

$$|H| = |P| = |xPx^{-1}|$$

which forces:

$$H = xPx^{-1}$$

and so any 2 Sylow p-subgroups are conjugate.

□

3.3 Sylow III

3.3.1 Definition: Normalizer

*Let G be a **group**, and $H \leq G$. Define the **normalizer** of H as the set:*

$$N_G(H) = \{g \mid g \in G : gHg^{-1} = H\}$$

3.4 Lemma: Properties of the Normalizer

1. *$N_G(H) \leq G$ and $H \triangleleft N_G(H)$ (in fact, $N_G(H)$ will be the **largest** subgroup of G with H as a normal subgroup)*
2. $$H \triangleleft G \iff N_G(H) = G$$
   We can think of $N_G(H)$ as indicating how "close" H is of being a normal subgroup of G)
3. *For any subgroup $H \leq G$:*
   $$|G/N_G(H)| = \text{the number of distinct conjugate subgroups to } H$$
4. *Let $p \mid |G|$ and let P be a **Sylow p-subgroup** of G. Then:*
   $$n_p = |G/N_G(P)|$$

Proof.

(1) $N_G(H) \leq G$ and $H \triangleleft N_G(H)$

Firstly, $N_G(H)$ is non-empty, since $e \in N_G(H)$. Hence, $N_G(H) \leq H$ if $n_1, n_2 \in N_G(H)$ implies that $n_1 n_2^{-1} \in N_G(H)$. Since $n_1, n_2 \in N_G(H)$ then:

$$n_1 H n_1^{-1} = H \qquad n_2 H n_2^{-1} = H$$

Hence:

$$\begin{aligned}(n_1 n_2^{-1})H(n_1 n_2^{-1})^{-1} &= (n_1 n_2^{-1})H(n_2 n_1^{-1}) \\ &= n_1 H n_1^{-1} \\ &= H\end{aligned}$$

so $N_G(H) \leq G$ as required.

Clearly, $H \subseteq N_G(H)$, since for any $h \in H$:

$$hHh^{-1} = H$$

by closure of the subgroup. Moreover, $H \leq G$, so it is a subgroup, and $H \leq N_G(H)$. By definition, $\forall g \in N_G(H), gHg^{-1} = H$, so H will be a normal subgroup of $N_G(H)$.

(2) $H \triangleleft G \iff N_G(H) = G$

If $H \triangleleft G$, then $\forall g \in G$:

$$gHg^{-1} = H$$

Hence:

$$N_G(H) = G$$

On the other hand, if $N_G(H) = G$, then:

$$\forall g \in G, \quad gHg^{-1} = H$$

so H is normal by definition.

(3) **The number of conjugate subgroups to H is $|G/N_G(H)|$**

Define X to be the set of all subgroups of G which are **conjugate** to H. That is:

$$X = \{K \mid K \leq G \ \wedge \exists g \in G : gHg^{-1} = K\}$$

Define the action of G on X via conjugation:

$$a \cdot (bHb^{-1}) = (ab)H(ab)^{-1}$$

Then:

$$Orb_G(H) = \{aHa^{-1} \mid a \in G\} = X$$

Moreover:

$$Stab_G(H) = \{a \mid a \in G : aHa^{-1} = H\} = N_G(H)$$

Hence, by the Orbit-Stabilizer Theorem:

$$|G| = |N_G(H)||X| \implies |X| = |G|/|N_G(H)| = |G/N_G(H)|$$

as required.

(4) $p \mid |G| \implies n_p = |G/N_G(P)|$

Since P is a Sylow p-subgroup, then the number of conjugates to P is precisely n_p (Sylow II says that all p-subgroups are conjugates of P), so from the claim above:

$$n_p = |G/N_G(P)|$$

as required.

□

3.4.1 Theorem: Sylow III

*Let $|G| = n$ and suppose that p is a **prime** such that:*

$$p \mid n$$

We can thus write:

$$|G| = n = p^m r, \qquad p \nmid r$$

*Let n_p be the number of **distinct Sylow p-subgroups** of G. Then:*

$$n_p \mid r \qquad n_p \equiv 1 \ (mod\ p)$$

(Theorem 4.1.4)

Proof. We have that $|G| = p^m r$, and by the previous lemma, if P is a Sylow p-subgroup, then:

$$n_p = |G/N_G(P)| = |G|/|N_G(P)|$$

But then:

$$|G| = p^m r \implies r = \frac{|G|}{|P|} = \frac{|G|}{|N_G(P)|}\frac{|N_G(P)|}{|P|} = n_p \frac{|N_G(P)|}{|P|}$$

Since $P \leq N_G(P)$, then $|P| \mid |N_G(P)|$ and so $\frac{|N_G(P)|}{|P|} \in \mathbb{Z}$. Hence, we have that:

$$n_p \mid r$$

as required.

For the second claim, define X to be the set of all Sylow p-subgroups of G. Consider $P \in X$ acting on X via conjugation.

Recall, when proving Sylow II, we showed that:

*Let p be prime, and let G be a **finite p-group**, acting on a **finite** set X. Then, if X_0 is the set of **fixed points** of X under G:*

$$|X_0| \equiv |X| \ (mod\ p)$$

(Lemma 4.3.1)

Hence, we will have that the set of fixed points X_0 of X under P is such that:

$$|X_0| \equiv n_p \ (mod\ p)$$

We claim that:

$$X_0 = \{P\}$$

such that $|X_0| = 1$.

Clearly, $P \in X_0$, since $\forall p \in P$:

$$pPp^{-1} = P$$

Now, suppose $\exists Q \in X_0$. Then:

$$\forall p \in P, \qquad pQp^{-1} = Q$$

In particular, this means that:

$$P \subseteq N_G(Q)$$

Hence, since P, Q are Sylow p-subgroups of G, it follows that P, Q are also Sylow p-subgroups of $N_G(Q)$ (since $|N_G(Q)| \leq |G|$, and P, Q are subgroups in G, and subsets of $N_G(Q)$). Moreover, we showed that:

$$Q \triangleleft N_G(Q)$$

which is true **if and only if** $n_p = 1$, so Q must be the only Sylow p-subgroup, and so $P = Q$.

Hence, P is the only fixed point, and so:

$$1 \equiv n_p \ (mod\ p) \implies n_p \equiv 1 \ (mod\ p)$$

as required. □