3 Conjugacy

Definition : 1) An element $g \in G$, a group, is <u>conjugate</u> to $g' \in G$ if and only if there exists $h \in G$ such that :

$$hgh^{-1} = g'$$

2) The orbit under conjugation of $g \in G$ is called the <u>conjugacy class</u> of g. We denote this class by $ccl_G(g)$.

So $ccl_G(g) = \{hgh^{-1} \mid h \in G\}$

Examples : 0) The identity element e in a group G is a conjugacy class of its own.

$$\begin{aligned} G(e) &= \{g(e) \mid g \in G\} \\ &= \{\underbrace{geg^{-1}}_{e} \mid g \in G\} \\ &= \{e \mid g \in G\} \\ &= \{e\}. \end{aligned}$$

1) In an abelian group G, any conjugacy class has size (cardinality) equal to 1.

$$\begin{aligned} G(g) &= \{g'(g) \mid g' \in G\} \\ &= \{g'gg'^{-1} \mid g' \in G\} \\ &= \{g \mid g' \in G\} \quad ; \ G \text{ abelian}, \ g'g = gg' \\ &= \{g\}. \end{aligned}$$

Consequence : in an abelian group all the conjugacy classes consist of a single element.

Conversely, suppose G acts on itself by conjugation, and each conjugacy class is of size 1, then G must be abelian.

Take $g, h \in G$, to prove : $gh = hg$, i.e. $ghg^{-1} = h$.

But ghg^{-1} is in the orbit of h ;

$$G(h) = \{\underbrace{g(h)}_{ghg^{-1}} \mid g \in G\}$$

and by assumption, this orbit has a single element.
Also h is in this orbit, so ghg^{-1} and h have to agree.

Conclusion: G is abelian, giving:

Proposition: Conjugacy classes in G are all size 1 $\Leftrightarrow$ G is abelian.

Examples: 1)
$$\begin{aligned} C_n &= \text{cyclic group of order } n, \quad n \geq 1 \\ &= \{ e^{2\pi i k/n} \mid k \in \mathbb{Z} \} \\ &= \{ e^{2\pi i k/n} \mid 0 \leq k < n \} \end{aligned}$$

C_n is abelian so has conjugacy classes:
$$\{e^0\}, \{e^{2\pi i/n}\}, \ldots, \{e^{2\pi i(n-1)/n}\}.$$

2) The symmetric group S_3.

$$ccl_{S_3}(e) = \{e\}$$

$$ccl_{S_3}((123)) = \left\{ \left. \begin{array}{l} e(123)e^{-1}, \\ (123)(123)(123)^{-1}, \\ (321)(123)(321)^{-1}, \end{array} \right\} = (123) \quad \left. \begin{array}{l} (12)(123)(12)^{-1}, \\ (13)(123)(13)^{-1}, \\ (23)(123)(23)^{-1} \end{array} \right\} = (132) \right\}$$

$$\begin{aligned} &= \{(123), (132)\} \\ &= ccl_{S_3}((132)). \end{aligned}$$

$$\begin{aligned} ccl_{S_3}((12)) &= \{(12), (13), (23)\} \quad (\text{Exercise}) \\ &= ccl_{S_3}((13)) \\ &= ccl_{S_3}((23)) \end{aligned}$$

Conclusion: The conjugacy classes in S_3 are
$$\{e\}, \{(123), (132)\}, \{(12), (13), (23)\}.$$

ie all 1-cycles together, all 2-cycles together, and all 3-cycles together, in one conjugacy class each.

3) $A_3 \leq S_3$ is abelian, so conjugacy classes are:
$$\{(1)\}, \{(123)\}, \{(132)\}.$$

4) The Dihedral group

$$D_5 = \langle r, h \mid r^5 = h^2 = e,\ hr = r^{-1}h \rangle$$

has its elements listed as: $\{ r^j h^i \mid 0 \le j \le 4,\ 0 \le i \le 1 \}$

Conjugacy class of r^k, in D_5, k fixed $(0 \le k \le 4)$:

$$\begin{aligned}
ccl_{D_5}(r^k) &= \{ r^j h^i r^k (r^j h^i)^{-1} \mid 0 \le j \le 4,\ 0 \le i \le 1 \} \\
&= \{ r^j h^i r^k h^{-i} r^{-j} \mid 0 \le j \le 4,\ 0 \le i \le 1 \} \\
&= \{ r^j r^k r^{-j} \mid 0 \le j \le 4,\ i = 0 \} \\
&\quad \cup \{ r^j h r^k h r^{-j} \mid 0 \le j \le 4,\ i = 1 \} \\
&= \{ r^k \} \cup \{ \underbrace{r^j h h r^{-k} r^{-j}}_{r^{-k}} \mid 0 \le j \le 4 \} \\
&= \{ r^k, r^{-k} \}.
\end{aligned}$$

This has two elements for $1 \le k \le 4$, and one element for $k = 0$.

Similarly for $r^k h$, k fixed:

$$\begin{aligned}
ccl_{D_5}(r^k h) &= \{ r^j r^k h r^{-j} \mid 0 \le j \le 4,\ i = 0 \} \\
&\quad \cup \{ r^j h r^k h h r^{-j} \mid 0 \le j \le 4,\ i = 1 \} \\
&= \{ r^j r^k r^j h \mid 0 \le j \le 4 \} \\
&\quad \cup \{ r^j r^{j-k} h \mid 0 \le j \le 4 \} \\
&= \{ r^{2j+k} h \mid 0 \le j \le 4 \} \\
&\quad \cup \{ r^{2j-k} h \mid 0 \le j \le 4 \}.
\end{aligned}$$

These are the same set since $r^{2j} = r^0, r^2, r^4, r^6 = r, r^8 = r^3$

$$= \{ r^i h \mid 0 \le i \le 4 \}$$

independent of k.

Summary: the conjugacy classes in D_5 are:

$\{e\}$, $\{r, r^{-1}\} = \{r^4, r^{-4}\}$, $\{r^2, r^{-2}\} = \{r^3, r^{-3}\}$,
$\{h, rh, r^2h, r^3h, r^4h\}$.

These are the orbits. Stabilizers:

$$\begin{aligned}
G_e &= \{ g \in G \mid geg^{-1} = e \} = D_5 \\
G_r &= \langle r \rangle = G_{r^2} = G_{r^3} = G_{r^4} \quad \text{(5 elements in each)} \\
G_{r^k h} &= \{ e, r^k h \} \quad \text{(2 elements in each)}
\end{aligned}$$

Exercise: Work out Cayley's Theorem for $G = S_3$ acting on itself by conjugation

Prepare for statement relating orbits and stabilizers.

Recall: A (left) coset of a subgroup $H \leq G$ is an equivalence class under the equivalence relation $\sim$, where

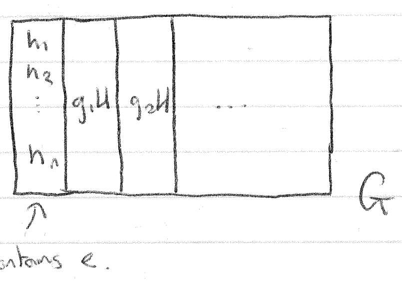
$$g_1 \sim g_2 \iff g_1^{-1} g_2 \in H$$

The equivalence classes, denoted

$$gH = \{ gh \mid h \in H \}$$

are then called (left) cosets of H in G.

Note: G is split into slices of the same size, i.e. $|H|$



Theorem: (Orbit-Stabilizer Theorem)

Suppose G acts on a set X, then for any $x \in X$, there is a bijection:

$$\beta : G(x) \xrightarrow{1:1} \{ \text{left cosets of } G_x \text{ in } G \}$$

given by

$$g(x) \longmapsto g\, G_x$$

Proof: Preconsideration

$$\begin{aligned} g(x) = h(x) &\iff \underbrace{g^{-1}g}_{e}(x) = g^{-1}h(x) \\ &\iff x = g^{-1}h(x) \\ &\iff g^{-1}h \in G_x \\ &\iff g^{-1}h\, G_x = G_x \\ &\iff h\, G_x = g\, G_x . \end{aligned}$$

From this we get

i) Well-definedness of β (using $\Longrightarrow$)

ii) Injectivity of β (using $\Leftarrow$)

For iii) Surjectivity:

Given any coset C on RHS, we take any element in it, say $\tilde{g}$.

So then $C = \tilde{g} G_x$

[$\tilde{g} = \tilde{g}e$ is in both, and equivalence classes are disjoint or agree]

Then take $\tilde{g}(x)$, for which

$$\beta(\tilde{g}(x)) = \tilde{g} G_x = C$$

Corollary: If G is finite, acting on a finite set X, then

$$|G(x)| \cdot |G_x| = |G|, \text{ for any } x \in X.$$

ie. The size of its orbit $G(x)$ is 'complementary' to the size of its stabilizer G_x.

Proof: By the Orbit-Stabilizer Theorem, get

$$G(x) \overset{1:1}{\longleftrightarrow} \{\text{left cosets of } G_x \text{ in } G\}$$
$$\Rightarrow |G(x)| = |\{\text{left cosets of } G_x \text{ in } G\}|$$

But all the cosets under G_x have the same size, ie.

$$|G_x| = |eG_x| = |gG_x| \text{ for any } g \in G.$$

Hence $\frac{|G|}{|G_x|}$ is the number of cosets of G_x in G, so

$$|G(x)| = \frac{|G|}{|G_x|}$$

Claim follows.

Note: This still makes sense for infinite groups if we write it as $|G(x)||G_x| = |G|$.

[Calculus for cardinal numbers]

Corollary: If the finite group G acts on (itself (by conjugation)) or the finite set X, then the orbit lengths all divide the group order.

$$\forall x \in X \quad |G(x)| \text{ divides } |G|.$$

In particular, the size of the conjugacy classes in G divide $|G|$

Examples: 1) D_n, for n odd has orbits and stabilizers under conjugation as:

Elements	e	$r \quad r^{-1}$	$r^2 \quad r^{-2}$	$\cdots$	$r^{\frac{n-1}{2}} \quad r^{-\frac{(n-1)}{2}}$	h	rh	$\cdots$	$r^{n-1}h$
Orbits	$\{e\}$	$\{r, r^{-1}\}$	$\{r^2, r^{-2}\}$	$\cdots$	$\{r^{\frac{n-1}{2}}, r^{-\frac{(n-1)}{2}}\}$	$\{h, rh, \ldots, r^{n-1}h\}$			
Sizes	1	2	2	$\cdots$	2	n			
Stabilizers	D_n	$\langle r\rangle$	$\langle r\rangle$	$\cdots$	$\langle r\rangle$	$\langle h\rangle$	$\langle rh\rangle$	$\cdots$	$\langle r^{n-1}h\rangle$
Sizes	$2n$	n	n	$\cdots$	n	2	2	$\cdots$	2

2) For infinite groups:

$G = \mathbb{Z}$ acting on $X = \mathbb{R}$ by

$$n \longmapsto \varphi(n) : \mathbb{R} \longrightarrow \mathbb{R}$$
$$r \longmapsto (-1)^n r.$$

Elements	0	$r \neq 0$
Orbits	$\{0\}$	$\{r, -r\}$
Sizes	1	2
Stabilizers	$\mathbb{Z}$	$2\mathbb{Z}$
Sizes of set of cosets in $\mathbb{Z}$	1	2
(order of quotient group)	$\lvert\mathbb{Z}/\mathbb{Z}\rvert = 1$	$\lvert\mathbb{Z}/2\mathbb{Z}\rvert = 2$

Question: Let G act on X. Suppose x and y are in the <u>same</u> G-orbit. Then G_x and G_y are conjugate to each other, and, so $|G_x| = |G_y|$, ie.

$$G_x = h G_y h^{-1}, \text{ for some } h \in G$$

Proof: x, y in the same orbit means $x = h(y)$ for some $h \in G$.

ANT: G

Now $G_x = \{ g \in G \mid g(x) = x \}$, rewrite

$$G_x = G_{h(y)}$$
$$= \{ g \in G \mid g(h(y)) = h(y) \}$$
$$= \{ g \in G \mid \underbrace{h^{-1}(g(h(y)))}_{:= g'(y)} = \underbrace{h^{-1}h(y)}_{y} \}$$

So $h^{-1}gh = g' \Rightarrow g = hg'h^{-1}$

$$= \{ hg'h^{-1} \mid g'(y) = y \}$$
$$= h \underbrace{\{ g' \mid g'(y) = y \}}_{G_y} h^{-1}$$

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

Use action of a group on a set for the first 'structural' result on groups, a partial converse to Lagrange's Theorem.

Theorem: (Cauchy)

Let G be a finite group and p a prime such that $p \mid |G|$. Then there is a subgroup of G of order p.

Proof: Want to find an $x \in G$ st $x^p = e$, $x \neq e$.

Idea: Look at $\underbrace{G \times G \times \cdots \times G}_{p \text{ factors}}$ $[\![:= (((G \times G) \times G) \times \cdots) \times G]\!]$,
again a group, and at the subset

$$\Omega := \{ (x_1, \ldots, x_p) \in G \times \ldots \times G \mid x_1 x_2 \cdots x_p = e \}.$$

There is a natural group action of $\mathbb{Z}_p$ on $G \times G \times \cdots \times G$, by 'cyclicly shifting':

$$\bar{1} \in \mathbb{Z}_p : (x_1, \ldots, x_p) \longmapsto (x_2, x_3, \ldots, x_p, x_1)$$
$$\vdots$$
$$\bar{m} \in \mathbb{Z}_p : (x_1, \ldots, x_p) \longmapsto (x_{m+1}, \ldots, x_p, x_1, \ldots, x_m)$$

This action induces an action of $\mathbb{Z}_p$ also on Ω.

$x_1 \ldots x_p = e \Rightarrow x_2 \cdots x_p = x_1^{-1}$; x_1^{-1} on left
$\Rightarrow x_2 \cdots x_p x_1 = e$; x_1 on right

hence:

$(x_1, \ldots, x_p) \in \Omega \Rightarrow (x_2, \ldots, x_p, x_1) \in \Omega$
$\Rightarrow (x_{m+1}, \ldots, x_p, x_1, \ldots, x_m) \in \Omega$

Now the size of any $\mathbb{Z}_p$-orbit in Ω divides $|\mathbb{Z}_p| = p$, so size is 1 or p.

Clearly we know at least one orbit of size 1,

$$(e, \dots, e) \in \Omega \subset G \times \dots \times G$$

But $|\Omega| = |G|^{p-1}$, since we can independently choose $x_1, \dots, x_{p-1}$, then $x_p := (x_1 \dots x_{p-1})^{-1}$ complements this to an element in Ω.

In particular $p \mid |\Omega| = |G|^{p-1} = (p \cdot d)^{p-1}$, hence there must be <u>another</u> orbit (in fact at least $p-1$) of size 1, since

$$\Omega = \dot{\bigcup} \{\text{orbits of size } 1\} \ \dot{\cup} \ \dot{\bigcup} \{\text{orbits of size } p\}$$

$$\Rightarrow |\Omega| = \underbrace{\sum_{\text{orbits of size } 1} 1}_{\text{need another to make this divisible by } p} + \sum_{\text{orbits of size } p} p \equiv 0 \ (p)$$

Such an orbit necessarily has the form $\{(g, g, \dots, g)\} \subset \Omega$ with $g \neq e$.

This g does it, since $(g, g, \dots, g) \in \Omega$, so get $g \cdots g = g^p = e$

Theorem: Any group G of order $2p$, p prime, is either cyclic or dihedral.

Proof: $p = 2$: We know that only $\mathbb{Z}_4$ and $V_4 \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \cong D_2$ exist as groups of order 4.

$p \geq 3$: Use Cauchy's Theorem to find elements a and b of order 2 and p respectively.

With $B := \langle b \rangle$, then

$$G = \underbrace{\langle b \rangle}_{\text{subgroup } B} \ \dot{\cup} \ \underbrace{a \langle b \rangle}_{\text{coset wrt subgroup } B}$$

[Proof: a cannot be in $\langle b \rangle$, a has even order, any element in $\langle b \rangle$ has <u>odd</u> order.]

In order to relate to dihedral relation, try to find ba in one of these cosets.

It cannot lie in $\langle b \rangle$ [Otherwise $ba = b^k$, for some k, hence $a = b^{k-1}$, contradiction]

Hence must be of the form ab^k, for some $1 \le k \le p-1$.

$$ba = ab^k$$
$$\Rightarrow \quad aba = b^k \quad ; \text{ multiply by } a \text{ on left}$$
$$\Rightarrow \quad b = ab^k a \quad ; \text{ same on right}$$

$$\begin{aligned} b &= ab^k a \\ &= \underbrace{(aba)(aba)\cdots(aba)}_{k \text{ factors}} \\ &= (aba)^k \\ &= (b^k)^k \\ &= b^{k^2} \end{aligned}$$

So $k^2 - 1 = 0 \ (p)$
$\Rightarrow k = 1$ or $k = p-1 \equiv -1 \ (p)$

First case $\Rightarrow$ cyclic group
Second case $\Rightarrow$ dihedral relations, dihedral group.

Conjugacy Classes of S_n

Definition: Let $x \in S_n$ be a permutation given in disjoint cycle form.

$$x = (a_1^{(1)} a_2^{(1)} \cdots a_{k_1}^{(1)})(a_1^{(2)} \cdots a_{k_2}^{(2)}) \cdots (a_1^{(r)} \cdots a_{k_r}^{(r)})$$

with $1 < k_1 \le k_2 \le \cdots \le k_r$, and $n \ge k_1 + k_2 + \cdots + k_r$.

Then we say that x has <u>cycle shape</u> (or <u>cycle type</u>) $[k_1, k_2, \ldots, k_r]$.

For $x = (1)$, we put $[1]$

Example: $(1\,5\,7)(2\,3)(4\,6\,10) = (2\,3)(1\,5\,7)(4\,6\,10) \in S_{10}$, has cycle shape $[2,3,3]$.

Example: $\underbrace{(1\,5\,7)(2\,3)(4\,5\,10)}$ is not in disjoint cycle form

It is $(2\,3)(1\,5\,10\,4\,7)$ so has cycle shape $[2,5]$.

Lemma: Let $x = (i_1\ i_2\ \cdots\ i_k)$ be a k-cycle in S_n, then for any $g \in S_n$ we can "read" off" the conjugate element of x by g as follows:

$$g(x) := gxg^{-1}$$
$$= (\underbrace{g(i_1)}_{\in\{1,\dots,n\}}\ g(i_2)\ \cdots\ g(i_k))$$

Here g is viewed as a permutation of $\{1,\dots,n\}$, in 2-row notation

$$g = \begin{pmatrix} 1 & 2 & \cdots & n \\ g(1) & g(2) & \cdots & g(n) \end{pmatrix}$$

Proof: Put $T = \{i_1,\dots,i_k\}$ the indices in x.

Take any $r \in \{1,\dots,k\}$, then

$$gxg^{-1}(g(i_r)) = gx(g^{-1}(g(i_r)) \quad ; g^{-1}g = e$$
$$= gx\underbrace{(i_r)}_{i_{r+1}}$$
$$= g(i_{r+1})$$

For any other $i \in \{1,\dots,n\} - T$, get

$$gxg^{-1}(g(i)) = gx(i) \quad ; \quad x(i) = i$$
$$= g(i)$$

Hence as a permutation, gxg^{-1} can be written as

$$(g(i_1)\ g(i_2)\ \cdots\ g(i_k))$$

Example: $x = (1345)$, $g = (12)(345)$

$$gxg^{-1} = \underbrace{(12)(345)}_{g}\ (1345)\ \underbrace{(543)(21)}_{g^{-1}}$$

$$= (2453)$$

and

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix}$$

$$(g(1)\ g(3)\ g(4)\ g(5)) = (2\ 4\ 5\ 3) \quad \checkmark$$

ANT : 6

Theorem: For $x \in S_n$, the conjugacy class $ccl_{S_n}(x)$ consists of all the elements in S_n of the same cycle shape as x.

Proof: Lemma shows this for x a k-cycle, $k \le n$.

More generally write

$$x = (a_1^{(1)} \cdots a_{k_1}^{(1)}) \cdots (a_1^{(r)} \cdots a_{k_r}^{(r)})$$

as a product of disjoint cycles. Then

$$\begin{aligned} gxg^{-1} &= g(a_1^{(1)} \cdots a_{k_1}^{(1)}) \cdots (a_1^{(r)} \cdots a_{k_r}^{(r)})g^{-1} \\ &= g(a_1^{(1)} \cdots a_{k_1}^{(1)})g^{-1}g \cdots g^{-1}g(a_1^{(r)} \cdots a_{k_r}^{(r)})g^{-1} \\ &= (g(a_1^{(1)}) \cdots g(a_{k_1}^{(1)})) \cdots (g(a_1^{(r)}) \cdots g(a_{k_r}^{(r)})) \end{aligned}$$

is of the same cycle shape, all $g(a_i^{(j)})$ are mutually different!

Conversely let x be as above, and

$$y = (b_1^{(1)} \cdots b_{k_1}^{(1)}) \cdots (b_1^{(r)} \cdots b_{k_r}^{(r)})$$

be of the same cycle shape. Then form a bijection $\{1, \ldots, n\} \xrightarrow{g} \{1, \ldots, n\}$ by putting

$$g(a_i^{(j)}) = b_i^{(j)}$$

and extending to a bijection in any way, so $gxg^{-1} = y$.

Example: In S_4, cycle shapes, and representative of the conjugacy class:

Cycle Shape :	[1]	[2]	[3]	[4]	[2,2]
Representative :	(1)	(12)	(123)	(1234)	(12)(34)

How many elements are there of a given cycle shape in S_n?

1) Suppose $x = (i_1 \ldots i_k)$ is a single k-cycle. Then

For i_1 have n choices, then
for i_2 have $n-1$ choices, then
for i_3 have $n-2$ choices, then
$\vdots$

for i_k have $n-(k-1)$ choices.

We have overcounted as each k cycle has k ways in which we can write it.

So

$$\gamma(n;k) := \frac{n(n-1)\cdots(n-k+1)}{k}$$

is the number of elements in the conjugacy class $ccl_{S_n}(x)$.

2) Suppose x is of cycle shape $[k_1, \ldots, k_r]$ with <u>strict</u> inequalities $1 < k_1 < k_2 < \cdots < k_r$, a product of r disjoint cycles of different lengths.

Then

$$\gamma(n; k_1, \ldots, k_r) := \gamma(n; k_1)\gamma(n-k_1, k_2) \cdots \gamma(n-k_1-k_2-\cdots-k_{r-1}, k_r)$$

is the number of elements in $ccl_{S_n}(x)$.

3) Suppose x is of arbitrary cycle shape $[\underbrace{k_1}_{s_1 \text{ times}}, \ldots, \underbrace{k_r}_{s_r \text{ times}}]$, $1 < k_1 < k_2 < \cdots < k_r$, then

$$\gamma(n; \underbrace{k_1, \ldots, k_1}_{s_1}, \underbrace{k_2, \ldots, k_2}_{s_2}, \ldots, \underbrace{k_r, \ldots, k_r}_{s_r})$$

overcounts by $s_1! \cdot s_2! \cdot \cdots \cdot s_r!$ (we can permute the cycles of length k_1, and can permute the cycles of length k_2 ...).

So

$$\frac{\gamma(n; k_1, \ldots, k_1, \ldots, k_r, \ldots, k_r)}{s_1! \cdots s_r!}$$

is the number of elements in $ccl_{S_n}(x)$.

Examples: 1) S_4 cycle shapes:

Cycle Shapes	$[1]$	$[2]$	$[3]$	$[4]$	$[2,2]$
Expression for number of elements	1	$\frac{4\cdot 3}{2}$	$\frac{4\cdot 3\cdot 2}{3}$	$\frac{4\cdot 3\cdot 2\cdot 1}{4}$	$\frac{\frac{4\cdot 3}{2}\cdot\frac{2\cdot 1}{2}}{2}$
Number of elements	1	6	8	6	3

2) S_7 : number of elements of cycle shape $[2,2,2]$

$$\frac{\frac{7\cdot 6}{2}\cdot\frac{5\cdot 4}{2}\cdot\frac{3\cdot 2}{2}}{3!} = 105$$

Conjugacy Classes in A_n.

Observe, since $A_n \subseteq S_n$, that

$$\begin{aligned} ccl_{A_n}(x) &= \{gxg^{-1} \mid g \in A_n\} \\ &= \{gxg^{-1} \mid g \in S_n,\ g \text{ even}\} \\ &\subseteq \{gxg^{-1} \mid g \in S_n\} \\ &= ccl_{S_n}(x). \end{aligned}$$

So $ccl_{A_n}(x) \subseteq ccl_{S_n}(x)$.

Sometimes these agree, sometimes they don't.

Proposition: Let $n \geq 2$, and $x \in A_n$, then.

i) If x commutes with <u>some</u> odd permutation in S_n, then $ccl_{A_n}(x) = ccl_{S_n}(x)$.

ii) Otherwise $ccl_{S_n}(x)$ splits into two conjugacy classes,

$$ccl_{A_n}(x) \quad \text{and} \quad ccl_{A_n}((12)x(12)^{-1})$$

of the same size.

Proof: i) Let $x \in A_n$, suppose $g \in S_n$, g odd, commutes with x.

Now let $y \in ccl_{S_n}(x)$, want to show $y \in ccl_{A_n}(x)$ have that $y = hxh^{-1}$ for some $h \in S_n$.

Case 1: h even, then we are done.

Case 2: h odd, then

$$\begin{aligned} (hg)x(hg)^{-1} &= hgxg^{-1}h^{-1} \\ &= hx\underbrace{gg^{-1}}_{e}h^{-1} \\ &= hxh^{-1} \\ &= y \end{aligned}$$

But hg is <u>even</u> (both h and g are odd), and so $y \in ccl_{A_n}(x)$.

ii) Now suppose x does not commute with any odd permutation in S_n.

Then the stabilizers of $x \in S_n$ and A_n agree:

$$
\begin{aligned}
(S_n)_x &= \{ g \in S_n \mid \underbrace{g(x)}_{\text{action by conjugation}} = x \} \\
&= \{ g \in S_n \mid gxg^{-1} = x \} \\
&= \{ g \in S_n \mid gxg^{-1} = x,\ g \text{ odd} \} \\
&\quad \cup \{ g \in S_n \mid gxg^{-1} = x,\ g \text{ even} \}
\end{aligned}
$$

But $\{ g \in S_n \mid gxg^{-1} = x,\ g \text{ odd} \} = \{ g \in S_n \mid gx = xg,\ g \text{ odd} \}$
$= \emptyset$ by assumption, so

$$
\begin{aligned}
&= \{ g \in S_n \mid gxg^{-1} = x,\ g \text{ even} \} \\
&= \{ g \in A_n \mid gxg^{-1} = x \} \\
&= (A_n)_x .
\end{aligned}
$$

Corollary to Orbit-Stabilizer Theorem gives

$$
\begin{aligned}
|S_n| &= |ccl_{S_n}(x)| \cdot |(S_n)_x| , \text{ and} \\
|A_n| &= |ccl_{A_n}(x)| \cdot |(A_n)_x|
\end{aligned}
$$

Since $|S_n| = 2|A_n|$, we get:

$$|ccl_{S_n}(x)| = 2\,|ccl_{A_n}(x)|$$

Finally note that: $ccl_{A_n}((12)x(12)^{-1}) = \{ hxh^{-1} \mid h \in S_n, h \text{ odd} \}$
so:

$$ccl_{S_n}(x) = ccl_{A_n}(x) \cup ccl_{A_n}((12)x(12)^{-1})$$

Example: In S_5, the conjugacy class of the cycle (123) stays the same in A_5, e.g. take (45)

For (12345) the conjugacy class in S_5 splits into two classes in A_5, it only commutes with its powers — even.

Example: For $n = 3$, in S_3

S_3-Cycle Shapes	$[1]$	$[2]$	$[3]$
Representative	(1)	(12)	(123)

A_3 conjugacy classes.

[1], the identity obviously stays.
[2], odd so doesn't appear

Question: Does (123) commute with some odd permutation, i.e. with (12), (23) or (13)?

No! So $ccl_{S_3}((123))$ splits into two conjugacy classes of the same size, i.e. size 1.

So A_3 conjugacy classes: $\{(1)\}$, $\{(123)\}$, $\{(132)\}$.

Example: For $n=4$, in S_4

S_4-Cycle Shapes	[1]	[2]	[3]	[4]	[2,2]
Representatives	(1)	(12)	(123)	(1234)	(12)(34)
Number of Elements	1 $=1$	$\frac{4\times 3}{2}$ $=6$	$\frac{4\times 3\times 2}{3}$ $=8$	$\frac{4\times 3\times 2\times 1}{4}$ $=6$	$\frac{4\times 3}{2}\times\frac{2\times 1}{2}$ $=3^2$
Pass to A_4 conjugacy class	$\{(1)\}$	X	Possibly splits	X	Stays, use size is odd so can't split, is (12)(3

Claim: [3] splits into two classes of size 4.

$g(123)g^{-1} = (123)$ implies $(g(1)\ g(2)\ g(3)) = (123)$
hence either:

i) $g(1) = 1$
$g(2) = 2$
$g(3) = 3$

$g = (1)(2)(3)$, even permutation

or ii) $g(1) = 2$
$g(2) = 3$
$g(3) = 1$

$g = (123)$, even.

or iii) $g(1) = 3$
$g(2) = 1$
$g(3) = 2$

$$g = (132), \quad \text{even.}$$

Hence the Proposition ii) implies the class splits.

A nice combinatorial application of group actions and conjugacy.

Question: How many orbits under a group action do we have?

Theorem: (Burnside's Counting Theorem)

Let G (finite) act on X (finite), then the number of orbits under G in X is given by

$$\frac{1}{|G|} \sum_{g \in G} |X^g|$$

where $X^g := \{x \in X \mid g(x) = x\}$, i.e. the elements in X fixed by g.

Proof: Use two ways to count a certain subset of $G \times X$.

$$\begin{aligned} Y &:= \{(g,x) \in G \times X \mid g(x) = x\} \\ &= \dot{\bigcup_{g \in G}} \{(g,x) \in \{g\} \times X \mid g(x) = x\} \\ &\overset{\text{bijection}}{\longleftrightarrow} \dot{\bigcup_{g \in G}} X^g, \quad \text{where } X^g = \{x \in X \mid g(x) = x\} \end{aligned}$$

But:

$$\begin{aligned} Y &= \{(g,x) \in G \times X \mid g(x) = x\} \\ &= \dot{\bigcup_{x \in X}} \{(g,x) \in G \times \{x\} \mid g(x) = x\} \\ &\overset{\text{bijection}}{\longleftrightarrow} \dot{\bigcup_{x \in X}} G_x, \quad \text{where } G_x = \{g \in G \mid g(x) = x\}. \end{aligned}$$

So:

$$\dot{\bigcup_{g \in G}} X^g = \dot{\bigcup_{x \in X}} G_x$$

Now take sizes on both sides, and get

$$\sum_{g \in G} |X^g| = \sum_{x \in X} \underbrace{|G_x|}_{|G|/|G(x)|} = |G| \sum_{x \in X} \frac{1}{|G(x)|}$$

Only need to show

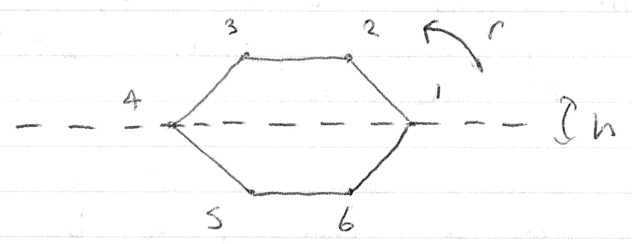
$$\sum_{x \in X} \frac{1}{|G(x)|}$$ coincides with the number of orbits.

But X decomposes into a disjoint union of the orbits.

$$X = G(x_1) \,\dot\cup\, G(x_2) \,\dot\cup \cdots \dot\cup\, G(x_r)$$

Simple observation that two elements in the same orbit have the same orbit length, to conclude.

Examples: 1) Let $G = D_6$ be the symmetry group acting on the set X of vertices of a regular hexagon.



$$D_6 = \langle r, h \mid r^6 = h^2 = e, \; rh = hr^{-1} \rangle$$

Number of orbits?

Burnside Counting:

g	X^g	$\lvert X^g \rvert$
e	X	$\lvert X \rvert = 6$
r	$\varnothing$	0
r^2	$\varnothing$	0
r^j, $1 \le j \le 5$	$\varnothing$	0
h	$\{1, 4\}$	2
hr	$\varnothing$	0
hr^2	$\{3, 6\}$	2
hr^3	$\varnothing$	0
hr^4	$\{2, 5\}$	2
hr^5	$\varnothing$	0

So:

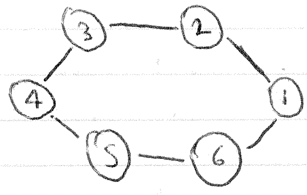
$$\frac{1}{|G|} \sum_{g \in G} |X^g| = \frac{1}{12}\left(6 + 2 + 2 + 2 + \underbrace{0 + \cdots + 0}_{8 \text{ times}}\right)$$

$$= 1$$

And indeed there is even a rotation that maps any given vertex to any other.

2) How many different bracelets with 6 beads can we get using red, green and blue beads?

Form a bracelet by putting one bead at each of the 6 vertices of a hexagon. The chain being the union of its sides.



Possible layouts : $L = \{ (c_1, \dots, c_6) \mid c_i \in \{\text{red}, \text{green}, \text{blue}\} \}$
How many different such layouts? 3^6 to start with.
But we overcounted!

Two bracelets agree if we can map them into each other by a symmetry of D_6.

Hence:

$$\begin{aligned} & |\{\text{different bracelets of the above kind}\}| \\ = & |\{\text{orbits of } L \text{ under the action of } D_6\}| \\ = & \frac{1}{|D_6|} \sum_{g \in G} |L^g| \end{aligned}$$

by Burnside Counting.

Remark: i) x, y in same orbit $\Rightarrow |G_x| = |G_y|$ (previously)
ii) g, g' in the same conjugacy class $\Rightarrow |X^g| = |X^{g'}|$

Example (2 continued)

Conjugacy classes of G	Representative	As Permutation	$(c_1, \dots, c_6) \in L^g$	$\lvert L^g \rvert$	$\lvert ccl\ g \rvert$
$\{e\}$	e	$(1)(2)(3)(4)(5)(6)$	all	3^6	1
$\{r, r^{-1}\}$	r	(123456)	$c_1 = c_2 = \dots = c_6$	3	2
$\{r^2, r^{-2}\}$	r^2	$(135)(246)$	$c_1 = c_3 = c_5$, $c_2 = c_4 = c_6$	3^2	2
$\{r^3\}$	r^3	$(14)(25)(36)$	$c_1 = c_4$, $c_2 = c_5$, $c_3 = c_6$	3^3	1
$\{h, hr^2, hr^4\}$	h	$(1)(26)(35)(4)$	$c_2 = c_6$, $c_3 = c_5$	3^4	3
$\{hr, hr^3, hr^5\}$	hr	$(16)(25)(34)$	$c_1 = c_6$, $c_2 = c_5$, $c_3 = c_4$	3^3	3

So by Burnside :

$$
\begin{aligned}
&\text{Number of Different Bracelets} \\
&= \text{Number of Orbits} \\
&= \frac{1}{12}\left(3^6 \cdot 1 + 3 \cdot 2 + 3^2 \cdot 2 + 3^3 \cdot 1 + 3^4 \cdot 3 + 3^3 \cdot 3\right) \\
&= \frac{1}{12}\left((3^6 + 3^5 + 3^4 + 3^3 + 3^2 + 3) + (3^2 + 3)\right) \\
&= \frac{1}{4}\left((3^5 + 3^4 + 3^3 + 3^2 + 3^1 + 3^0) + (3+1)\right) \\
&= \frac{1}{4}\left(\frac{3^6 - 1}{3 - 1} + 4\right) \\
&= \frac{1}{4}(364 + 4) \\
&= 92
\end{aligned}
$$

Exercise : How many ways are there to paint the faces of a dodecahedron with 3 colours, upto rotation?

(Result should be divisible by 1011)

Classification of Groups of Order p^2, p prime.

Definition : (Recall)

The centre of a group G, $Z(G)$, is defined as

$$
\begin{aligned}
Z(G) &= \{ g \in G \mid g \text{ commutes with } \underline{\text{any}}\ h \in G \} \\
&= \{ g \in G \mid hg = gh,\ \forall h \in G \}
\end{aligned}
$$

Remark : 1) Precisely the elements in $Z(G)$ have conjugacy class of size 1.

2) $Z(G) \subset G_h$, for any $h \in G$, action by conjugation

3) $Z(G) = G \iff G$ is abelian

4) $Z(G)$ is a group.

Proposition : Let p ~~be~~ a prime, and G a group, with $|G| = p^r$, for some $r \geq 1$, then $Z(G)$ is non-trivial.

Proof: (Argument similar to in Cauchy's Theorem)

$$G = \dot{\bigcup} \, ccl_G(x)$$, a disjoint union of its conjugacy classes.

$$\Rightarrow |G| = \sum |ccl_G(x)| \qquad (*)$$

The only possible orbit sizes are p^i, $0 \leq i \leq r$, they have to divide $|G|$, the group order.

Assume $Z(G) = \{e\}$, then by remark 1), all other conjugacy classes have size divisible by p.

But then $p \mid$ LHS of $(*)$, but RHS of $(*)$ is $1 \; (p)$.

Corollary: If $|G| = p^2$, for p prime, then G is abelian.

Proof: By the proposition above, we get $Z(G) \neq \{e\}$.

Since $Z(G)$ is a subgroup, its order has to divide p^2, hence $|Z(G)| = p$ or p^2.

Case 1: $|Z(G)| = p^2$, then $G = Z(G)$ hence G is abelian.

Case 2: $|Z(G)| = p$, assume $h \in G - Z(G)$.

Then in particular, $|ccl_G(h)| > 1$, moreover it has to divide $|G| = p^2$.

Furthermore, $p = |Z(G)| \leq |G_h|$, by remark 2)

Now Orbit-Stabilizer Theorem, for h:

$$\underbrace{|ccl_G(h)|}_{\geq p} \cdot \underbrace{|G_h|}_{\geq p} = \underbrace{|G|}_{= p^2}$$

Hence $|ccl_G(h)| = |G_h| = p$.

But then $Z(G) \subset G_h$ implies $Z(G) = G_h$, both of the same order.

Then $h \in G_h = Z(G)$

Conclusion: $|Z(G)| = p$ cannot hold.

Corollary: Let G be of order p^2, p prime, then

$$G \cong \mathbb{Z}_{p^2}, \quad \text{or} \quad G \cong \mathbb{Z}_p \times \mathbb{Z}_p$$

Proof: Case 1: $\exists\, g \in G$ of order p^2, then $G = \langle g \rangle$, is necessarily cyclic of order p^2.

Case 2: No element $g \in G$ of order p^2 exists. Then each element $g \in G$, $g \neq e$, has order p.

Hence take $g \in G - \{e\}$, and form $H = \langle g \rangle$, this is cyclic of order p.

In order to apply our criterion for a group being written as a product of two of its subgroups, try to establish a second subgroup K, with $HK = G$ and $H \cap K = \{e\}$.

ii) Take any $k \in G - H$, and put $K = \langle k \rangle$, then K is cyclic of order p, and $H \cap K = \{e\}$.

[[Suppose $k^r = g^s$, for some $r, s \in \mathbb{Z}$, with $\gcd(s,p) = 1$.

Then $(k^r)^t = (g^s)^t = g^1 = g$, for appropriate $t \in \mathbb{Z}$, using the Euclidean algorithm so $st + pn = 1$.

$\Rightarrow g \in \langle k \rangle$
$\Rightarrow g^r \in \langle k \rangle, \quad \forall r \in \mathbb{Z}$
$\Rightarrow H = K$

But $k \in G - H$, so $k \notin H$.]]

i) $HK = \{ g^i k^j \mid 0 \leq i, j < p \}$.

All these are different, so cardinality is p^2, hence $HK = G$.

iii) $hk = kh \quad \forall h \in H, k \in K$, clear due to previous corollary, that G is abelian.

Upshot: by our criterion, we conclude

$$G \cong H \times K \cong \mathbb{Z}_p \times \mathbb{Z}_p$$

Mention Sylow Theorem (cf QS1).

Theorem : (Sylow)

Let G be a group of order $p^r m$, p prime, where $\gcd(p,m)=1$. Then there is a subgroup of G of order p^r.

In fact we can find a subgroup of order p^s, $0 \leq s \leq r$.

[Compare with Cauchy's Theorem where $r=1$].

Normal Subgroups, Quotient Groups, and the First Isomorphism Theorem.

A subgroup $H < G$ partitions G into <u>left</u> cosets, but also into <u>right</u> cosets. These do not have to agree.

Example : $D_3 = \langle r, h \mid r^3 = h^2 = e,\ rh = hr^{-1} \rangle$

Take $H := \langle h \rangle = \{e, h\}$

Then the <u>left</u> cosets of H in D_3 are :

$$\begin{aligned} eH &= \{e, h\} \\ rH &= \{r, rh\} \\ r^2H &= \{r^2, r^2h\} \end{aligned}$$

But the <u>right</u> cosets of H in D_3 are :

$$\begin{aligned} He &= \{e, h\} \\ Hr &= \{r, hr\} \\ Hr^2 &= \{r^2, hr^2\} \end{aligned}$$

These two partitions are different, eg.

$$rH \cap Hr = \{r\}, \text{ as } rh \neq hr.$$

Definition : A subgroup N is called a <u>normal subgroup</u> in G if

$$gN = Ng \quad \forall g \in G$$

equivalently if $gNg^{-1} = N \quad \forall g \in G$, or
equivalently if : $\forall g \in G, \forall h \in N,\ ghg^{-1} = h'$, for some $h' \in N$

We write $N \trianglelefteq G$.

Examples : 0) Trivial normal subgroups of G are :

$\{e\}$, since $g\{e\} = \{g\} = \{e\}g, \ \forall g \in G$

G , since $gG = G = Gg, \ \forall g \in G$.

1) Suppose $H < G$ is a subgroup such that $|G|/|H| = 2$, H is of <u>index 2</u> in G, then H is a normal subgroup of G.

Proof : Left cosets are H, gH ; for any $g \notin H$.
Right cosets are H, Hg.

One of the cosets agrees, hence the second cosets must agree as well, G is partitioned, ie.

$$gH = G \setminus H = Hg$$

2) $A_n \triangleleft S_n$
$C_n = \langle r \rangle \triangleleft D_n = \langle r, h \mid r^n = h^2 = e, \ rh = hr^{-1}$

Proposition : If $N < G$, is a subgroup, then

$N \triangleleft G \iff N$ is the union of conjugacy classes in G

Proof : "$\Leftarrow$" : Suppose N is the union of conjugacy classes in G. Then with $h \in N$, we also need $ghg^{-1} \in N$ for any $g \in G$.

But ghg^{-1} is in the same conjugacy class as h, hence is indeed in N.

So N is normal using the third equivalence above.

"$\Rightarrow$" : Suppose $N \triangleleft G$; with $h \in N$, we have $ghg^{-1} \in N$ by the above criterion, $\forall g \in G$.

Hence $ccl_G(h) = \{ghg^{-1} \mid g \in G\}$, the conjugacy class of h in G, lies in N.

Hence N must be a union of conjugacy classes in G.

Corollary : $Z(G)$ is a normal subgroup of G

Proof: $Z(G)$ is the union of all 1 element conjugacy classes in G, and $Z(G)$ is a subgroup.

Examples: 1) Find all the normal subgroups of S_4:

— $\{e\}$, and S_4 itself are normal in S_4, the 'trivial normal subgroups' in S_4.

Use criterion above, the conjugacy classes in S_4 are:

Cycle Shape	[1]	[2]	[3]	[4]	[2,2]
Number of elements	1	6	8	6	3

Now try to find sums of these orders which add up to a divisor of $|S_4| = 24$, by Lagrange.

— $1+3$ is a possibility

— $6+6 \mid 24$, but the union of the corresponding conjugacy classes would not form a group, it doesn't contain the identity.

— $1+3+8$ is the only other possibility

First case: $ccl_{S_4}((1)) \cup ccl_{S_4}((12)(34))$, this is a group isomorphic to the <u>Klein-4-group</u>.

Second case: $ccl_{S_4}((1)) \cup ccl_{S_4}((12)(34)) \cup ccl_{S_4}((123))$, these are precisely the <u>even</u> permutations in S_4 which indeed form a subgroup, <u>A_4</u>.

2) Non-trivial normal subgroups of A_4:

Conjugacy classes in A_4 are the conjugacy classes of

Representative	(1)	(123)	(132)	(12)(34)
Size	1	4	4	3

Find sums of these which divide $|A_4| = 12$, where '1' is a summand.

Only possibility is: $1+3$, and indeed $ccl_{A_4}((1)) \cup ccl_{A_4}((12)(34))$ gives the <u>Klein-4-group</u>

Reminiscent of characterising <u>ideals</u> as distinguished <u>subrings</u>.

Normal subgroups are kernels of homomorphisms of <u>groups</u>. They guarantee a structure of a group on the set of cosets with respect to that subgroup.

Proposition: Let $N \lhd G$, then

i) $(gN) \cdot (hN) = (gh)N$

ii) With the product induced by i), the set

$$G/N = \{ gN \mid g \in G \}$$

of cosets, forms a group.

iii) The map:

$$\pi : G \longrightarrow G/N$$
$$g \longmapsto gN$$

gives a homomorphism of groups. It's kernel is given by N.

Proof: i)
$$\begin{aligned}(gN)(hN) &= g(Nh)N \\ &= g(hN)N \\ &= (gh)N\end{aligned}$$

ii) Identity element in $G/N = \{gN \mid g \in G\}$ is $eN = N$.

Inverse element of gN in G/N is given by $g^{-1}N$.

Associativity follows from in G

iii)
$$\begin{aligned}\pi(g_1 g_2) &= (g_1 g_2)N \\ &= (g_1 N)(g_2 N) \quad ; \text{by i)} \\ &= \pi(g_1)\pi(g_2)\end{aligned}$$

Hence π is indeed a homomorphism, and

$$\begin{aligned}\ker \pi &= \{ g \in G \mid gN = N \} \\ &= \{ g \in G \mid g \in N \} \\ &= N\end{aligned}$$

since $gN = N \Rightarrow ge = g \in N$, and $g \in N \Rightarrow gN = N$.

Definition: Let $N \lhd G$, then $G/N = \{ gN \mid g \in G \}$, with multiplication as in the proposition, is called the <u>quotient group</u> of G wrt N.

As for rings, a central statement for groups is:

Theorem: (First Isomorphism Theorem (for Groups)):

Let $\emptyset : G \to G'$ be a homomorphism of groups, then

i) $\ker \emptyset \lhd G$
ii) There exists an isomorphism

$$\bar{\emptyset} : G/\ker\emptyset \xrightarrow{\cong} \emptyset(G) < G'$$

In particular, if $\emptyset$ is surjective, then

$$G/\ker\emptyset \cong G'.$$

Proof: i) Put $N := \ker \emptyset$

Show that $gNg^{-1} = N$, $\forall g \in G$, whence $N \lhd G$

$$\begin{aligned}
x \in gNg^{-1} &\iff x = ghg^{-1} \text{ for some } h \in N \\
&\iff g^{-1}xg \in N \\
&\iff \emptyset(g^{-1}xg) = e_{G'} \\
&\overset{\emptyset \text{ homomorphism}}{\iff} \emptyset(g)^{-1}\emptyset(x)\emptyset(g) = e_{G'} \\
&\iff \emptyset(x) = \emptyset(g)\emptyset(g)^{-1} \\
&\iff \emptyset(x) = e_{G'} \\
&\iff x \in \ker\emptyset = N, \quad \forall g \in G
\end{aligned}$$

ii) We first check that $\emptyset$ respects cosets:

$$\begin{aligned}
\emptyset(gN) &= \{ \emptyset(gh) \mid h \in N \} \\
&= \{ \emptyset(g)\underbrace{\emptyset(h)}_{e_{G'}} \mid h \in N \} \\
&= \{ \emptyset(g) \}.
\end{aligned}$$

So define:

$$\begin{aligned}
\bar{\emptyset} : G/\ker\emptyset &\longrightarrow \emptyset(G) \\
gN &\longmapsto \emptyset(g)
\end{aligned}$$

[Take $\emptyset(gN) = \{\emptyset(g)\}$, then take the unique element in that set]

— $\bar{\phi}$ is a homomorphism of groups:

$$\begin{aligned}\bar{\phi}((gN)(hN)) &= \bar{\phi}(ghN)\\ &= \phi(gh)\\ &= \phi(g)\phi(h) \quad ; \phi \text{ homomorphism}\\ &= \bar{\phi}(gN)\bar{\phi}(hN)\end{aligned}$$

— $\bar{\phi}$ is surjective onto $\phi(G)$

[Clear!]

— $\bar{\phi}$ is injective:

$$\begin{aligned}\bar{\phi}(gN) = \bar{\phi}(hN) &\Rightarrow \phi(g) = \phi(h) \quad ; \text{by definition of } \bar{\phi}\\ &\Rightarrow \phi(gh^{-1}) = e_{G'}\\ &\Rightarrow gh^{-1} \in N\\ &\Rightarrow gN = hN.\end{aligned}$$

Examples: 1) Let

$$\phi : S_n \longrightarrow \{\pm 1\} \cong \mathbb{Z}/2\mathbb{Z}$$
$$\sigma \longmapsto \text{sign}(\sigma) = \begin{cases} 1 & \text{if } \sigma \text{ even} \\ -1 & \text{if } \sigma \text{ odd}\end{cases}$$

Then $\ker\phi = \{\text{even permutations in } S_n\} = A_n$ and by the First Isomorphism Theorem, since $\phi(S_n) = \{\pm 1\}$, we get

$$S_n/A_n \xrightarrow{\cong} \{\pm 1\}$$

2a) Let

$$\varphi : \mathbb{C}^* \longrightarrow \mathbb{R}_{>0}$$
$$z \longmapsto |z|$$

both with multiplication as the binary operation

— φ is a homomorphism of groups

$$\begin{aligned}\varphi(z_1 z_2) &= |z_1 z_2|\\ &= |z_1||z_2| \quad ; \text{Complex Analysis}\\ &= \varphi(z_1)\varphi(z_2)\end{aligned}$$

— φ is surjective.

Suppose $r \in \mathbb{R}_{>0}$, then also have $r \in \mathbb{C}^* \supset \mathbb{R}_{>0}$, and

$$\varphi(r) = |r| = r.$$

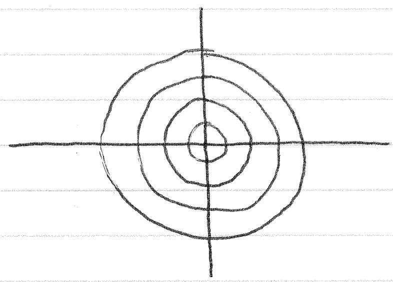
— $$\ker \varphi = \{ z \in \mathbb{C}^* \mid |z| = \underbrace{1}_{\text{identity in } \mathbb{R}_{>0} \text{ under multiplicat}} \}$$

The unit sphere, S^1

F.I.T. then implies

$$\mathbb{C}^*/S^1 \xrightarrow{\cong} \mathbb{R}_{>0}$$

where the cosets on the left are the circles with centre $0 \ (\in \mathbb{C})$.



b) Have

$$\begin{aligned} \psi : \mathbb{C}^* &\longrightarrow S^1 \\ z &\longmapsto \frac{z}{|z|} \end{aligned}$$

— ψ a homomorphism (clear)

— ψ surjective (clear)

— $\ker \psi = \mathbb{R}_{>0}$

So FIT implies

$$\mathbb{C}^*/\mathbb{R}_{>0} \xrightarrow{\cong} S^1$$

3) Want a surjective homomorphism $S_4 \longrightarrow S_3$

Let S_4 act on the set

$$X = \{ \underbrace{(14)(23)}_{x_1}, \underbrace{(13)(24)}_{x_2}, \underbrace{(12)(34)}_{x_3} \}$$

by conjugation. (X is a conjugacy class in S_4!)

Then we get a homomorphism

$$\varphi : S_4 \longrightarrow S_X \cong S_{|X|} = S_3$$

where S_X is the bijections of X.

Eg.

$$(12) \longmapsto \begin{pmatrix} x_1 \longmapsto (24)(13) = x_2 \\ x_2 \longmapsto (23)(14) = x_1 \\ x_3 \longmapsto (21)(34) = x_3 \end{pmatrix}$$

or as a bijection is, $(x_1\ x_2) \in S_X$

$$(13) \longmapsto (x_1\ x_3) \in S_X$$

$(14)(23) \longmapsto e \in S_X$, the identity in S_X

Now φ is surjective, $(x_1\ x_2)$ and $(x_1\ x_3)$ generate S_X, so we get a surjective homomorphism $S_4 \to S_3$.

$\operatorname{Ker}\varphi$ contains $(14)(23)$, hence, as it is normal, it also contains the whole $\operatorname{ccl}_{S_4}((14)(23))$, together with e_{S_4}, the identity.

Hence $|\operatorname{Ker}\varphi| \geq 4$.

In fact, this is an equality

$$|S_4| / |\operatorname{Ker}\varphi| = |S_4 / \operatorname{Ker}\varphi|$$

$$= |S_X| \quad ; \text{FIT implies } S_4/\operatorname{Ker}\varphi \cong S_X$$

$$= |S_3|$$

$$= 6$$

Hence $|\operatorname{Ker}\varphi| = 4$.

Conclusion:

$$\ker\varphi = \{e, (12)(34), (13)(24), (14)(23)\}$$
$$\cong V_4$$

And

$$S_4/V_4 \xrightarrow{\cong} S_3$$

4 Finitely Generated Abelian Groups.

Definition: $G = \langle g_1, \dots, g_r \rangle$ is <u>finitely generated</u> if there exists $r \geq 0$, and there exists $g_1, \dots, g_r \in G$ such that any $g \in G$ can be represented in terms of the g_i.

Examples: 1) $\mathbb{Z} = \langle 1 \rangle$
$= \langle 2, 3 \rangle$
$= \langle 257, 36, \dots \rangle$

2) $\mathbb{Z}_n = \langle \bar{1} \rangle$

3) $\mathbb{Z}_n^*$ is.

Eg. $\mathbb{Z}_{15}^* \cong \mathbb{Z}_2 \times \mathbb{Z}_4 = \langle (\bar{1}, \bar{0}), (\bar{0}, \bar{1}) \rangle$

4) $\mathbb{Z}_5 \times \mathbb{Z} \times \mathbb{Z} = \langle (\bar{1}, 0, 0), (\bar{0}, 1, 0), (\bar{0}, 0, 1) \rangle$

Non-example: $\mathbb{Q}$ is not finitely generated.

[Suppose $\mathbb{Q} = \langle \frac{p_1}{q_1}, \dots, \frac{p_r}{q_r} \rangle$, $p_i, q_i \in \mathbb{Z}$

Then any element by the $\frac{p_i}{q_i}$ is a $\mathbb{Z}$-linear combination of these, hence has a denominator dividing $\operatorname{lcm}(q_1, \dots, q_r)$, so can never generate all of $\mathbb{Q}$]

From now on write groups additively, so

$$G = \langle g_1, \dots, g_r \rangle = \{ a_1 g_1 + \dots + a_r g_r \mid a_i \in \mathbb{Z}, 1 \leq i \leq r \}$$

First 'insight'. Can write any such G as a homomorphic image of some $\mathbb{Z}^m$, where we can choose m as the number of some set of generators, via

$$\varphi : \mathbb{Z}^r \longrightarrow G = \langle g_1, \dots, g_r \rangle$$
$$(a_1, \dots, a_r) \longmapsto a_1 g_1 + \dots + a_r g_r$$

Theorem: Any finitely generated abelian group G can be written as

$$G \cong \mathbb{Z}^n / K$$

for some $n \geq 0$, $K < \mathbb{Z}^n$.

Proof: Use F.I.T.

Definition: In the situation of the theorem, we call $\underline{a} \in K$ a relation and K the relation subgroup of G.

Moreover if there are no non-trivial relations in K, i.e. if $a_1 g_1 + \dots + a_n g_n = 0$ implies $a_1 = \dots = a_n = 0$, then G is called a free abelian group of rank n.

[And $G \cong \mathbb{Z}^n / \{0\}$, which is clearly isomorphic to $\mathbb{Z}^n$]

Proposition: Every subgroup H of $\mathbb{Z}^n$ is itself a free abelian group generated by $r \leq n$ elements (i.e. of rank $\leq n$)

Proof: (Idea)

For $\mathbb{Z}$ it is well known from previous, this is $n=1$.

For $n \geq 2$ use induction on n; crucial idea is to look at subgroups $H_0 \leq H$ with

$$H_0 = \{(a_1, \dots, a_n) \in H \mid a_n = 0\}$$

Either $H_0 = H$ or $H \cong H_0 \times \langle \underline{b} \rangle$, with $\underline{b} = (b_1, \dots, b_n)$, $b_n \neq 0$.

Remark: By the proposition, an $H \leq \mathbb{Z}^n$ is finitely generated, i.e. is of the form

$$H = \langle \underline{a_1}, \dots, \underline{a_m} \rangle$$

for some $a_i \in \mathbb{Z}^n$, $m \leq n$.

Form a matrix:

$$A = A(H) = \begin{pmatrix} \underline{a_1} \\ \underline{a_2} \\ \vdots \\ \underline{a_m} \end{pmatrix}$$

Definition: If $G \cong \mathbb{Z}^n / H$, then $A = A(H)$ is called a <u>relation matrix for G</u>.

Proposition: i) Any matrix $A \in M(m, n, \mathbb{Z})$ can be transformed into a matrix $\tilde{A} \in M(m, n, \mathbb{Z})$ in "diagonal form" using only elementary row and column operations.

Here elementary column operations are of the following kind

1) Multiply a column by -1
2) Swap two columns
3) Add an <u>integer</u> multiple of some column to another one.

And similarly with elementary row operations.

Here $\tilde{A}$ is in diagonal form if its entries $\tilde{a}_{jk} = 0$ whenever $j \neq k$.

ii) Moreover, we can achieve that the entries $\tilde{a}_{ii}$ in $\tilde{A}$ successively divide each other:

$$\tilde{a}_{11} \mid \tilde{a}_{22} \mid \cdots \mid \tilde{a}_{mm}$$

Example:

$$A = \begin{pmatrix} 8 & -4 & 22 \\ 4 & -8 & 8 \end{pmatrix} \overset{r_1 \leftrightarrow r_2}{\sim} \begin{pmatrix} 4 & -8 & 8 \\ 8 & -4 & 22 \end{pmatrix}$$

$$\overset{r_2 \to r_2 - 2r_1}{\sim} \begin{pmatrix} 4 & -8 & 8 \\ 0 & 12 & 6 \end{pmatrix}$$

$$\overset{c_2 \mapsto c_2 + c_1}{\sim} \begin{pmatrix} 4 & 0 & 8 \\ 0 & 12 & 6 \end{pmatrix}$$

$$\overset{c_3 \mapsto c_3 - 2c_1}{\sim} \begin{pmatrix} 4 & 0 & 0 \\ 0 & 12 & 6 \end{pmatrix}$$

$$\overset{c_2 \leftrightarrow c_3}{\sim} \begin{pmatrix} 4 & 0 & 0 \\ 0 & 6 & 12 \end{pmatrix}$$

$$\overset{c_3 \mapsto c_3 - 2c_2}{\sim} \begin{pmatrix} 4 & 0 & 0 \\ 0 & 6 & 0 \end{pmatrix}$$

$$= \tilde{A}$$

This is now in diagonal form. Note this does not satisfy the requirements in ii) since $4 \nmid 6$. Manipulate further.

$$\begin{pmatrix} 4 & 0 & 0 \\ 0 & 6 & 0 \end{pmatrix} \overset{c_2 \mapsto c_2 + c_1}{\sim} \begin{pmatrix} 4 & 4 & 0 \\ 0 & 6 & 0 \end{pmatrix}$$

$$\overset{r_1 \mapsto r_1 - r_2}{\sim} \begin{pmatrix} 4 & -2 & 0 \\ 0 & 6 & 0 \end{pmatrix}$$

$$\overset{c_1 \leftrightarrow c_2}{\sim} \begin{pmatrix} -2 & 4 & 0 \\ 6 & 0 & 0 \end{pmatrix}$$

$$\overset{r_2 \mapsto r_2 + 3r_1}{\sim} \begin{pmatrix} -2 & 4 & 0 \\ 0 & 12 & 0 \end{pmatrix}$$

$$\overset{c_2 \mapsto c_2 + 2c_1}{\sim} \begin{pmatrix} -2 & 0 & 0 \\ 0 & 12 & 0 \end{pmatrix}$$

$$\overset{c_1 \mapsto -1 \times c_1}{\sim} \begin{pmatrix} 2 & 0 & 0 \\ 0 & 12 & 0 \end{pmatrix}$$

which does satisfy the requirements in ii) since $2 \mid 12$.

This is used in the following typical setting.

Example: Let G be the group generated by $n = 3$ generators x, y, z, subject to the following relations

$$\begin{aligned} 8x - 4y + 22z &= 0 \\ 4x - 8y + 8z &= 0 \end{aligned}$$

Then we can write $G = \mathbb{Z}^3 / H$, where

$$H = \langle (8, -4, 22), (4, -8, 8) \rangle$$

With the relation matrix as above:

$$A = \begin{pmatrix} 8 & -4 & 22 \\ 4 & -8 & 8 \end{pmatrix}$$

Found we can 'diagonalise' A to $\tilde{A} = \begin{pmatrix} 4 & 0 & 0 \\ 0 & 6 & 0 \end{pmatrix}$, from this we can read off, after completing $\tilde{A}$ to a square matrix (by possibly adding zeros):

$$\longrightarrow \begin{pmatrix} 4 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

That

$$G \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \underbrace{\mathbb{Z}/0\mathbb{Z}}_{\cong \mathbb{Z}}$$

ANT: 9.

This is an example of the following:

Theorem: (Fundamental Theorem of Finitely Generated Abelian Groups)

Let G be a finitely generated abelian group. Then G is isomorphic to a group of the following form:

$$\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_k} \times \mathbb{Z}^r$$

with $r \geq 0$, $k \geq 0$, $d_j \geq 1$ for $1 \leq j \leq k$.

Moreover if we require

$$d_1 \mid d_2 \mid d_3 \mid \cdots \mid d_k, \quad \text{and} \quad d_1 > 1 \qquad (*)$$

then this form is in fact unique.

Definition: The number r as in the theorem is called the <u>rank</u> of G, and the $d_1, \ldots, d_k$ are called the <u>torsion invariants</u> of G if they satisfy $(*)$

Remark: i) G (as in the theorem) is finite $\Leftrightarrow$ $r = 0$

ii) $r = k = 0$ means G is the trivial group.

iii) Whenever we have an entry in the relation matrix $\tilde{A}$ (diagonalised), which is ± 1, then we can ignore the corresponding factor in the direct product:

$$\mathbb{Z}/_{1\mathbb{Z}} \cong \{e\}.$$

iv) The torsion invariants have to be given <u>with repetitions</u>, i.e.

$$\mathbb{Z}_7 \times \mathbb{Z}_7 \times \mathbb{Z}_{105}$$

has torsion invariants '7, 7, 105', <u>not</u> '7, 105'.

Applications:

— Classify all ~~finite~~ abelian groups of a given order, up to isomorphism.

Examples: i) Classify all abelian groups of order 8.

By the theorem any such is isomorphic to a product of the form

$$\mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_k}$$

with $d_1 | \cdots | d_k$, and $d_1 \cdots d_k = 8 = 2^3$, hence $k \leq 3$.

Rephrase condition $d_1 | d_2$ as:

"exponent of 2 in d_1 $\leq$ exponent of 2 in d_2"

And similarly for $d_i | d_{i+1}$

Hence looking for $d_1 | \cdots | d_k$ such that $d_1 \cdots d_k = 8$ is equivalent to looking for <u>non-decreasing partitions</u> of 3 (the exponent of 2)

I.e. $1, 1, 1$
or $1, 2$
or 3

So

	$n_1 = n_2 = n_3 = 1$	$n_1 = 1, n_2 = 2$	$n_1 = 3$
As a partition	$1, 1, 1$	$1, 2$	3
Corresponding d_j	$2^1, 2^1, 2^1$	$2^1, 2^2$	2^3
Corresponding group	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	$\mathbb{Z}_2 \times \mathbb{Z}_4$	$\mathbb{Z}_8$

This is a complete list, up to isomorphism!

2) Classify all abelian groups of order $200 = 2^3 \times 5^2$.

The only primes involved are 2 and 5. By the theorem we need to find all possibilities

$d_1, \ldots, d_k$ such that $d_1 \cdots d_k = 200$, and $d_1 | \cdots | d_k$, and $d_1 > 1$.

Condition $d_1 | d_2$ translates as:

"exponent of 2 in d_1 $\leq$ exponent of 2 in d_2", and
"exponent of 5 in d_1 $\leq$ exponent of 5 in d_2".

Similarly for any $d_i | d_{i+1}$.

We need to find all

— non-decreasing partitions of 3 (exponent of 2)
[seen: 1,1,1 ; 1,2 ; 3]

— non-decreasing partitions of 2 (exponent of 5)
[ie: 1,1 and 2]

These partitions are independent, hence overall we get $3 \times 2 = 6$ possibilities for a pair (non-decreasing partition of 3, non-decreasing partition of 2).
So:

	Partitions					
Exponent of 2	1,1,1	1,1,1	1,2	1,2	3	3
Exponent of 5	1,1	2	1,1	2	1,1	2
Corresponding d_j	2, 10, 10 (↑$2^1 5^0$ ↑$2^1 5^1$ ↑$2^1 5^1$)	2, 2, 50	10, 20	2, 100	5, 40	200
Corresponding group	$\mathbb{Z}_2 \times \mathbb{Z}_{10} \times \mathbb{Z}_{10}$	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{50}$	$\mathbb{Z}_{10} \times \mathbb{Z}_{20}$	$\mathbb{Z}_2 \times \mathbb{Z}_{100}$	$\mathbb{Z}_5 \times \mathbb{Z}_{40}$	$\mathbb{Z}_{200}$

This is a complete list of all abelian groups of order 200.

— Determine the number of elements of a given order in some abelian group

Definition: Let G be a finite group, (using multiplicative notation):

$$A_m(G) := |\{ g \in G \mid g^m = e \}| = |\{ g \in G \mid \text{order of } g \text{ divides } m \}|$$

$$O_m(G) := |\{ g \in G \mid g \text{ has order } \underline{\text{precisely}}\ m \}| = |\{ g \in G \mid g^m = e,\ g^k \neq e \text{ for } 1 \leq k < m \}|$$

Exercise: "A_m is multiplicative", ie.

$$A_m(G \times H) = A_m(G) A_m(H)$$

for G, H abelian.

Warning: The corresponding statement for O_m is <u>not</u> true (in general)

Proposition: $A_m(\mathbb{Z}_n) = \gcd(m, n)$.

Relating A_m and O_m:

For a prime p, and $r \geq 0$, we have, for G abelion

$$\{ g \in G \mid g^{p^r} = e \} = \{ g \in G \mid \text{order of } g \text{ is } p^r \}$$
$$\cup \{ g \in G \mid \text{order of } g \text{ is } p^{r-1} \}$$
$$\vdots$$
$$\cup \{ g \in G \mid \text{order of } g \text{ is } p^0 = 1 \}.$$

a disjoint union, so:

$$A_{p^r}(G) = O_{p^r}(G) + O_{p^{r-1}}(G) + \cdots + O_{p^0}(G)$$

And so $O_{p^r}(G) = A_{p^r}(G) - A_{p^{r-1}}(G)$.

Example: Find the number of elements of order 8 in

$$\mathbb{Z}_{12} \times \mathbb{Z}_{40} \times \mathbb{Z}_{102}$$

Proposition, and multiplicativity give for

$$\begin{aligned} A_8(\mathbb{Z}_{12} \times \mathbb{Z}_{40} \times \mathbb{Z}_{102}) &= A_8(\mathbb{Z}_{12})\, A_8(\mathbb{Z}_{40})\, A_8(\mathbb{Z}_{102}) \\ &= \gcd(8,12)\, \gcd(8,40)\, \gcd(8,102) \\ &= 4 \times 8 \times 2 \\ &= 64 \end{aligned}$$

Then $O_{2^3}(\mathbb{Z}_{12} \times \mathbb{Z}_{40} \times \mathbb{Z}_{102}) = A_{2^3}(\mathbb{Z}_{12} \times \mathbb{Z}_{40} \times \mathbb{Z}_{102}) - A_{2^2}(\mathbb{Z}_{12} \times \mathbb{Z}_{40} \times \mathbb{Z}_{102})$
and:

$$\begin{aligned} A_{2^2}(\mathbb{Z}_{12} \times \mathbb{Z}_{40} \times \mathbb{Z}_{102}) &= 4 \times 4 \times 2 \\ &= 32 \end{aligned}$$

So:

$$\begin{aligned} O_8(\mathbb{Z}_{12} \times \mathbb{Z}_{40} \times \mathbb{Z}_{102}) &= O_{2^3}(\mathbb{Z}_{12} \times \mathbb{Z}_{40} \times \mathbb{Z}_{102}) \\ &= 64 - 32 \\ &= 32 \end{aligned}$$

So there are 32 elements of order exactly 8.

Remark: For non-prime powers m, one can use a kind of inclusion-exclusion principle, eg.

$$O_6(G) = A_6(G) - A_3(G) - A_2(G) + A_1(G).$$