MA 419: Basic Algebra

Aryaman Maithani

Autumn 2019

Contents

1 Groups

Let G be a set with an associative law of composition $\cdot$. $(G, \cdot)$ is called a group if it has an identity element and every element of G is invertible.
That is,

1. $\exists e \in G : \forall g \in G : e \cdot g = g = g \cdot e.$
2. $\forall g \in G : \exists g' \in G : g \cdot g' = e = g' \cdot g.$

We often shorten $a \cdot b$ and write ab instead.
e is often denoted by 1.

Example:
$S_3 = \langle x, y | x^3 = 1, y^2 = 1, yx = x^2 y \rangle$

2 Subgroup

Let $(G, \cdot)$ be a group and $H \subset G$.
H is a subgroup of H if:

1. $\cdot|_H$ is a binary operation on H. (Closure)
2. $(H, \cdot|_H)$ is a group.

Notation: $H \leq G$.

2.1 Subgroups of $\mathbb{Z}$

1. Given $n \in \mathbb{Z}$, define $n\mathbb{Z} := \{nm | m \in \mathbb{Z}\}$.
2. Given $a, b \in \mathbb{Z}$, define $a\mathbb{Z} + b\mathbb{Z} = \{an + bm | n, m \in \mathbb{Z}\}$.
3. If $H \leq \mathbb{Z}$, then $H = \{0\}$ or $H = n\mathbb{Z}$ where n is the smallest positive element of H.
4. $a\mathbb{Z} + b\mathbb{Z}$ is the smallest subgroup of $\mathbb{Z}$ containing a and b.
5. If $(a, b) \neq (0, 0)$, then the smallest positive element of $a\mathbb{Z} + b\mathbb{Z}$ is defined to be $\gcd(a, b)$.
6. If $\operatorname{lcm}(a, b) = l$, then $\langle l \rangle$ is the largest subgroup of $\langle a \rangle \cap \langle b \rangle$.

3 Order and Cyclic groups

Let G be a group and $x \in G$.

Definition 1. $\langle x \rangle$ is the smallest subgroup of G containing x.
$\langle x \rangle = \{\cdots, x^{-2}, x^{-1}, 1, x, x^2, \cdots\}$.

Definition 2. Order of an element x of G is denoted by $o(x)$ and is defined as $o(x) := |\langle x \rangle|$.

G is said to be cyclic if there exists $x \in G$ such that $\langle x \rangle = G$.

4 Sign of permutations

Given $\sigma \in S_n$, σ has a matrix associated to it. Denote it by $[\sigma]$.
$\text{sign}(\sigma) := \det([\sigma])$.
The sign of any transposition is -1.
As any element of S_n can be written as a product of transpositions, the sign is always ± 1.
Permutations with sign 1 are called even permutations and the rest are called odd permutations.
The set of even permutations is denoted by A_n.

5 Homomorphisms

Definition 3. Let G and G' be groups.
A map $\alpha : G \to G'$ is said to be a group homomorphism if:

$$\alpha(g_1 g_2) = \alpha(g_1)\alpha(g_2) \quad \forall g_1, g_2 \in G.$$

(High abuse of notation has been done.)

Definition 4. Let $\alpha : G \to G'$ be a homomorphism.
$\ker \alpha := \{g \in G | \alpha(g) = 1\} = \alpha^{-1}(1)$.
$\operatorname{im} \alpha := \{\alpha(g) | g \in G\}$.

Fact: $\ker \alpha \leq G$ and $\operatorname{im} \alpha \leq G'$.
α is 1-1 $\iff$ $\ker \alpha = \{1\}$.

6 Conjugates, normal subgroup, normaliser, center

Definition 5. $G \to$ group. Let $a, g \in G$. Then the element is gag^{-1} of G is said to be the **conjugate** of a by g.

Definition 6. Let $H \leq G$. H is called a **normal subgroup** of G if

$$\forall h \in H, \forall g \in G : ghg^{-1} \in H.$$

Notation: $H \trianglelefteq G$.

Fact: If K is the kernel of $\varphi : G \to G'$, then $K \trianglelefteq G$.
Remark: Suppose G is generated by $g_1, g_2, \cdots, g_n$. Let $H \leq G$. Then

$$H \trianglelefteq G \iff \forall i \in [n], \forall h \in H : g_i h g_i^{-1} \in H$$

Definition 7. Let $g \in G$. Define $C_g : G \to G$ as $x \mapsto gxg^{-1}$ under C_g.

C_g is a homomorphism for all $g \in G$. In fact, it is an isomorphism.

Definition 8. Let $H \leq G$.
The **normaliser** of H in G is defined as -

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

$N_G(H) \leq G$.

Definition 9. The **center** of a group G is defined -

$$Z(G) := \{g \in G \mid \forall x \in G : gx = xg\}.$$

$Z(G) \trianglelefteq G$.

7 Isomorphisms

Definition 10. $\varphi : G \to G' \longleftarrow$ homomorphism
If φ is bijective, then we say that φ is an isomorphism.

Definition 11. Let G and G' be groups. If there exists $\varphi : G \to G'$ such that φ is an isomorphism, then we say that G and G' are isomorphic.

Facts:
1. φ is an isomorphism $\iff \ker \varphi = (1)$ and φ is onto.
2. If $\varphi : G \to G'$ is a 1-1 homomorphism, then $\bar{\varphi} : G \to \operatorname{im} G\ (\leq G')$ is an isomorphism.
3. Let $\varphi : G \to G'$ be an isomorphism. Let φ^{-1} be the set theoretic inverse of φ. Then, φ^{-1} is a homomorphism and hence, an isomorphism.

Given any set of groups, the relation "is isomorphic to" is an equivalence relation.

Definition 12. $\operatorname{Aut} G := \{\varphi : G \to G \mid \varphi \text{ is a bijection}\}$.
Elements of the above set are called automorphisms of G.

$\operatorname{Aut} G$ is a group under composition.
Example:
1. Let G be a group. Fix $g \in G$. Define $\varphi_G : G \to G$ as $x \mapsto gxg^{-1}$.
   This is an automorphism.
2. $\varphi_g = \mathrm{id} \iff \varphi_g(x) = x\ \forall x \in G \iff g \in Z(G)$.

8 Cosets

Definition 13. Let $G \longleftarrow$ group and $H \leq G$. For $a \in G$, $aH := \{ah : h \in H\}$. This is said to be a left coset of H by a.

Definition 14. $G \longleftarrow$ group. $H \leq G$. Define $g \sim g'$ if $g = g'h$ for some $h \in H$.

This $\sim$ is an equivalence relation.
Thus, G is the disjoint union of left cosets of H in G.
Also, given $g,\ g' \in G$, it either the case that $gH = g'H$ or that $gH \cap g'H = \emptyset$.
Facts:
1. $gH \leq G \iff g \in H$.
2. Fix $g, g' \in G$. Then, we can have a map $\varphi : gH \to g'H$ such that $gh \mapsto g'h$. (Check that this is well-defined.)
   Then, φ is a bijection. $\implies |gH| = |g'H|$.

Definition 15. $[G : H] :=$ index of H in G
$=$ Number of distinct left cosets of H in G. (may be ∞)
$=$ Number of equivalence classes

By the last fact given above, we have it that G is the disjoint union of $[G : H]$ many left cosets of H.
Therefore, $|G| = [G : H]|H|$. (For finite)

Theorem 1. $G \longleftarrow$ finite group and $H \leq G$. Then, $|H| \mid |G|$.

Theorem 2. $|G| = p \longleftarrow$ prime. Then G is cyclic and has $p - 1$ generators.

If $\varphi : G \to G'$ is a homomorphism, $\varphi : G \to \operatorname{im}\varphi$ is onto and $\operatorname{im}\varphi \leq G'$.
If $g' \in \operatorname{im}\varphi$, then there exists $g \in G$ such that $g' = \varphi(g)$. Let $K = \ker\varphi$.
$\varphi^{-1}(g') = \{x \in G : \varphi(x) = g'.\}$ Then, $\varphi^{-1}(g') = gK$.
Also, $\{\text{cosets of } K \text{ in } G\} \cong \operatorname{im}\varphi$ (set isomorphism, i.e., bijection).
$gK \mapsto \varphi(g)$ is the map.
$\therefore |\operatorname{im}\varphi| = [G : K]$.
$|G| = [G : K]|K| \implies |G| = |\operatorname{im}\varphi| \cdot |K|$.
For finite G and G', we have it that $|\operatorname{im}\varphi|$ divides $|G|$ and $|\operatorname{im}\varphi|$ divides G'.
Ex.: The above can use to shown that $|A_n| = n!/2$ for $n \geq 2$.
(Consider the (onto) homomorphism sign : $S_n \to \{-1, 1\}$.)

9 A lemma on normal subgroups

Lemma 1. $G \longleftarrow$ group. $H \leq G$. TFAE:

1. $H \trianglelefteq G$. That is, $\forall g \in G, \forall h \in H : ghg^{-1} \in H$.
2. $gHg^{-1} = H \forall g \in G$.
3. Any left coset of G is also a right coset.

10 Correspondence Theorem

Let $\varphi : G \to G'$ be a group homomorphism.

1. If $H \leq G$, then $\varphi(H) \leq G'$.
2. Let $H \trianglelefteq G$, it is not necessary that $\varphi(H) \trianglelefteq G'$.
3. Assume φ is surjective. Now, if $H \trianglelefteq G$, then $\varphi(H) \trianglelefteq G'$.
4. If $H' \trianglelefteq G'$, then $\varphi^{-1}(H') \trianglelefteq G$. (No assumption of surjectivity.)

Theorem 3. Assume $\varphi : G \to G'$ is a surjective homomorphism.
Then, $\Omega_1 = \{\text{All subgroups of } G \text{ containing } \ker\varphi\} \cong \{\text{All subgroups of } G'\} = \Omega_2$.

Consequence:
Consider $\det : GL_2(\mathbb{R}) \to \mathbb{R}^\times$. This is a surjective map. Moreover, $\mathbb{R}^\times$ is abelian.
Thus, the set of subgroups of $GL_2(\mathbb{R})$ containing $SL_2(\mathbb{R})$ consists of normal subgroups. Moreover, it is in bijection with the set of subgroups of $\mathbb{R}^\times$.
$\det^{-1}(\{\pm 1\}) = SL_2(\mathbb{R}) \cup \{\det -1 \text{ matrices}\}$.

11 Product of Groups

Definition 16. Let G and G' be groups.
Then, the product $G \times G'$ is a group under component wise operation.

That is, for (g_1, g_1') and (g_2, g_2') belonging to $G \times G'$, $(g_1, g_1) \cdot (g_2, g_2') = (g_1 \cdot g_2, g_1' \cdot g_2')$.
(Where the $\cdot$ has different meanings depending on the elements.)

Now, we want to answer the following question -
Given a group G, when can we say that there exist groups G_1 and G_2 such that $G \cong G_1 \times G_2$ where G_1 and G_2 are non-trivial.
Consider the following maps:

$$\begin{tikzcd} G_1 \arrow[dr, "i_1"] & & G_1 \\ & G \arrow[ur, "p_1"] \arrow[dr, "p_2"] & \\ G_2 \arrow[ur, "i_2"] & & G_2 \end{tikzcd}$$

$i_1(g_1) = (g_1, 1)$. i_1 is an injective group homomorphism.
Thus, $G_1 \cong \operatorname{im} i_1 = G_1 \times \{1\}$.
Similarly, $G_2 \cong \operatorname{im} i_1 = \{1\} \times G_2$.
Both the latter groups are subgroups of G.
Thus, a necessary condition is - G must contain subgroups that are isomorphic to G_1 and G_2.
Also, let p_1 be defined as $p_1(g_1, g_2) = g_1$. Then, $\ker p_1 = \{1\} \times G_2 \longleftarrow$ normal subgroup of G.
Similar observation can be made for p_2.
Thus, if $G \cong G_1 \times G_2$, then G contains normal subgroups H_1 and H_2 which are isomorphic to G_1 and G_2. In fact, the following can be observed:
If $G \cong G_1 \times G_2$, then there exists normal subgroups H_1 and H_2 of G such that:

1. $H_1 \cong G_1$ and $H_2 \cong G_2$.
2. $H_1 \cap H_2 = (1)$.
3. $H_1 H_2 = G$.

Where $H_1 H_2 := \{h_1 h_2 \in G : h_1 \in H,\ h_2 \in H\}$.
Exercises:

1. $HK \leq G$ if ($H \trianglelefteq G$ or $K \trianglelefteq G$).
2. $HK \trianglelefteq G$ if ($H \trianglelefteq G$ and $K \trianglelefteq G$)
3. $HK \leq G$ iff $HK = KH$.

Let $H, K \leq G$ and $\varphi : H \times K \to G$ be defined as $(h, k) \mapsto hk$.
Then, $\operatorname{im} \varphi = HK \subset G$.
Let us see when φ is a homomorphism.
We need $\varphi(h, k)\varphi(h', k') = \varphi(hh', kk')$
$\iff hkh'k' = hh'kk' \iff kh' = h'k$.
That is, elements of K and H commute.
Then, we have it that $HK = KH$ and thus, $HK \leq G$.
(Note that $HK = KH$ does not imply that the elements of H and K individually commute. The latter is stronger and that is what implies homomorphism.)

If we want φ to be an isomorphism, we need $\operatorname{im} \varphi = HK = G$.
Also, we need φ to be 1-1. Thus, $\ker \varphi = (1) = \{(1, 1)\}$.
If $(h, k) \in \ker \varphi$, then we have it that $hk = 1$ or $h = k^{-1}$. As H and K are both subgroups, this tells us that $h, k \in H \cap K$. For the sake of isomorphism, we want 1 to be the only element in $H \cap K$.
Thus, we arrive at the conclusion that $H \cap K = \{(1, 1)\}$.

Explicitly stating our results:
There exist $H, K \leq G$ such that $\varphi : H \times K \to G$ given by $(h, k) \mapsto hk$ is an isomorphism iff

1. $hk = kh \quad \forall h \in H,\ k \in K$,
2. $H \cap K = (1)$, and
3. $HK = G$.

The first and third conditions let us conclude that $H \trianglelefteq G$ and $K \trianglelefteq G$.

Example:

Let $G = GL_2(\mathbb{R})^+ := \{M \in GL_2(\mathbb{R}) : \det M > 0\}$.
Let $H = SL_2(\mathbb{R})$ and $K = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} : a \in \mathbb{R}_{>0} \right\}$.
Then, by above theorem $G \cong H \times K$. (Can be verified that H and K satisfy the three criteria.)
Moreover, it can be seen that K is naturally isomorphic to $(\mathbb{R}_{>0}, \cdot)$. Thus, we get that $GL_2(\mathbb{R})^+ \cong SL_2(\mathbb{R}) \times \mathbb{R}_{>0}$.

12 Quotient group

$G \longleftarrow$ group. If $H \leq G$, then define
$G/H := \{gH : g \in G\}$.
We want to define $(gH)(g'H)$ such that it is also a left coset of H.
By the set theoretic definition, $(gH)(g'H) = \{ghg'h' : h, h' \in H\}$.
It is clear $gg' \in (gH)(g'H)$. Thus, if it is a coset, then it must be the coset $(gg')H$.
That would then mean

$$\begin{aligned}
& (gH)(g'H) = gg'H \\
\iff & ghg'h' = gg'h'' && \forall h, h' \in H, \exists h'' \in H \\
\iff & g'^{-1}hg' = h''(h')^{-1} \\
\iff & g'^{-1}hg' \in H \\
\iff & H \trianglelefteq G.
\end{aligned}$$

Now, assume $H \trianglelefteq G$, then G/H is a quotient group. (under the natural product)
There's a natural map $\Pi : G \to G/H$ given by $g \mapsto gH = \bar{g}$.
Π is a group homomorphism. Also, Π is surjective with $\ker \Pi = H$.

12.1 First isomorphism theorem

$$\begin{tikzcd}
G \arrow[rr, two heads, "\varphi"] \arrow[dr, two heads, "\Pi"'] & & G' \\
& G/K \arrow[ur, two heads, "\bar{\varphi}"'] &
\end{tikzcd}$$

Let $\varphi \longleftarrow$ surjective homomorphism.
If $\varphi(g) = g'$, then $\varphi^{-1}(g') = gK$.
Let $K = \ker \varphi$. Given any coset of K, every element in that coset is mapped to the same element under φ. Define $\bar{\varphi} : G/K \to G'$ as $gK \mapsto \varphi(g)$. This is well defined.
As φ was a surjection, so is $\bar{\varphi}$. Moreover, $\bar{\varphi}$ is 1-1. Thus, we have it that $G/K \cong G'$.

13 Symmetries of a Plane

Let $P \longleftarrow$ plane.
An isometry (rigid motion) of P is a distance preserving map $\sigma : P \to P$. That is, $\text{dist}(p, q) = \text{dist}(\sigma(p), \sigma(q))$.
We shall stick to the standard Euclidean distance for the remainder of the notes.

Definition 17. If $S \in P$ such that $\sigma(S) = S$, then σ is called a symmetry of S.

Observation: If σ and τ are isometries of P, then $\sigma \circ \tau$ is also an isometry.
$\Sigma(P)$ = set of all isometries of P. Then, $\Sigma(P)$ is a group under composition.
Examples:

1. Translation.
   Let v be a vector in P. Then define $t_v : P \to P$ as $t_v(p) = p + v$.
   $t_v \in \Sigma(P)$ for all $v \in P$.
2. Rotation.
   Let $p \in P$ and $\theta \in [0, 2\pi)$.
   Define $\rho_{\theta,p} : P \to P$ as rotation by angle θ is counter-clockwise direction about p.
   Then, the above is an isometry.
3. Reflection.
   Let l be a line in P.
   Let $r_l : P \to P$ be reflection about line l. This is also an isometry.
4. Glide reflection.
   Fix a line l in the plane P and fix a vector v parallel to l.
   $t_v \circ r_l \longleftarrow$ glide reflection.
   Glide reflections are also isometries.

Theorem 4. $\Sigma(P)$ consists precisely of translations, rotations, reflections and glide reflections.

Proof. Omitted. $\square$

Definition 18. Let $\sigma \in \Sigma(P)$. σ is called orientation preserving it preserves orientation.
If σ is not orientation preserving, then it is called orientation reversing.

I'm not going into the details of orientation. It is what you intuitively think it should mean.
Translations and rotations are orientation preserving. Reflections and glide reflections are not.

14 Group Action

$G \longleftarrow$ group, $X \longleftarrow$ set.
G acts (operates) on X if there is a map

$$\varphi : G \times X \to X$$

such that

1. $\varphi(1, x) = x \quad \forall x \in X$, and
2. $\varphi(g_1 g_2, x) = \varphi(g_1, \varphi(g_2 x)) \quad \forall g_1, g_2 \in G, \forall x \in X$.

Given a group action, note the following:
Fix $g \in G$, then φ_g is a bijection, where $\varphi_g : X \to X$ defined as $\varphi_g(x) = \varphi(g, x)$.
To show that this is a bijection, note that $\varphi_{g^{-1}}$ is the required set theoretic inverse.

Definition 19. Let $x \in X$.
The orbit of x is defined as

$$O_x := \{\varphi_g(x) : g \in G\} \subset X.$$

The stabiliser of x is defined as

$$G_x := \{g \in G : \varphi_g(x) = x\} \subset G.$$

It is clear that it is always that case that $x \in O_x$ and $1 \in G_x$.

Definition 20. If there exists $x \in X$ such that $O_x = X$, then we say that the action is transitive.

Examples of group action.

1. Let P be a plane and $G = \Sigma(P)$.
   Let $\varphi : G \times P \to P$ be defined as $(\sigma, p) \mapsto \sigma(p)$.
   It can be verified that this is a group action.
   Moreover, this is a transitive group action.
   Given any $x \in X$, the stabiliser of x consists of the identity map, the rotations about x and the reflections about lines l such that $x \in l$.

2. Let P be a plane and $X = \{l : l \text{ is a line in } P\}$.
   Then $G \times P \to P$ defined similarly as before, is once again a transitive group action.
   The stabiliser of any line l consists of the identity, translations by vectors parallel to l, reflection about l, glide reflections about l and rotations by π about any point on l.

3. Can similarly do this for circles.

14.1 Dihedral groups

Let P be a plane and x_n be a regular $n-$gon in the plane.
Consider the group action described above. The *dihedral group of order n* is the stabiliser of x_n.
Given any $n-$gon, it is easy to see that the element x and y are symmetries of x_n, where x is rotation about the center in the counterclockwise direction by angle $2\pi/n$ and y is reflection about any of its line of symmetry.
It can be verified that $x^n = 1$ and $y^2 = 1$.
Moreover, it can be shown that

$$D_n = \langle x, y | x^n = y^2 = 1, yx = x^{-1}y \rangle.$$

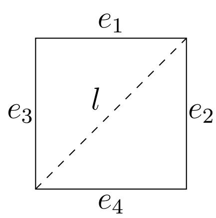
14.2 Partitions by orbits

Assume that G acts on X. If the action is φ, then let us write $\varphi(g, x)$ as simply gx.
Define a relation on X by

$$x \sim y \text{ if } \exists g \in G : y = gx.$$

Then, $\sim$ is an equivalence relation on X.
For $x \in X$, $[x]$ is the equivalence class of x.
Observe that $[x] = O_x$, by definition.
Thus, the orbits of elements of X partition X.
This means that if an action is transitive, there is only one orbit.
What this also means is that if $O_x = X$ for some $x \in X$, then $O_x = X$ for all $x \in X$.
Examples

1. S_n acts naturally on $S = \{1, 2, \ldots, n\}$.
   Define $S_n \times S \to S$ as $(\sigma, i) \mapsto \sigma(i)$.
   $O_1 = S$. Thus, this action is transitive. Also, $G_1 \cong S_{n-1}$.
2. $G = D_4 \longleftarrow$ isometries of a square.



Then, $G = \langle x, y | x^4 = y^2 = 1, yx = x^3y \rangle$.
Where $x \longrightarrow$ rotation by $2\pi/4$ about center and $y \longrightarrow$ reflection about line l.
$|D_4| = 8$.
Let $X = \{e_1, e_2, e_3, e_4\} \longleftarrow$ edges of the square.
G acts on X in the natural way.
$O_{e_1} = X$. $G_{e_1} = \{1, xy\}$.

Suppose $g_1, g_2 \in G$ and $x \in X$ such that $g_1x = g_2x$.
Observe that $g_1x = g_2x \iff g_2^{-1}(g_1x) = x \iff (g_2^{-1}g_1)x = x \iff g_2^{-1}g_1 \in G_x$.
That is equivalent to saying $g_1 \in g_2G_x$.

Suppose $y = gx$ is given and we have G_x. Can we find G_y?
$G_y = \{g_1 \in G : g_1y = y\} = \{g_1 \in G : g_1(gx) = gx\} = \{g_1 \in G : g^{-1}g_1gx = x\}$
$\iff G_y = \{g_1 \in G : g^{-1}g_1g \in G_x\} = \{g_1 \in G : g \in gG_xg^{-1}\}$.
$\iff G_y = gG_xg^{-1}$.
Thus, if we know the stabiliser of x, we can find the stabiliser of any element in the orbit of x.

14.3 Action on cosets

$G \longleftarrow$ group and $H \leq G$. $G/H \longleftarrow$ set of all cosets of H. (H is not necessarily normal, so G/H is not necessarily a group.)
There is a natural action of G on G/H :

$$G \times G/H \to G/H$$

$$(g, C) \mapsto gC$$

We take $H \in G/H$, then we get that $O_H = G/H$. Thus, this action is transitive.
Also, $G_H = H$. Thus, by our previous result, we get that $G_{aH} = aHa^{-1}$.

Example
Let $G = S_3$ and $H = \langle (12) \rangle$. That is, $H = \{1, (12)\}$.
Then, $G/H = \{H, (13)H, (23)H\} = \{a_1, a_2, a_3\}$ where $a_1 = \{1, (12)\}$, $a_2 = \{(13), (123)\}$ and $a_3 = \{(23), (132)\}$.
Let $s = (13)H$. Then, $O_s = G/H$. (We had noted the action is transitive before as well.)
$G_s = (13)H(13)^{-1} = \{1, (23)\}$.
Let us observe one more thing:
For a fixed $g \in S_3$, define $m_g : G/H \to G/H$ as left multiplication by g.
Let $g = (12)$. Under this map, we see the following

$$a_1 \mapsto a_1$$

$$a_2 \mapsto a_3$$

$$a_3 \mapsto a_2$$

With a slight abuse of notation, we can write it as $m_{(12)} = (a_3, a_2)$. Similarly, we get that $m_{(13)} = (a_2, a_1)$ and $m_{(123)} = (a_1, a_2, a_3)$.
What we have observed is that there is a natural correspondence from the elements of G to S_3.

In general, given an action $G \times S \to S$, we get a map $m : G \to \mathrm{Perm}(S)$ defined as $g \mapsto m_g$.
If we take two elements of the group - g_1 and g_2, we see that $m(g_1g_2) = m_{g_1g_2}$.
Note that $m_{g_1g_2}$ is a function from S to S. Given any element $x \in S$, we get that $m_{g_1g_2}(x) = (g_1g_2)x$. By our axioms of group action, we get that it is equal to $g_1(g_2x) = m_{g_1}(m_{g_2}(x))$.
This shows that $m_{g_1g_2} = m_{g_1} \circ m_{g_2}$. Recall that the set of permutations (self bijections) of a

set form a group under composition. Thus, what we have shown is that the above map m is in fact a group homomorphism from G to $\mathrm{Perm}(S)$.

Moreover, $\ker m = \{g \in G : m_g = \mathrm{id}_S\} = \{g \in G : m_g(s) = s \quad \forall s \in S\} = \{g \in G : gs = s \quad \forall s \in S\}$.
$\iff \ker m = \bigcap_{s \in S} G_s$.
This also shows that the intersection of all the stabilisers is a normal subgroup. Moreover, if it is non-trivial, we get a non-trivial normal subgroup of G.

15 Orbit - Stabiliser Theorem

Let G be a group acting on a set X. Take $x \in X$. Consider the following natural map

$$G \xrightarrow{\phi} O_x \text{ defined as } g \overset{\phi}{\mapsto} gx.$$

This is a surjective map. Let $g_1 \in gG_x$. Then $g_1 = gg'$ for some $g' \in G_x$.
Then, $g_1 \overset{\phi}{\mapsto} g_1 x = (gg')x = g(g'x) = gx = \phi(g)$.
Thus, every element in the same coset of G_x goes to the same element.
This gives us a natural isomorphism defined in the following manner:

$$G/G_x \xrightarrow{\psi} O_x \text{ defined as } gG_x \mapsto gx.$$

This map is well defined due to our observations earlier. It is easy to show that this is one-one and onto.
This gives us that $|O_x| = [G : G_x]$.

Corollary 1. When G is a finite set acting on X, we have that

$$|G| = |G_x||O_x|.$$

Recall that if G acts on X, then $m_g : X \to X$ was a bijection for all g and we got a group homomorphism $m : G \to \mathrm{Perm}(X)$ by sending g to m_g.
We had derived that $\ker m = \bigcap_{x \in X} G_x$.
If it is the case that $\ker m = (1)$, then G can be thought of as a subgroup of $\mathrm{Perm}(X)$ as $m : G \to m(G)$ is an isomorphism and $m(G) \subset X$.

16 Simple groups

Definition 21. A group G is simple if it has no nontrivial normal subgroups.

In the above, trivial subgroups mean - (1) and G.
Example:
Let G be a finite group of order n. Let $H \lneq G$ such that $[G : H] = r$. G acts on G/H by left multiplication.

$$m : G \longrightarrow \mathrm{Perm}(G/H) \cong S_r$$

If $n \nmid r!$, then m is not one-one. (One-one would mean that $m(G)$ has order n but $m(G) \leq \mathrm{Perm}(G/H)$.)

Thus, the kernel is not (1).
$\ker m = \bigcap_{a \in G} G_{aH} = \bigcap_{a \in G} aHa^{-1} \leq H \lneq G.$
Thus, $\ker m$ is not equal to the whole group either. This gives us that $\ker m$ is a nontrivial normal subgroup. Thus, G is not simple.

The above example also shows that given $H \leq G$, we know that $\bigcap_{g \in G} gHg^{-1} \trianglelefteq G$.

Also, $\bigcap_{g \in G} ghg^{-1}$ is the largest normal subgroup of G contained in H.

A side note: Given $G \longleftarrow$ group and $H \leq G$, H/G is the set of right cosets of H in G. If we define an map $G \times H/G \to H/G$ as $(g, C) \mapsto Cg$, this won't satisfy the axioms of group action in general.
Thus, we define $g \cdot C$ as $C \cdot g^{-1}$.

G acts on $S = \wp(G) \setminus \{\emptyset\}$ with $(g, C) := gC = \{gc : c \in C\}$.

We saw that if G acts on X, then $m : G \to \text{Perm}(X)$ is a homomorphism.
Conversely, if $\varphi : G \to \text{Perm}(X)$, then we can define $f : G \times X \to X$ as $(g, x) \mapsto (\varphi(g))(x)$.
Then, f is a group action.
Moreover, the homomorphism corresponding to f turns out to be φ. Thus, there is a bijection between these objects.

Theorem 5 (Cayley)**.** Let G be a group and $X = G/H$ where $H = (1) \leq G$.
Let φ be the natural action of G on X.
Then, $m : G \to \text{Perm}(X)$ has its kernel given by -
$\ker m = \bigcap_{g \in G} gHg^{-1} = \bigcap_{g \in G} \{1\} = (1).$
Thus, m is injective.
This shows that G can embedded into $\text{Perm}(G)$. That is, it can be seen as a subgroup of a symmetric group.

Definition 22. If m is injective, then our action is called faithful.

In case of a faithful action, 1 is the only g in G such that $gx = x$ for all $x \in X$.
G acts on G by conjugation.
$G \times G \to G$ defined as $(g, x) \mapsto gxg^{-1}$.
$O_x = \{gxg^{-1} : g \in G\}$. If a normal subgroup contains x, then it must contain O_x.

$\varphi_g : G \to G$ given by $x \mapsto gxg^{-1}$ is an automorphism.
Moreover, $m : G \to \operatorname{Aut} G$ given by $g \mapsto \varphi_G$ is a homomorphism.

Suppose G is generated by g_1 and g_2. Let $H \leq G$. If $\varphi_{g_1}(H) = \varphi_{g_2}(H) = H$, then $\varphi_g(H) = H \quad \forall g \in G$.
This will follow from the fact that $g \mapsto \varphi_g$ is a homomorphism.
Given $x \in G$, we get that $O_x = [x] \longleftarrow$ conjugacy class of x in G.
Moreover, the stabiliser $G_x = \{g \in G : xg = gx\}$. This called the centraliser of x.
Also, we have the homomorphism $m : G \to \operatorname{Aut} G$ whose kernel is given by $\ker m = \bigcap_{x \in G} G_x = Z(G) \longleftarrow$ center of G.

$x \in Z(G) \iff Z(x) = G \iff O_x = C(x) = \{x\}$.
In general, $x \notin Z(G) \implies Z(G) \subsetneq Z(x)$ and $x \in Z(G) \implies Z(x) = G$.

17 Class Equation

G is the disjoint union of orbits, that is, conjugacy classes.
In general, $G = \bigsqcup_{x \in S \subset G} C(x)$ which gives us that $|G| = \sum_{x \in S \subset G} |C(x)|$.
The above is known as the class equation.
(S is a subset of G with the property that given any $x \in G$, there is exactly one member $|S \cap C(x)| = 1$.)
Observation: Given a finite group G such that $|G| = 1 + 1 + \cdots + 1 + n_1 + \cdots + n_k$ is the class equation, (where $n_i > 1$ for all valid i) we know the following: The number of 1s, say n, is the cardinality of $Z(G)$. Moreover, given any n_i, $n < |G|/n_i < |G|$ and $n \mid |G|/n_i \mid |G|$. (Each n_i actually represents the cardinality of the *orbit* of some element in G.)
Examples.

1. Find the class equation of $G = S_3$.
   $Z(G) = \{1\}$. Also, $O_x = \{x, x^2\}$. That is, $|O(x)| = 2$.
   The only possibility left for $|O_y|$ is 3.
   Thus, the class equation is $|G| = 1 + 2 + 3$.

2. Find the class equation of $G = D_4$.
   $Z(D_4) = \{1, x^2\}$.
   Thus, $|G| = 1 + 1 + \text{something}$.
   For $x \in G \setminus Z(G)$, we have it that $Z(G) \lneq Z(x) \lneq G$. As $|Z(G)| = 2$ and $|G| = 8$, the only possibility is $|Z(x)| = 4$ or $|O(x)| = 2$. This gives us that the "something" can only consist of 2s. As we have 6 left, we get that $|G| = 1 + 1 + 2 + 2 + 2$.

3. Let G be a group such that $|G| = 10$. Show that $1 + 1 + 1 + 2 + 5$ cannot be the class equation.
   $Z(G)$ cannot have 3 elements. ■

4. Show that $1 + 1 + 2 + 2 + 2 + 2$ is not possible.
   We are given that $|Z(G)| = 2$ and $|Z(x)| = 10/2 = 5$ for some $x \in G$. But this is a contradiction as $|Z(G)|$ should divide $|Z(x)|$ but $2 \nmid 5$.

Definition 23. If $|G| = p^n$ for some prime p and $n \in \mathbb{N}$, then G is said to be a $p-$group.

Theorem 6. If G is a $p-$group, then $Z(G) \neq (1)$.

Proof. Assume $Z(G) = 1$, then the class equation will give us that:

$$p^n = 1 + p^{\alpha_1} + \cdots p^{\alpha_k}.$$

This is a contradiction as the left hand side is divisible by p but the right hand side is not. □

Theorem 7. If $|G| = p^2$ for some prime p, then G is abelian.

Proof. By the previous theorem, we know that $|Z(G)| > 1$. If $|Z(G)| = p^2$, then we are done. Assume not. Then, $|Z(G)| = p$.
Thus, $G \setminus Z(G)$ is nonempty. Let $x \in G \setminus Z(G)$. Then, we have it that $Z(G) \lneq Z(x) \lneq G$. However, considering the divisibilities of orders, this is not possible. □

Theorem 8. If $|G| = p^2$ for some prime p, then $G \cong \mathbb{Z}/p^2\mathbb{Z}$ or $G \cong (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})$.

Proof. G contains an element of order p^2, then G is cyclic and we are done.
Assume G does not have an element of order p^2. In that case, all elements ($\neq 1$) have order p.
Choose $1 \neq x \in G$. Choose $y \in G \setminus \langle x \rangle$.
Then, we have it that $\langle x \rangle \cong \langle y \rangle \cong \mathbb{Z}/p\mathbb{Z}$. Moreover, $\langle x \rangle \cap \langle y \rangle = (1)$.
As G is abelian, by previous theorem, we also have it that $\langle x \rangle\langle y \rangle = \langle y \rangle\langle x \rangle$.
Lastly, we also have it that $\langle x \rangle\langle y \rangle = G$. Thus, $G \cong \langle x \rangle \times \langle y \rangle$ and we are done. $\square$

18 Classification Theorems

Theorem 9 (Classification of finite Abelian Groups)**.** Let G be a finite abelian group.
$|G| = p_1^{n_1} \cdots p_k^{n_k}$: p_is are distinct primes.
Then, $G \cong G_1 \times G_2 \times \cdots \times G_k$ where $|G_i| = p_i^{n_i}$ for each valid i.
Now, let us assume that $|G| = p^n$.
For each partition $\mathcal{P}$ of n such that $\mathcal{P} = (t_1, t_2, \ldots, t_s)$ and $\sum_{k=1}^{s} t_k = n$, define the following:

$$G_{\mathcal{P}} := (\mathbb{Z}/p^{t_1}\mathbb{Z}) \times \cdots \times \left(\mathbb{Z}/p^{t_s}\mathbb{Z}\right).$$

Then, $G \cong G_{\mathcal{P}}$ for some partition $\mathcal{P}$.

Theorem 10 (Classification of finitely generated Abelian Groups)**.** Let G be a finitely generated abelian group.
Then, $G \cong \mathbb{Z}^r \times T$ for some natural number r and group T such that $|T| < \infty$. This r is known as the rank of G.

19 Conjugation in S_n

Let $p \in S_n$ and $q \in S_n$. We can visualise qpq^{-1} easily in terms of q by replacing each element i in the cycle representation of p with $q(i)$.
Example: Let $p = (123)(457)$ and $q = (134267)$. Then $qpq^{-1} = (q(1), q(2), q(3))(q(4), q(5), q(7)) = (364)(251)$.
Thus, all conjugates of an element have the same cycle type. Moreover, it can be easily seen that given any element y of the same cycle type as x, one can find a $q \in S_n$ such that $y = qxq^{-1}$.
Thus, the conjugacy class of any element p consists of all the elements of the same cycle type as p.

Theorem 11. Two permutations $p, q \in S_n$ are conjugates iff p and q have the same cycle type.

Thus, one can now find the class equations of S_n (relatively) easily.
Example: Find the class equation of S_4.
Let us consider the possible cycle types and the number of elements with that cycle type:
$id \longrightarrow 1$
$(12) \longrightarrow \frac{1}{2}{}^4P_2 = 6$
$(123) \longrightarrow \frac{1}{3}{}^4P_3 = 8$
$(1234) \longrightarrow \frac{1}{4}{}^4P_4 = 6$
$(12)(34) \longrightarrow \frac{1}{2!}\left(\frac{1}{2}{}^4P_2\right)\left(\frac{1}{2}{}^2P_2\right) = 3$
Thus, the class equation is $|S_4| = 1 + 6 + 8 + 6 + 3$.
Facts:

1. S_n is generated by transposition.
2. A_n is generated by $3-$cycles.
3. If $n \geq 5$, then all $3-$cycles are conjugates in A_n.

Theorem 12. If $n \geq 5$, then A_n is simple. That is, A_n has no nontrivial normal subgroups.

Proof. Let $(1) \neq H \trianglelefteq A_n$.
We shall prove the theorem by showing that H contains a $3-$cycles. As H is normal, it must contain all the conjugates (in A_n) of this $3-$cycle. By the last fact above, this would then contain all the $3-$cycles. By the second fact, we'll get that $A_n \subset H$ and thus, proving that $H = A_n$.
Rest is omitted. $\square$

G acts on $S = \wp(G) \setminus \{\emptyset\}$ by conjugation.
$\varphi : G \times S \to S$ such that $(g, A) \overset{\varphi}{\mapsto} gAg^{-1}$.
Let $H' \leq G$. $O_H =$ all conjugate subgroups of H.
$G_H = \{g \in G : gHg^{-1} = H\} = N_G(H) \longleftarrow$ normaliser of H in G.
$H \trianglelefteq N_G(H) \longleftarrow$ largest subgroup of G containing H such that H is normal in that.
$|G| = |O_H||G_H|$. Thus, $[G : G_H] = |O_H|$.
$H \trianglelefteq G$ iff $N_G(H) = G$ iff $O_H = \{H\}$.

Example:
$x = (12)(34) \in G = S_5$. $H = \langle x \rangle$.
What is $N_G(H)$?
It is clear that $|H| = 2$. Also, O_H (under conjugation) consists of all the elements of S_5 which have cycle type $2, 2, 1$. There are 15 such elements. Thus, $|N_G(H)| = |G_H| = |G|/|O_H| = 8$.
Also, note that if $g = g_1 g_2 \cdots g_r \longleftarrow$ product of disjoint cycles, then each $g_i \in Z(g) = N_G(\langle g \rangle)$ as each g_i will commute with g.
Thus, we already have it that (12) and (34) belong to $N_G(H)$. Thus, $\langle (12), (34) \rangle \subset N_G(H)$. We still need 4 more elements.
Note that if we find the element that conjugates (12) to (34), even that must belong to $N_G(H)$. That element can be easily found to be $(13)(24)$.
Thus, $N_G(H) = \langle (12), (34), (13)(24) \rangle \longleftarrow$ check that this contains 8 elements.

20 Conjugation in A_n

Given $p \in S_n$, we know that all of its conjugates in S_n are precisely those permutations that have the same cycle type. However, they may not be conjugates in A_n.
Let $p \in S_n$. We know that $|C_{S_n}(p)| = \dfrac{|S_n|}{|Z_{S_n}(p)|}$.
Similarly, $|C_{A_n}(p)| = \dfrac{|A_n|}{|Z_{A_n}(p)|}$.
Case 1. Suppose it is the case that $Z_{S_n}(p)$ does not contain any odd permutation. This means that $|Z_{S_n}(p)| = |Z_{A_n}(p)|$ and thus, $|C_{A_n}(p)| = \dfrac{|A_n|}{|Z_{A_n}(p)|} = \dfrac{\frac{1}{2}|S_n|}{|Z_{S_n}(p)|} = \dfrac{1}{2}|C_{S_n}(p)|$.
Case 2. Suppose it is the case that $Z_{S_n}(p)$ does contains an odd permutation. Let σ be any such permutation. Let $H = Z_{S_n}(p) \cap A_n$. That is, the set of all even permutations in $Z_{S_n}(p)$. Moreover, this is a subgroup.
Let τ be an odd permutation in $Z_{S_n}(p)$. Note that $Z_{S_n}(p)$ is a subgroup. Thus, $\sigma^{-1}\tau \in Z_{S_n}(p)$. Also, note $\sigma^{-1}\tau$ is an even permutation. Thus, $\sigma^{-1}\tau \in H$. Or equivalently, $\tau \in \sigma H$. Thus,

we have shown that whenever τ is an odd permutation in $Z_{S_n}(p)$, it must belong to σH. This shows that $|H| = |Z_{A_n}(p)| = \frac{1}{2}|Z_{S_n}(p)|$.
Thus, we get that $|C_{A_n}(p)| = |C_{S_n}(p)|$.

Example:
Let $G = A_5$. Take $x = (12345) \in A_5$.
We know that number of 5−cycles in A_5 is 24. All of these are conjugates in S_5. Are they still conjugates in A_5?
Let us assume that this is indeed the case. This tell us that $|O_x| = 24$. However, 24 does not divide $|A_5| = 60$. Thus, it cannot be the case.
We have shown above that the only other possibility is for $|O_x|$ to be $24/2 = 12$.
What this means is that there are two conjugacy classes in A_5 that consist of 5−cycles.

21 Sylow Theorem

$G \longleftarrow$ group.
$|G| = p^\alpha m$ where $\alpha \geq 1$, $p \to$ prime, $p \nmid m$.
$\text{Syl}_p(G) = \{\text{subgroups of } G \text{ of order } p^\alpha\}$.
An element of $\text{Syl}_p(G)$ is called a Sylow p−subgroup of G.
$n_p(G) := |\text{Syl}_p(G)|$.

Theorem 13 (Sylow)**.** There are three parts to the theorem:
First. $n_p \geq 1$.
Second.

1. All Sylow p subgroups of G are conjugates.
2. If H is a p−group, then H is contained in some Sylow p−subgroup.

Third.

1. Fix $M \in \text{Syl}_p(G)$.
   $n_p = |O_M| \longleftarrow$ number of conjugacy classes of M
   $[G : N_G(M)] = n_p$
   $\implies |N_G(M)| = \frac{|G|}{n_p} = \frac{p^\alpha m}{n_p}$.
   Also, $M \leq N_G(M)$. As $|M| = p^\alpha$, we get that $p^\alpha \mid |N_G(M)|$.
   (a) $n_p \mid m$
   (b) $n_p \equiv 1 \mod p$

Consequences: Let G be a finite group.

1. If $p \mid |G|$, then G has an element of order p.

   Proof. $|G| = p^\alpha m$, where $\alpha \geq 1$. By Sylow Theorem, there exists $H \leq G$ such that $|H| = p^\alpha$.
   Choose $1 \neq x \in H$. Then $\text{ord}(x) = p^\beta$ for some $1 \leq \beta \leq \alpha$.
   Choose $y = x^{p^{\beta-1}}$. Then $\text{ord}(y) = p$. □

2. If $p \mid |G|$ and $H \in \text{Syl}_p(G)$, then $H \trianglelefteq G$ iff $n_p = 1$.

3. Assume $|G| = pq$ where $p < q \longleftarrow$ primes.

Proof. Then $n_q \mid p$. Thus, $n_q = 1$ or p.
Also, $n_q = 1 + kp$ for some $k \in \mathbb{Z}$. As $p < q$, we have it that $n_q = 1$.
Thus, $H \in \mathrm{Syl}_q(G)$ is a nontrivial normal subgroup of G. Thus, G is not simple. □

4. If $\mathrm{ord}(G) = p$, then G is abelian and simple. (There are no nontrivial subgroups to begin with.)

5. If $\mathrm{ord}(G) \neq$ prime and G is abelian, then G is not simple.

   Proof. Using (1), we get that G has a proper subgroup. As G is abelian, this is normal. □

6. If $|G| = p^\alpha$ for prime p and $\alpha \geq 2$, then G is not simple.

   Proof. As G is a $p-$group, $Z(p) \neq (1)$.
   If $Z(G) = G$, then G is abelian and we are done by (5).
   If $Z(G) \neq G$, then we have it that $Z(G)$ is a nontrivial normal subgroup of G and we are done. □

7. $|G| = p^2 q$. $p, q \longleftarrow$ primes, then G is not simple.

   Proof. (i) $p > q$. Then similar arguments as (3) show that $n_p = 1$ and thus, we are done.
   (ii) $p < q$. Then $n_q \mid p^2$ and $n_q \equiv 1 \mod q$. If $n_q = 1$, then we are done. Assume $n_q \neq 1$.
   If $n_q = p$, then $p = 1 + kp$ for some $k \in \mathbb{N}$. This is not possible as $q > p$.
   Thus, the only possibility left is that $n_q = p^2$.
   In that case, $\mathrm{Syl}_q(G) = \{P_1,\ P_2, \ldots,\ P_{p^2}\}$ such that P_i has prime order (q) for all valid i.
   Given $i \neq j$, P_i and P_j are distinct. Thus, $P_i \cap P_j$ is a proper subgroup of P_i. As P_i has prime order, we have it that $P_i \cap P_j = (1)$.
   Thus, if we calculate the number of elements in G that have order q, we get that it is:
   $n = p^2(q-1)$.
   Thus, the number of element remaining is $p^2 q - p^2(q^2 - 1) = p^2$.
   By Sylow Theorem, these remaining p^2 elements *have* to form a subgroup. More importantly, this is the only subgroup of order p^2.
   Thus, $n_p = 1$. $\implies$ G is not simple. □

8. $|G| = pqr$. $p < q < r \longleftarrow$ primes.
   For sake of contradiction, assume that $n_r, n_q, n_p > 1$.
   By arguments similar to previous ones, we know that n_r must be pq.
   # of elements of order $r = pq(r-1)$.
   $n_q > 1$, $n_q \equiv 1 \mod q$ and $n_q \mid pr$ gives us that $n_q \geq r$. $\therefore$ # of elements of order $q \geq r(q-1)$.
   Similarly, we get that $n_p \geq q$ and hence, # of elements of order $p \geq q(p-1)$.
   The above number are counting distinct elements. Thus, we get that -
   $|G| \geq pq(r-1) + r(q-1) + q(p-1) = pqr + (r-1)(q-1) > pqr$. A contradiction.

Theorem 14. Suppose $|G| \leq 200$ and $60 \neq |G| \neq 168$ and $|G|$ is not a prime. Then, G is not simple.