Groups

Shing Tak Lam*

April 13, 2021

This document is intended for revision purposes. As a result, it does not contain any exposition. This is based off lectures given by Dr Ana Khukhro in Michaelmas 2020, but the order of content, as well as some of the proofs have been modified after the fact, primarily to provide simpler proofs for theorems. Note that this also contains theorems from examples sheets, as some are useful elsewhere.

Throughout this document, G is a group, H is generally another group or a subgroup of G. φ is a homomorphism. N is usually a normal subgroup.

A summary of proofs is also provided, it is centred and italicised and occurs before the proof.

Groups is on *Paper 3*.

Contents

*stl45@cam.ac.uk

1 Subgroups

Lemma (Fast subgroup check). *If $H \subseteq G$, H is nonempty and $\forall a, b \in H, ab^{-1} \in H$, then H is a subgroup of G.*

Proof. Say $x \in H$. Then $xx^{-1} = e \in H$. So $eb^{-1} = b^{-1} \in H$. So $ab = a(b^{-1})^{-1} \in H$ for all $a, b \in H$. □

Proposition. *Let $X \subseteq G$. Then $\langle X \rangle$ is the intersection of all subgroups containing X. It is also the smallest subgroup containing X. That is, if $X \subseteq H \leq G$, then $\langle X \rangle \leq H$.*

Proof. Let $\langle X \rangle$ be the intersection of all subgroups containginging X. Then if $X \subseteq H \leq G$, we must have that $\langle X \rangle \leq H$.

Conversely, if $\langle X \rangle$ is a subgroup satisfying the minimality property, then we must have $\langle X \rangle \leq \bigcap_{X \subseteq H \leq G} H$ as $\langle X \rangle$ is a subgroup of each of the H. From minimality, we must have that $\langle X \rangle \cap \bigcap_{X \subseteq H \leq G} H = \langle X \rangle$, and we are done. □

2 Homomorphisms

Definition (Image). The image of a homomorphism $\varphi : G \to H$ is

$$\operatorname{Im}(\varphi) = \{h \in H : \exists g \in G, \varphi(g) = h\}$$

Definition (Kernel). The kernel of a homomorphism $\varphi : G \to H$ is

$$\ker(\varphi) = \{g \in G : \varphi(g) = e\}$$

Proposition. *φ is surjective if and only if $\operatorname{Im}(\varphi) = H$.*

Proof. By definition. □

Proposition. *φ is injective if and only if* $\ker(\varphi) = \{e\}$.

Proof. ($\implies$). If $\varphi(m) = e$, then $\varphi(m) = \varphi(e)$, so $m = e$.
($\impliedby$). If $\varphi(x) = \varphi(y)$ then $\varphi(xy^{-1}) = e$, $xy^{-1} \in \ker\varphi$ and $xy^{-1} = e$, so $x = y$. $\square$

Proposition. $\operatorname{Im}\varphi \leq H$

Proof. $e \in \operatorname{Im}\varphi$. If $g, h \in \operatorname{Im}\varphi$, let $x, y \in G$ be such that $\varphi(x) = g$, $\varphi(y) = h$. Then $gh^{-1} = \varphi(x)\varphi(y)^{-1} = \varphi(xy^{-1})$. $\square$

Proposition. $\ker\varphi \leq G$

Proof. $e \in \ker\varphi$, and if $g, h \in \ker\varphi$, $\varphi(gh^{-1}) = \varphi(g)\varphi(h)^{-1} = e$, so $gh^{-1} \in \ker\varphi$ by the fast subgroup check. $\square$

3 Direct Product Theorem

Theorem. *If $H, K \leq G$, $H \cap K = \{e\}$, $G = HK$, $\forall h \in H, \forall k \in k, hk = kh$, then $G \cong H \times K$.*

Proof. Consider $\varphi(h, k) = hk$. φ is a group homomorphism (by commutativity), and clearly it is surjective.
If $\phi(h, k) = hk = e$, then $h = k^{-1}$ so $h \in K$, and $h = e$. Then $k = e$, so $(h, k) = (e, e)$ as required. $\square$

4 Examples of Groups

4.1 Cyclic Groups

Definition (Cyclic Group)**.** A group G is cyclic if there exists $a \in G$ such that $G = \langle a \rangle$.

Proposition. *An infinite cyclic group is isomorphic to $\mathbb{Z}$.*

Use the "obvious" map, there is no $k > 0$ such that $b^k = e$.

Proof. Suppose $G = \langle a \rangle$. Define $\varphi : \mathbb{Z} \to G$ by $\varphi(k) = a^k$. $\varphi(k + m) = a^{k+m} = a^k a^m = \varphi(k)\varphi(m)$. So φ is a homomorphism. Clearly φ is surjective. Now suppose if $m \in \ker(\varphi)$. Then $\varphi(m) = a^m = e$. If $m \neq 0$, this would mean that G is finite. Contradiction. So φ is injective. $\square$

Proposition. *If $|G| = n$, $G = \langle b \rangle$, then $G \cong C_n$.*

Map generator to generator. Check cases where $i + j < n$ and $\geq n$ separately.

Proof. Let $C_n = \langle a \rangle$. Define $\varphi : C_n \to G$ by $\varphi(a^k) = b^k$. For any $a^j, a^k \in C_n$, $\varphi(a^j a^k) = b^{j+k} = b^j b^k = \varphi(a^j)\varphi(a^k)$ if $j + k < n$. If $j + k \geq n$ then $\varphi(a^j a^k) = \varphi(a^{j+k-n}) = b^{j+k-n} = b^{j+k}(b^n)^{-1} = b^{j+k} = b^j b^k = \varphi(a^j)\varphi(a^k)$. So φ is a homomorphism.

Since $G = \langle b \rangle$, and $b^n = e$, all elements of G can be written as b^k with $0 \leq k < n$. So φ is surjective. Given that $\varphi(a^k) = e$ means that $b^k = e$, we must have that $k = 0$, as otherwise we get a contradiction with the definition of the order of an element. Thus φ is an isomorphism. $\square$

4.2 Dihedral Groups

Definition (Dihedral Group)**.** The dihedral group of order $2n$ is the group of symmetry of the regular n-gon. Algebraically it is $D_{2n} = \langle r, s \mid r^n = s^2 = e, rs = sr^{-1} \rangle$. Geometrically r is a rotation by $2\pi/n$, s is a reflection through a fixed line, and sr^n are the reflections across different lines of symmetry.

4.3 Quaternions

Definition. The quaternion group, Q_8 is given by the following presentation

$$Q_8 = \langle -1, i, j, k \mid (-1)^2 = 1, i^2 = j^2 = k^2 = ijk = -1 \rangle$$

A complex matrix representation of Q_8 can be given by $1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $i = \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix}$, $j = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and $k = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$.

5 Lagrange's Theorem

5.1 Cosets

Definition (Left coset)**.** Let $H \leq G$, $g \in G$. Then $gH = \{gh : h \in H\}$ is a left coset of H in G.

Definition (Index)**.** The index of $H \leq G$, denoted as $|G : H|$ is the number of distinct cosets of H in H.

Proposition. *For $g_1, g_2 \in G, H \leq G$.*

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

$$g_2 \in g_2 H = g_1 H. \; g_1 = g_1(g_1^{-1} g_2)(g_1^{-1} g_2)^{-1}$$

Proof. ($\implies$). $g_2 \in g_2 H = g_1 H$, so there exists h_1 such that $g_2 = g_1 h_1$. Then $g_1^{-1} g_2 = h_1 \in H$.

($\impliedby$). Now let $h \in H$ be arbitrary. $g_1 h = g_1(g_1^{-1} g_2)(g_1^{-1} g_2)^{-1} h = g_2((g_1^{-1} g_2)^{-1} h) \in g_2 H$. So $g_1 H \subseteq g_2 H$. Similarly, $g_2 h = g_2(g_2^{-1} g_1)(g_1^{-1} g_2) h = g_2((g_1^{-1} g_2) h) \in g_2 H$. So $g_1 H = g_2 H$. ☐

5.2 Lagrange's Theorem

Lemma. *Cosets cover. That is,*

$$G = \bigcup_{g \in G} gH$$

Proof. For all $g \in G$, $g \in gH$ so $G \subseteq \bigcup_{g \in G} gH$. Reverse inclusion is trivial. ☐

Lemma. *Cosets are disjoint.*

Consider elements in the intersection, show the cosets are equal.

Proof. Suppose if there exists $g \in g_1 H \cap g_2 H$. Then $g = g_1 h_1 = g_2 h_2$. With this, $g_2 = g_1 h_1 h_2^{-1}$. So for any $h \in H$, $g_2 h = g_1 h_1 h_2^{-1} h = g_1(h_1 h_2^{-1} h) \in g_1 H$. So $g_2 H \subseteq g_1 H$. Similarly $g_1 H \subseteq g_2 H$. So $g_1 H = g_2 H$. ☐

Proposition. *Cosets partition G.*

Lemma. *If H is finite, then for any $g \in G$, $|gH| = |H|$.*

Left multiplication is a bijection.

Proof. Suffices to show $f : H \to gH$, defined by $f(x) = gx$ is a bijection. Surjection is clear by definition of gH. If $gh_1 = gh_2$, then $g^{-1} g h_1 = g^{-1} g h_2$, so $h_1 = h_2$ and f is injective. ☐

Theorem (Lagrange's Theorem)**.** *If G is a finite group and $H \leq G$, then*

$$|G| = |G : H||H|$$

Cosets form a partition, all partitions are the same size.

Proof. From the above, G can be written as the union of disjoint cosets, all of the same size. So

$$|G| = \text{number of cosets} \times |H| = |G : H||H|$$

. □

Corollary. *For any $H \leq G$, $|H| \mid |G|$.*

Corollary. *For any $g \in G$, $\text{ord}(g) \mid |G|$.*

Corollary. *For any $g \in G$, $g^{|G|} = e$.*

5.3 Fermat-Euler

Definition (Units modulo n)**.** Let

$$\mathbb{Z}_n^* = \{k \in \mathbb{Z}_n : \gcd(n, k) = 1\}$$

Proposition. *$\mathbb{Z}_n^*$ is the set of elements that are invertible under multiplication.*

Proof. See Numbers and Sets. □

Definition (Euler Totient Function)**.**

$$\phi(n) = |\mathbb{Z}_n^*|$$

Theorem (Fermat-Euler)**.** *Let $n \geq 1$, $N \in \mathbb{Z}$ coprime to n. Then*

$$N^{\phi(n)} \equiv 1 \pmod{n}$$

Consider $a = N \mod n \in \mathbb{Z}_n^*$, use Lagrange.

Proof. As N is comprime to n, let $a = N \mod n \in \mathbb{Z}_n^*$. Then $a^{\phi(n)} = a^{|\mathbb{Z}_n^*|} = 1$.

We have that $N = kn + a$, so $N^{\phi(n)} = (a + kn)^{\phi(n)} = a^{\phi(n)} + n(\dots) \equiv 1 \pmod{n}$. □

6 Quotient Groups

6.1 Normal Subgroups

Definition (Normal Subgroup)**.** A subgroup $N \leq G$ is normal if for all $g \in G$, $gN = Ng$. We write $N \trianglelefteq G$.

Theorem. *The following are equivalent.*

(i) $\forall g \in G, gN = Ng$

(ii) $\forall g \in G, \forall n \in N, gng^{-1} \in N$

(iii) $\forall g \in G, N = gNg^{-1}$*, where* $gNg^{-1} = \{gng^{-1} : n \in N\}$.

Proof. We shall first show that (i) $\iff$ (iii).

($\implies$). Given $g \in G$, $n \in N$, $ng \in Ng$, so there exists n' such that $ng = gn'$. Then $n = gn'g^{-1} \in gNg^{-1}$.

($\impliedby$) Given $g \in G$, $n \in N$, $n = g^{-1}n'g$ for some $n' \in N$, and $gn = gg^{-1}n'g = n'g \in Ng$. Also, $n = gn''g^{-1}$ for some $n'' \in N$. So $ng = gn''g^{-1}g = gn'' \in gN$. So $gN = Ng$.

Clearly (iii) $\implies$ (ii), and also that (ii) $\implies$ $\forall g \in G, gNg^{-1} \subseteq N$.

Given $g \in G$, $n \in N$, from (ii), we also have that $g^{-1}ng = n'$ for some $n' \in N$. So $n = gn'g^{-1} \in gNg^{-1}$. □

Proposition. *Any subgroup of an abelian group is normal.*

Proof. $gng^{-1} = gg^{-1}n = n \in N$. ☐

Proposition. *Any index 2 subgroup is normal.*

The cosets are N and $G \backslash N$

Proof. The left and right cosets must be $N = eN = Ne$ and $G \backslash N$. So the left and right cosets of N are equal. ☐

Proposition. *For any homomorphism $\varphi : G \to H$,*

$$\ker \varphi \trianglelefteq G$$

Proof. Given $k \in \ker \varphi$, $g \in G$, $\varphi(gkg^{-1}) = \varphi(g)\varphi(k)\varphi(g)^{-1} = \varphi(g)\varphi(g)^{-1} = e$, so $gkg^{-1} \in \ker \varphi$. ☐

6.2 Simple Groups

Definition (Simple group)**.** A group G is simple if the only normal subgroups of G are G and $\{e\}$.

6.3 Quotients

Definition (Quotient Group)**.** Let $N \trianglelefteq G$. Then we denote by G/N the quotient group of G by N. This is defined with the operation

$$(g_1 N)(g_2 N) = g_1 g_2 N$$

for $g_1, g_2 \in G$.

Proposition. *The Quotient Group is a group.*

Show that the definition of multiplication in G/N is independent of the choice of coset representative. Group properties are inherited from G.

Proof. First we need to show that the group operation is independent of the choice of g_1, g_2. Suppose $g_1 N = g_1' N$ and $g_2 N = g_2' N$. Then we need to show that $(g_1 N)(g_2 N) = g_1 g_2 N = g_1' g_2' N = (g_1' N)(g_2' N)$.

$g_1 N = g_1' N$ means that $g_1^{-1} g_1' \in N$, and similarly we have that $g_2^{-1} g_2' \in N$. So $g_1' = g_1 n_1$ and $g_2' = g_2 n_2$. Then $g_1' g_2' N = g_1 n_1 g_2 n_2 N = g_1 n_1 g_2 N$. So we need to show that $n_1 g_2 N = g_2 N$, ie $g_2^{-1} n_1 g_2 \in N$. As $N \trianglelefteq G$ this is satisfied.

The group properties are clear, and inherited from G. ☐

Definition (Quotient map)**.** Given $N \trianglelefteq G$, the quotient map $\pi : G \to G/N$ is defined by $\pi(g) = gN$.

Theorem. *π is a surjective homomorphism.*

Proof. $\pi(gh) = ghN = (gN)(hN) = \pi(g)\pi(h)$ so π is a homomorphism. Surjectivity is clear. ☐

Theorem. $\ker \pi = N$.

Proof. $\pi(g) = N \iff gN = N \iff g \in N$. ☐

6.4 Isomorphism Theorems

Theorem (First Isomorphism Theorem)**.** *Let $\varphi : G \to H$ be a homomorphism. Then*

$$G/\ker\varphi \cong \operatorname{Im}\varphi$$

$\psi(g\ker\varphi) = \varphi(g)$ *is the isomorphism.*

Proof. Define $\psi : G/\ker\varphi \to \operatorname{Im}\varphi$ by $\psi(g\ker\varphi) = \varphi(g)$. First we need to show that ψ is well defined. If $g_1\ker\varphi = g_2\ker\varphi$, then $g_1 = g_2k$ for some $k \in \ker\varphi$. So $\psi(g_1\ker\varphi) = \varphi(g_1) = \varphi(g_2k) = \varphi(g_2)\varphi(k) = \varphi(g_2) = \psi(g_2\ker\varphi)$.

Now, $\psi((g_1\ker\varphi)(g_2\ker\varphi)) = \psi(g_1g_2\ker\varphi) = \varphi(g_1g_2) = \varphi(g_1)\varphi(g_2) = \psi(g_1\ker\varphi)\psi(g_2\ker\varphi)$, so ψ is a homomorphism.

Now suppose if $\psi(g_1\ker\varphi) = e$, then $\phi(g_1) = e$, so $g_1 \in \ker\varphi$, and $g_1\ker\varphi = \ker\varphi$. So $\ker\psi = \{\ker\varphi\}$.

Surjectivity is clear, so ψ defines an isomorphism. □

Theorem (Correspondence Theorem)**.** *Let $N \trianglelefteq G$, then there is a bijection between the subgroups of G/N and the subgroups of G containing N.*

Consider preimage under quotient map

Proof. Given $N \leq M \leq G$, $N \trianglelefteq G$, then clearly $N \trianglelefteq M$, and clearly $M/N \leq G/N$.

Conversely, given $H \leq G/N$, we can take the preimage of H under the quotient map, $\pi^{-1}(H) = \{g \in G : gN \in H\}$, and this is a subgroup of G. Clearly $e \in \pi^{-1}(H)$. If $g, h \in \pi^{-1}(H)$, then $gN, hN \in H$. So $(gh^{-1})N = (gN)(hN)^{-1} \in H$, and $gh^{-1} \in \pi^{-1}(H)$. Also, if $g \in N$, then $gN = N$ and $g \in \pi^{-1}(H)$.

The first part defines a map from subgroups of G containing N to subgroups of G/N, and the second part defines a map from subgroups of G/N to subgroups of G containing N.

We can then check that $\pi(\pi^{-1}(M/N)) = M$ and $\pi^{-1}(H)/N = H$. □

Theorem (Second Isomorphism Theorem)**.** *Let $H \leq G$ and $N \trianglelefteq G$. Then $H \cap N \trianglelefteq H$ and $H/(H \cap N) \cong HN/N$.*

Proof. As $N \trianglelefteq G$, $HN = \{hn : h \in H, n \in N\}$ is a subgroup of G. Define $\varphi : H \to HN/N$ by $\varphi(h) = hN$. $\ker\varphi = H \cap N$, and result follows from the First Isomorphism Theorem. □

Theorem (Third Isomorphism Theorem)**.** *Let $N \leq M \leq G$, $N \trianglelefteq G$, $M \trianglelefteq G$. Then $M/N \triangleleft G/N$ and $(G/N)/(M/N) \cong G/M$.*

Proof. Define $\varphi : G/N \to G/M$ by $\varphi(gN) = gM$. This is well defined as $N \leq M$, and we note that φ is a surjective homomorphism. If $\varphi(gN) = gM = M$, then $g \in M$, so $\ker\varphi = M/N$. Result follows from First Isomorphism Theorem. □

7 Group actions

Definition (Group Action)**.** Let G be a group, X be a set, an action of G on X is a function $\alpha : G \times X \to X$. We write $\alpha_g(x) = \alpha(g, x)$ or just $g(x)$ if it is clear. α satisfies

- $\forall g \in G, \forall x \in X$, $\alpha_g(x) \in X$.
- $\forall x \in X$, $\alpha_e(x) = x$.
- $\forall g, h \in G, \forall x \in X$, $\alpha_{gh}(x) = \alpha_g(\alpha_h(x))$

We write $G \circlearrowleft X$ if G acts on X.

Lemma. *For all $g \in G$, $\alpha_g : X \to X$ is a bijection.*

Two sided inverse means it's bijective.

Proof. $\alpha_{g^{-1}}(\alpha_g(x)) = \alpha_{g^{-1}g}(x) = \alpha_e(x) = x$ and $\alpha_g(\alpha_{g^{-1}}(x)) = \alpha_{gg^{-1}}(x) = \alpha_e(x) = x$. So it has a two sided inverse and is bijective. $\square$

Proposition. *Let G be a group, X be a set. $\alpha : G \times X \to X$ is an action if and only if $\rho : G \to \mathrm{Sym}(X)$ defined by $\rho(g) = \alpha_g$ is a homomorphism.*

$(\rho(g))(x) = \alpha_g(x)$, check definitions.

Proof. ($\implies$). From lemma above, $\alpha_g \in \mathrm{Sym}(X)$. In addition, $\rho(gh) = \alpha_{gh} = \alpha_g \alpha_h = \rho(g)\rho(h)$, so ρ is a homomorphism.

($\impliedby$). Suppose ρ is a homomorphism. Define $\alpha_g(x) = (\rho(g))(x)$. Since $\rho(g) \in \mathrm{Sym}(X)$, $\alpha_g(x) \in X$. $\rho(e) = \mathrm{id}$, so $\alpha_e(x) = \mathrm{id}(x) = x$. $\rho(gh) = \rho(g)\rho(h)$, so $\alpha_g(\alpha_h(x)) = \alpha_{gh}(x)$. $\square$

Definition (Kernel of Action)**.** The kernel of an action α is the kernel of the corresponding homomorphism $\rho : G \to \mathrm{Sym}(X)$.

Definition (Faithful)**.** An action α is faithful if $\ker \rho = \{e\}$.

7.1 Orbit-Stabiliser

Definition (Orbit)**.** Let $G \circlearrowleft X$, the orbit of $x \in X$ is

$$\mathrm{Orb}(x) = \{g(x) : g \in G\} \subseteq X$$

Definition (Stabiliser)**.** Let $G \circlearrowleft X$, the stabiliser of $x \in X$ is

$$\mathrm{Stab}(x) = \{g \in G : g(x) = x\} \subseteq G$$

Definition (Transitive)**.** An action is transitive if $\mathrm{Orb}(x) = X$ for all $x \in X$.

Lemma. *For all $x \in X$, $\mathrm{Stab}(x) \leq G$.*

Proof. $e \in \mathrm{Stab}(x)$ as $e(x) = x$. For $g, h \in \mathrm{Stab}(x)$, $gh^{-1}(x) = gh^{-1}(h(x)) = gh^{-1}h(x) = g(x) = x$, so $gh^{-1} \in \mathrm{Stab}(x)$. By the fast subgroup check, $\mathrm{Stab}(x) \leq G$. $\square$

Lemma. *Let $G \circlearrowleft X$, the orbits of $x \in X$ partition X.*

Consider the intersection of the orbits

Proof. For $x \in X, x \in \mathrm{Orb}(x)$, so $X = \bigcup_{x \in X} \mathrm{Orb}(x)$.

Now suppose if $z \in \mathrm{Orb}(x) \cap \mathrm{Orb}(y)$. Then for some $g, h \in G$, we have that $g(x) = z$ and $h(y) = z$. For any $t \in \mathrm{Orb}(y)$, $t = k(y) = kh^{-1}(z) = kh^{-1}g(x)$. So $t \in \mathrm{Orb}(x)$, and $\mathrm{Orb}(y) \subseteq \mathrm{Orb}(x)$, and symmetrically, $\mathrm{Orb}(x) \subseteq \mathrm{Orb}(y)$. Thus $\mathrm{Orb}(x) = \mathrm{Orb}(y)$, and orbits partition. $\square$

Theorem (Orbit-Stabiliser)**.** *Let G be a finite group, $G \circlearrowleft X$, then for all $x \in X$,*

$$|G| = |\mathrm{Orb}(x)||\mathrm{Stab}(x)|$$

$h(x) = g(x) \iff hg^{-1} \in \mathrm{Stab}(x) \iff h\,\mathrm{Stab}(x) = g\,\mathrm{Stab}(x)$, so $|\mathrm{Orb}(x)| = |G : \mathrm{Stab}(x)|$.

Proof. First, we note that $\mathrm{Orb}(x)$ must be finite as G is finite.

Also, $h(x) = g(x) \iff h^{-1}g(x) = x \iff h^{-1}g \in \mathrm{Stab}(x)$. So this means that $h\,\mathrm{Stab}(x) = g\,\mathrm{Stab}(x)$. So distinct points in $\mathrm{Orb}(x)$ are in bijection with distinct cosets of $\mathrm{Stab}(x)$. Thus $|\mathrm{Orb}(x)| = |G : \mathrm{Stab}(x)| = |G|/|Stab(x)|$ and result follows. $\square$

Lemma (Burnside's Lemma)**.** *Let* $\mathrm{Fix}(g) = \{x \in X : g(x) = x\}$*. Then the number of orbits is*

$$\frac{1}{|G|}\sum_{g\in G}|\mathrm{Fix}(g)|$$

Count $\{(g, x) : g(x) = x\}$ *by summing over* x*, then summing over* g*, orbits partition*

Proof. Let $S = \{(g, x) : g(x) = x\}$. Then

$$S = \bigcup_{g\in G}\{g\} \times \mathrm{Fix}(g) = \bigcup_{x\in X}\mathrm{Stab}(x) \times \{x\}$$

So $|S| = \sum_{g\in G}|\mathrm{Fix}(g)| = \sum_{x\in X}|\mathrm{Stab}(x)| = |G|\sum_{x\in X}\frac{1}{\mathrm{Orb}(x)}$.
As orbits partition, let $O_1, \dots, O_m$ be the orbits. Then

$$\sum_{x\in X}\frac{1}{\mathrm{Orb}(x)} = \sum_{k=1}^{m}\sum_{x\in O_k}\frac{1}{|O_k|} = m$$

□

7.2 Cauchy's Theorem

Theorem. *If* G *is a finite group,* p *a prime, and* $p \mid |G|$*, then* G *has an element of order* p*.*

Consider $X = \{(g_1, \dots, g_p) : g_1 \dots g_p = e\} \subseteq G^p$*.* $\mathrm{ord}(g) \mid p \iff (g, \dots, g) \in X$*.* $p \mid |X|$ *as* $p \mid |G|^{p-1}$*. Let* C_p *act on* X *by 'cycling'. By Orbit Stabiliser sizes of orbits are 1 or p. There must be at least* $p - 1$ *size 1 orbits as* $(e, \dots, e) \in X$*.*

Proof. Consider the group G^p. Let $X \subseteq G^p$ be defined by $X = \{(g_1, \dots, g_p) : g_1 \dots g_p = e\}$. Note that $\mathrm{ord}(g) \mid p \iff (g, \dots, g) \in X$. Now define an action $\alpha : C_p \times X \to X$. Let $C_p = \langle a\rangle$. Then $a(g_1, \dots, g_p) = (g_2, \dots, g_n, g_1)$. If $g_1 \dots g_p = e$ then $g_2 \dots g_n g_1 = g_1^{-1}g_1 \dots g_n g_1 = g_1^{-1}eg_1 = e$.

Now, we know that $|X| = |G|^{p-1}$, as for each element of X, $(g_1, \dots, g_{p-1}, g_p)$, $g_1, \dots, g_{p-1}$ are arbitrary, and then g_p is unique. Thus we know that $p \mid |X|$.

By Orbit-Stabiliser, we have that for any $x \in X$, $|\mathrm{Orb}(x)||\mathrm{Stab}(x)| = \left|C_p\right| = p$. This means that the sizes of orbits must be 1 or p. As orbits partition, we have that

$$|X| = (\text{number of size 1 orbits}) + p \times (\text{number of size } p \text{ orbits})$$

Thus, the number of size 1 orbits must be a multiple of p. As $\mathrm{Orb}((e, \dots, e)) = (e, \dots, e)$, there must in fact be at least $p - 1$ more. Orbits of size 1 are of the form $(g, \dots, g)$, so we must have some $g \in G$. $g \neq e$ such that $g^p = e$. □

7.3 Left regular action

Definition (Left regular action)**.** A group G acts on itself by $g(x) = gx$.

Theorem. *Left regular action is an action.*

Proof. Clear from definition and group axioms. □

Lemma. *The left regular action is faithful.*

Proof. If $g(x) = gx = x$ for all $x \in G$, then $ge = e$, so $g = e$. □

Lemma. *The left regular action is transitive.*

Proof. Given $x, y \in G$, setting $g = yx^{-1}$, $g(x) = yx^{-1}x = y$. □

Theorem (Cayley's Theorem)**.** *Every group is isomorphic to a subgroup of a symmetric group.*

Left regular action is faithful, First Isomorphism Theorem

Proof. Let $G \circlearrowleft G$ by the left regular action. This gives us a homomorphism $\rho : G \to \mathrm{Sym}(G)$, and as $\ker \rho = \{e\}$, from the First Isomorphism Theorem, we get that

$$G \cong G/\ker \rho \cong \mathrm{Im}\, \rho \leq \mathrm{Sym}(G)$$

□

Proposition. *A group G acts on it's subgroups by $g(H) = gH$, and this action is transitive.*

Proof. Clear from definitions. □

7.4 Conjugation Action

Definition (Conjugate)**.** Given $g, h \in G$, the conjugate of g by h is hgh^{-1}.

Proposition. *$G \circlearrowleft G$ by conjugation, that is $g(x) = gxg^{-1}$.*

Proof. Clear from definitions. □

Proposition. $\mathrm{ord}(ghg^{-1}) = \mathrm{ord}(h)$

Proof. $(ghg^{-1})^n = gh^ng^{-1}$, so $(ghg^{-1})^n = e \iff h^n = e$. □

Definition (Centre)**.** The centre of a group $Z(G)$ is the kernel of the conjugation action.

$$Z(G) = \{g \in G : \forall h \in G, ghg^{-1} = h\}$$

The centre is the set of elements of G that commute with all the others, as $gh = hg$.

Definition (Conjugacy Class)**.** The conjugacy class of an element $x \in G$ is the orbit of x under the conjugation action.

$$\mathrm{ccl}_G(x) = \{gxg^{-1} : g \in G\}$$

Definition (Centraliser)**.** The centraliser of an element $x \in G$ is the stabiliser of x under the conjugation action.

$$C_G(x) = \{g \in G : gxg^{-1} = x\}$$

The centraliser of x is the set of elements of G which commute with x.

Proposition.

$$Z(G) = \bigcup_{g \in G} C_G(g)$$

Proof. Consider $\subseteq$ and $\supseteq$. □

Theorem. *If G is a finite abelian group, acting on a finite set X, and the action is transitive and faithful, then $|G| = |X|$.*

Proof. Let $x \in X$ be arbitrary. Consider $g \in \mathrm{Stab}(x)$. Let $y \in X$ be arbitrary. Then as $\mathrm{Orb}(y) = X$, there exists h such that $h(x) = y$. Then $g(y) = gh(x) = hg(x) = h(x) = y$. As the action is faithful, $g = e$. So $|\mathrm{Stab}(x)| = 1$, $|\mathrm{Orb}(x)| = |X|$. □

Proposition. *G acts on its subgroups by $g(H) = gHg^{-1}$.*

Proof. Clear from definitions. □

Proposition.

$$gHg^{-1} \cong H$$

Proposition. *Singleton orbits are normal subgroups.*

Proof. N is normal if and only if $\forall g, gNg^{-1} = N$. □

Lemma. *Normal subgroups are those that are a union of conjugacy classes.*

Proof. $N = \bigcup_{h \in N} \mathrm{ccl}_G(h)$, as we clearly have that $\forall h \in N, \mathrm{ccl}_G(h) \subseteq N$.

Conversely, if H is a union of conjugacy classes, then given $g \in G, h \in H$, $ghg^{-1} \in \mathrm{ccl}_G(h) \subseteq H$. So H is normal. □

8 Small Groups

8.1 Order 1

The only group of order 1 is the trivial group.

8.2 Prime order

Proposition. *If $|G| = p$ with p prime, then $G \cong C_p$.*

Proof. By Lagrange, the elements in G must have order dividing p, but as p is prime, the order of any non-identity element must be p. This means that it generates the group. □

8.3 Order 4

Lemma. *All groups of order ≤ 5 are abelian.*

Consider $\{e, x, y, xy, yx\}$, two of them must be equal.

Proof. Orders $1, 2, 3$ and 5 are trivial. Consider a group G with $|G| = 4$. Choose distinct non-identity $x, y \in G$.

Consider the set $\{e, x, y, xy, yx\}$. We must have that (at least) two of the elements there are equal. If $x = xy$ or $x = yx$, then $y = e$. Contradiction. If $y = xy$ or $y = yx$ then $x = e$. Contradiction. Thus we must have that $xy = yx$, and $xy \neq x$, $xy \neq y$. So the group is $\{e, x, y, xy\}$ and is abelian as $xy = yx$. □

Proposition. *The only groups of order 4 are C_4 and $V_4 = C_2 \times C_2$.*

Cases on whether there is an element of order 4.

Proof. If there exists an element of order 4, then it generates the group and the group is cyclic.

Otherwise, by Lagrange's Theorem, all the non-identity elements must have order 2. Choose 2 distinct elements of order 2, say b and c. From proof above, we have that $G = \{e, b, c, bc\}$. By the direct product theorem, this is isomorphic to $\langle b \rangle \times \langle c \rangle \cong C_2 \times C_2$. □

8.4 Order 6

Proposition. *The only groups of order* 6 *are* C_6 *and* D_6 *(*$\cong S_3$*).*

By Cauchy there are elements of order 2 and 3. Cases on whether there is an element of order 6.
$D_6 = \langle r, s \mid r^3 = s^2 = e, srs = r^{-1} \rangle$

Proof. By Lagrange's Theorem, the possible orders of elements are $1, 2, 3, 6$.

If there is an element g of order 6, then we are done, as $G = \langle g \rangle \cong C_6$.

By Cauchy's Theorem, we must have an element s of order 2, and an element r of order 3. $|G : \langle r \rangle| = 2$, so $\langle r \rangle$ is a normal subgroup of G. This means that $s^{-1}rs \in \langle r \rangle = \{e, r, r^2\}$. We can check each case separately.

If $s^{-1}rs = e$, then $r = e$. Contradiction.

If $s^{-1}rs = r$, then $sr = rs$, so $(sr)^n = s^n r^n$, and sr would have order 6, as $\mathrm{lcm}(2, 3) = 6$. Contradiction.

Thus $s^{-1}rs = r^2 = r^{-1}$, and $G = \langle s, r \rangle$, with $sr = r^{-1}s$, $s^2 = r^3 = e$. So $G \cong D_6$. □

8.5 Order 8

Lemma. *If all non-identity elements of a finite group have order* 2*, then it is abelian.*

Proof. Let $a, b \in G$ be arbitrary. Then $\mathrm{ord}(ab) \leq 2$. So $ab = (ab)^{-1}$. Thus $ab = a^{-1}b^{-1} = (ba)^{-1} = ba$. □

Lemma. *If all non-identity elements of a finite group have order* 2*, then it must be isomorphic to* $C^2 \times \ldots \times C^2$.

By Cauchy we know the size is 2^n*, choose elements, look at generated subgroups and use direct product theorem.*

Proof. By Cauchy's Theorem we know that the size of G must be 2^n for some n and from the lemma above we know that G is abelian.

If $|G| = 2$, then $G \cong C_2$ and we are done.

If $|G| > 2$, then choose $a_1 \in G$, $\mathrm{ord}(a_1) = 2$. There must be some $a_2 \in G$ such that $a_2 \notin \langle a_1 \rangle$. By the Direct Product Theorem, $\langle a_1, a_2 \rangle \cong \langle a_1 \rangle \times \langle a_2 \rangle \cong C_2 \times C_2$. If $|G| = 4$ then we are done. If not, choose $a_3 \notin \langle a_1, a_2 \rangle$ anf so on.

Continue until we get $G \cong \underbrace{C_2 \times \cdots \times C_2}_{n\text{copies}}$. □

Lemma. *Let* G *be a group, and* N *be a normal subgroup of index* m *in* G*. Then for any* $g \in G$, $g^m \in N$.

Lagrange on G/N

Proof. Let $g \in G$ be arbitrary. Consider $gN \in G/N$. By Lagrange we have that $(gN)^m = g^m N = N$. So $g^m \in N$. □

Proposition. *A group of order* 8 *is isomorphic to one of the following*

- C_8
- $C_4 \times C_2$
- $C_2 \times C_2 \times C_2$
- D_8
- Q_8

Order 8 $\implies C_8$. All order 2 $\implies C_2^3$. Otherwise there exists h with $\text{ord}(h) = 4$. $\langle h \rangle \trianglelefteq G$, so $g^2 \in \langle h \rangle$ for all g. $g^2 = e, h, h^2$ or h^3. Can't be h or h^3. For each case consider $ghg^{-1} = h$ or h^3.

Proof. First we check that they are not isomorphic. $C_8, C_4 \times C_2, C_2 \times C_2 \times C_2$ are abelian, D_8 and Q_8 are not. By looking at elements of order $2, 4$ and 8, the abelian groups are not isomorphic. D_8 has 5 elements of order 2, but Q_8 has only 1.

By Lagrange, the orders of elements of the group are 1, 2, 4 and 8.

- If we have an element of order 8, then $G \cong C_8$.
- If all non-identity elements have order 2, then $C \cong C_2 \times C_2 \times C_2$.
- Otherwise, we must have no elements of order 8, and at least one element h of order 4. Note that $\langle h \rangle$ is an index 2, and thus normal subgroup of G. From the lemma above, $g^2 \in \langle h \rangle$ for any $g \in G$. So $g^2 = e, h, h^2$ or h^3.

  If $g^2 = h$ or h^3, then $g^4 = h^2 \neq e$, and this means that $\text{ord}(g) = 8$. Contradiction. So we must have that $g^2 = e$ or h^2.

  - If $g^2 = e$, now consider ghg^{-1}. As $\langle h \rangle \trianglelefteq G$, we must have that $ghg^{-1} \in \langle h \rangle$. In addition, $\text{ord}(ghg^{-1}) = 4$, so $ghg^{-1} = h$ or h^3.
    * If $ghg^{-1} = h$, then $gh = hg$, $\langle h \rangle \cap \langle g \rangle = \{e\}$, and $G = \langle h \rangle \langle g \rangle$. So $G \cong \langle h \rangle \times \langle g \rangle \cong C_4 \times C_2$.
    * If $ghg^{-1} = h^3 = h^{-1}$, then $G \cong Q_8$ by mapping $h \mapsto r$ and $g \mapsto s$.
  - If $g^2 = h^2$, we still have that $ghg^{-1} = h$ or h^3.
    * If $ghg^{-1} = h$, then $(gh)^2 = ghgh = g^2h^2 = e$ has order 2. Applying the Direct Product Theorem to $\langle h \rangle \times \langle gh \rangle$ yields the desired result.
    * If $ghg^{-1} = h^3$, then define $\phi : G \to Q_8$ by $e \mapsto 1$, $h \mapsto i$, $g \mapsto j$, $gh^3 \mapsto k$.

$\square$

9 Möbius Group

Definition (Extended Complex Plane)**.** The extended complex plane $\hat{\mathbb{C}}$ is the complex plane with a point at infinity. Equivalently, $\hat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$.

Definition (Möbius Map)**.** A Möbius map is a function $f : \hat{\mathbb{C}} \to \hat{\mathbb{C}}$ of the form

$$f(z) = \frac{az + b}{cz + d}$$

where $a, b, c, d \in \mathbb{C}$, $ad - bc \neq 0$, $f(-d/c) = \infty$ and

$$f(\infty) = \begin{cases} \dfrac{a}{c} & \text{if } c \neq 0 \\ \infty & \text{if c} = 0 \end{cases}$$

Lemma. *Möbius maps are bijections.*

Proof. We claim that

$$f^{-1}(z) = \frac{dz - b}{-cz + a}$$

For $z \neq a/c, \infty$,

$$
\begin{aligned}
f(f^{-1}(z)) &= \frac{a\left(\dfrac{dz-b}{-cz+a}\right)+b}{c\left(\dfrac{dz-b}{-cz+a}\right)+d} \\
&= \frac{a(dz-b)+b(-cz+a)}{c(dz-b)+d(-cz+a)} \\
&= \frac{(ad-bc)z}{(ad-bc)} \\
&= z
\end{aligned}
$$

We also have that $f(f^{-1}(a/c)) = f(\infty) = a/c$ and $f(f^{-1}(\infty)) = f(-d/c) = \infty$. Thus $f \circ f^{-1} = \mathrm{id}$. We also have that $f^{-1} \circ f = \mathrm{id}$. □

Theorem (Möbius Group)**.** *The set $\mathcal{M}$ of Möbius maps forms a group under composition.*

Proof. Closure - Algebra bash. Check composition of Möbius maps is a Möbius map, that is, '$ad - bc \neq 0$' and also check that the values for $-d/c$ and ∞ match.

Identity - $\mathrm{id} : z \mapsto z$.

Inverse - From lemma above.

Associativity - Function composition is always associative. □

Proposition. *The Möbius group is generated by the following*

(i) $f(z) = az$ *($a \neq 0$)*

(ii) $f(z) = z + b$

(iii) $f(z) = 1/z$

Proof. If $c \neq 0$, then

$$
z \overset{(i)}{\longmapsto} z + \frac{d}{c} \overset{(iii)}{\longmapsto} \frac{1}{z + \frac{d}{c}} \overset{(i)}{\longmapsto} \frac{(ad-bc)c^{-2}}{z + \frac{d}{c}} \overset{(ii)}{\longmapsto} \frac{a}{c} + \frac{(ad-bc)c^{-2}}{z + \frac{d}{c}} = \frac{az+b}{cz+d}
$$

If $c = 0$, then

$$
z \overset{(i)}{\longmapsto} \frac{a}{d}z \overset{(ii)}{\longmapsto} \frac{a}{d}z + \frac{b}{d} = \frac{az+b}{d}
$$

□

Proposition. *The Möbius group acts on $\hat{\mathbb{C}}$.*

Proposition. *The action $\mathcal{M} \circlearrowleft \hat{\mathbb{C}}$ is faithful.*

Proof. Consider $\rho : \mathcal{M} \to \mathrm{Sym}(\hat{\mathbb{C}})$, defined by $(\rho(f))(z) = f(z)$. Then if $\rho(f) = \mathrm{id}$, we must then have that $f = \mathrm{id}$. □

9.1 Fixed Points

Definition (Fixed Point)**.** A fixed point of $f \in \mathcal{M}$ is $z \in \hat{\mathbb{C}}$ such that $f(z) = z$.

Proposition. *A Möbius map with at least 3 fixed points is the identity.*

Fundamental Theorem of Algebra.

Proof. Suppose $f(z) = \dfrac{az+b}{cz+d}$ has at least 3 fixed points. First suppose if ∞ is not a fixed point. Then $\dfrac{az+b}{cz+d} = z$ has three roots over $\mathbb{C}$, ie $cz^2 + (d-a)z + b = 0$ has 3 roots. Contradiction by FTA. So we must have that $c = d - a = b = 0$.

Now suppose if ∞ is a fixed point, then $f(\infty) = \infty$, so $c = 0$. Consequently $f(z) = \dfrac{az+b}{d} = z$ has two roots, ie $(a-d)z + b = 0$ has at least two roots. Contradiction by FTA, so $a - d = b = 0$.

In either case, $c = b = 0$, $a = d$ means that $f(z) = z$. ☐

Corollary. *If $f, g \in \mathcal{M}$ coincide at three points, then they are equal.*

$$fg^{-1} = \mathrm{id}.$$

Proof. Say $z_1, z_2, z_3 \in \hat{\mathbb{C}}$ are such that $f(z_1) = g(z_1)$, $f(z_2) = g(z_2)$, $f(z_3) = g(z_3)$. Then $g^{-1}f(z_i) = z_i$ for $i = 1, 2, 3$. So $g^{-1}f = \mathrm{id}$, and $f = g$. ☐

Theorem. *There is a unique Möbius map sending any three disjoint points of $\hat{\mathbb{C}}$ to any three distinct points in $\hat{\mathbb{C}}$.*

Map each triple to $(0, 1, \infty)$. Take $g^{-1}f$.

Proof. Suppose first that $f : (z_1, z_2, z_3) \mapsto (0, 1, \infty)$. If $z_1, z_2, z_3 \neq \infty$, then

$$f(z) = \frac{(z_2 - z_3)(z - z_1)}{(z_2 - z_1)(z - z_3)}$$

satisfies the requirements. If $z_1 = \infty$, then $f(z) = \dfrac{z_2 - z_3}{z_2 - z_1}$. If $z_2 = \infty$, then $f(z) = \dfrac{z - z_1}{z - z_3}$. If $z_3 = \infty$, then $f(z) = \dfrac{z - z_1}{z_2 - z_1}$.

Now suppose $f_1 : (z_1, z_2, z_3) \mapsto (0, 1, \infty)$, $f_2 : (w_1, w_2, w_3) \mapsto (0, 1, \infty)$. Then $f = f_2^{-1}f : (z_1, z_2, z_3) \mapsto (w_1, w_2, w_3)$. ☐

Lemma. *Every Möbius map has at least 1 fixed point.*

Fundamental Theorem of Algebra

Proof. $f(z) = \dfrac{az+b}{cz+d} = z \iff cz^2 + (d-a)z - b = 0$ has at least one root over $\mathbb{C}$. ☐

9.1.1 Conjugation and Iteration

Lemma. *f fixes z if and only if hfh^{-1} fixes $h(z)$.*

Lemma. *If $f \in \mathcal{M}$ has 1 fixed point, then it is conjugate to $z \mapsto z + 1$.*

$(z_1, f(z_1), z_0)$ distinct. Conjugate f by map of $(z_1, f(z_1), z_0)$ to $(0, 1, \infty)$. So f is conjugate to a map that fixes ∞ and maps 0 to 1.

Proof. Suppose $f(z_0) = z_0$. Choose $z_1 \neq z_0$. Then $(z_1, f(z_1), z_0)$ are three distinct points. So we have $g \in \mathcal{M}$ such that $g : (z_1, f(z_1), z_0) \mapsto (0, 1, \infty)$. Under gfg^{-1}, we have that $0 \mapsto z_1 \mapsto f(z_1) \mapsto 1$, and $\infty \mapsto z_0 \mapsto z_0 \mapsto \infty$. So ∞ is the fixed point of hfh^{-1}, and 0 is mapped to 1. As a result, we must have that $f(z) = az + 1$ for some $a \in \mathbb{C}$, $a \neq 0$. If $a \neq 1$, then $1/(1-a)$ is also a fixed point. So we must have that $a = 1$, and $gfg^{-1}(z) = z + 1$. ☐

Lemma. *If $f \in \mathcal{M}$ has 2 fixed points, then it is conjugate to $z \mapsto az$, $a \in \mathbb{C}$, $a \neq 0$.*

Conjugate by map of (z_0, z_1) to $(0, \infty)$. Then 0 and ∞ are fixed.

Proof. Say z_0, z_1 are fixed points of f. Let g be any Möbius map such that $(z_0, z_1) \mapsto (0, \infty)$. Then gfg^{-1} fixes 0 and ∞. So it must have the form $z \mapsto az$ for some $a \neq 0$. ☐

9.2 Complex Geometry

Definition (Circle)**.** A circle in $\hat{\mathbb{C}}$ is the set of $z \in \hat{\mathbb{C}}$ satisfying

$$Azz^* + B^*z + Bz^* + C = 0$$

where $A, C \in \mathbb{R}$, $B \in \mathbb{C}$, $|B|^2 > AC$.

Proposition. *∞ is in a circle if and only if $A = 0$.*

Proposition. *All circles on $\hat{\mathbb{C}}$ are either circles or lines in $\mathbb{C}$.*

Theorem. *Circles are preserved by Möbius maps.*

Proof. Let $S(A, B, C) = \{z : Azz^* + B^*z + Bz^* + C = 0\}$. We know that $\mathcal{M}$ is generated by $z \mapsto az$, $z \mapsto z + b$ and $z \mapsto 1/z$, and we only need to check these cases.

Under $z \mapsto az$, $S(A, B, C) \mapsto S\left(\frac{A}{aa^*}, \frac{B}{a^*}, C\right)$.

Under $z \mapsto z + b$, $S(A, B, C) \mapsto S(A, B - Ab, C + Abb^* - Bb^* - B^*b)$

Under $z \mapsto 1/z$, $S(A, B, C) \mapsto S(C, B^*, A)$. ☐

Definition (Cross Ratio)**.** If z_1, z_2, z_3, z_4 are distinct points in $\hat{\mathbb{C}}$, the cross ratio is

$$[z_1, z_2, z_3, z_4] = f(z_4)$$

where f is the unique Möbius map sending $(z_1, z_2, z_3) \mapsto (0, 1, \infty)$.

Proposition. *$[0, 1, \infty, w] = w$ for all $w \in \hat{\mathbb{C}} \backslash \{0, 1, \infty\}$.*

Proposition.

$$[z_1, z_2, z_3, z_4] = \frac{(z_4 - z_1)(z_2 - z_3)}{(z_2 - z_1)(z_4 - z_3)}$$

Proposition.

$$[\infty, z_2, z_3, z_4] = \frac{z_2 - z_3}{z_4 - z_3}$$

Proposition.

$$[z_1, z_2, z_3, z_4] = [z_2, z_1, z_4, z_3] = [z_3, z_4, z_2, z_1] = [z_4, z_3, z_2, z_1]$$

Theorem. *For any $g \in \mathcal{M}$,*

$$[z_1, z_2, z_3, z_4] = [g(z_1), g(z_2), g(z_3), g(z_4)]$$

Proof. Let f be the unique Möbius map $f : (z_1, z_2, z_3) \mapsto (0, 1, \infty)$. Then $[z_1, z_2, z_3, z_4] = f(z_4)$ by definition. Now $fg^{-1} : (g(z_1), g(z_2, g(z_3))) \mapsto (0, 1, \infty)$, so $[g(z_1), g(z_2), g(z_3), g(z_4)] = fg^{-1}(g(z_4)) = f(z_4) = [z_1, z_2, z_3, z_4]$. ☐

Corollary. *Four distince points $z_1, z_2, z_3, z_4 \in \hat{\mathbb{C}}$ are on a circle if and only if $[z_1, z_2, z_3, z_4] \in \mathbb{R}$.*

Proof. Let f be the unique Möbius map $f : (z_1, z_2, z_3) \mapsto (0, 1, \infty)$. Then the circle passing through z_1, z_2, z_3 is sent to the circle passing through $0, 1, \infty$ by f, ie $\mathbb{R} \cup \{\infty\}$. As a result, z_4 is on the circle with (z_1, z_2, z_3) if and only if $f(z_4) \in \mathbb{R}$. ☐

10 Symmetric Groups

Definition (Permutation)**.** Given a set X, a permutation on X is a bijective function $X \to X$. The set of all permutations is denoted by $\mathrm{Sym}(X)$.

Proposition. *$(\mathrm{Sym}(X), \circ)$ is a group.*

Definition (Symmetric Group)**.** If $|X| = n$, then S_n is the isomorphism class of $\mathrm{Sym}(X)$. We typically denote $X = \{1, ..., n\}$

Proposition. *$|S_n| = n!$.*

Proof. For each $\sigma \in S_n$, there is n choices for $\sigma(1)$, $(n - 1)$ for $\sigma(2)$ and so on. ☐

10.1 Disjoint Cycle Representation

Definition (Cycle)**.** A permutation of the form $a_1 \mapsto a_2 \mapsto \cdots \mapsto a_n \mapsto a_1$ is an n-cycle. It is written as $(a_1\ a_2\ \ldots\ a_n)$.

Definition (Transposition)**.** A transposition is a 2-cycle.

Lemma. *Disjoint cycles commute.*

Proof. Let σ and τ be disjoint cycles.

If $i \in \sigma$ and $i \notin \tau$, then $\sigma(i) \notin \tau$ as σ and τ are disjoint. So $\tau(\sigma(i)) = \sigma(i)$, and also $\tau(i) = i$, so $\sigma(\tau(i)) = \sigma(i)$. Similarly if $i \in \tau$ and $i \notin \sigma$, then $\sigma(\tau(i)) = \tau(\sigma(i))$.

If $i \notin \sigma$ and $i \notin \tau$, then $\sigma(i) = \tau(i) = i$, and result follows. □

Theorem (Disjoint Cycle Representation)**.** *Every permutation can be written as a product of disjoint cycles.*

Proof. Consider the sequence $1, \sigma(1), \sigma^2(1), \ldots$. As $\sigma^k(1) \in \{1, \ldots, n\}$, we must have $\sigma^a(1) = \sigma^b(1)$ for some $a > b$. There must be a minimal $k \geq 1$ such that $\sigma^k(1) = 1$. So $1, \sigma(1), \ldots, \sigma^{k-1}(1)$ are all distinct. So $(1\ \sigma(1)\ \ldots\ \sigma^{k-1}(1))$ is the first cycle. Then repeat this for the other numbers in $\{1, \ldots, n\}$ not in the current cycle to get the other cycles. □

Theorem. *Disjoint cycle representation is unique (up to commutativity).*

Proof. Suppose if $\sigma = (a_1\ \ldots\ a_{k_1})(a_{k_1+1}\ \ldots a_{k_2})\ldots(a_{k_{m-1}+1}\ \ldots\ a_{k_m}) = (b_1\ \ldots\ b_{r_1})(b_{r_1+1}\ \ldots b_{r_2})\ldots(b_{r_{s-1}+1}\ \ldots\ b_{r_s})$. We have that $a_1 = b_t$ for some t, and the other numbers in the cycles are determined by $\sigma(a_1), \sigma^2(a_1), \ldots$. As a result, the cycles containing a_1 and b_t are the same. Continue until all cycles are the same. □

10.2 Sign of a Permutation

Theorem. *Every permutation can be written as a product of transpositions.*

Proof. Suffices to show every cycle can be written as a product of transpositions.

$$(a_1\ \ldots\ a_k) = (a_1\ a_2)(a_2\ a_3)\ldots(a_{k-1}\ a_k)$$

□

Theorem. *Let $\sigma \in S_n$. Then the number of transpositions in any representation of σ will always be even, or always off.*

Proof. Define $\#(\sigma)$ for the number of cycles when σ is written as a product of disjoint cycles. Consider $\sigma(cd)$.

If c and d are in the same cycle in σ, say $(c\ a_2\ \ldots\ a_{i-1}\ d\ a_{i+1}\ \ldots\ a_k)$. Then $(c\ a_2\ \ldots\ a_{i-1}\ d\ a_{i+1}\ \ldots\ a_k)(c\ d) = (c\ a_{i+1}\ \ldots\ a_k)(d\ a_2\ \ldots\ a_{i-1})$, so $\#(\sigma(c\ d)) = \#(\sigma) + 1$.

If c and d are in different cycles, then $(c\ a_{i+1}\ \ldots\ a_k)(d\ a_2\ \ldots\ a_{i-1})(c\ d) = (c\ a_2\ \ldots\ a_{i-1}\ d\ a_{i+1}\ \ldots\ a_k)$. Then $(c\ a_2\ \ldots\ a_{i-1}\ d\ a_{i+1}\ \ldots\ a_k)$, so $\#(\sigma(c\ d)) = \#(\sigma) - 1$.

Note that $\#(e) = n$. If σ can be written as k transpositions, then we can write it as e composed with k transpositions. So

$$\#(\sigma) \equiv \#(e) + k \equiv n + k \pmod 2$$

As a result, $k \equiv \#(\sigma) - n \pmod 2$, as the right hand side is constant, the parity of k is constant. □

Definition (Sign)**.** The sign of a permutation σ is

$$\operatorname{sign}(\sigma) = (-1)^k$$

where σ can be written as k transpositions.

Definition (Even, Odd)**.** If $\operatorname{sign}(\sigma) = 1$, we say σ is even. If $\operatorname{sign}(\sigma) = -1$, we say σ is odd.

Proposition. *An odd length cycle is even, an even length cycle is odd.*

Proposition. $\text{sign} : S_n \to \{\pm 1\}$ *is a surjective homomorphism.*

Definition (Alternating group)**.** The alternating group $A_n = \ker \text{sign}$ is the group consisting of all of the even permutations of S_n.

Lemma. *If $H \leq S_n$ contains an odd permutation, then half of its elements are odd.*

Proof. Let τ be an odd permutation in H, E be the set of even permutations and O be the set of odd permutation in H.

Define $f : E \to O$ by $f(\sigma) = \sigma\tau$. This is a bijection, so $|E| = |O|$. □

Theorem.

$$|A_n| = \frac{|S_n|}{2} = \frac{n!}{2}$$

10.3 Conjugation

Lemma. $\sigma(a_1 \ \dots \ a_k)\sigma^{-1} = (\sigma(a_1) \ \dots \ \sigma(a_k))$

Proposition. *Two elements of S_n are conjugate in S_n if and only if they have the same cycle type.*

Proof. Suppose if $\sigma = \sigma_1 \dots \sigma_k$. Then $\rho\sigma\rho^{-1} = \rho\sigma_1\rho^{-1} \dots \rho\sigma_k\rho^{-1}$. By the lemma above, $\rho\sigma\rho^{-1}$ and σ have the same cycle type.

On the other hand, if two permutations have the same cycle type, say $\sigma = (a_1 \ \dots \ a_{k_1})(a_{k_1+1} \ \dots) \dots$ and $\tau = (b_1 \ \dots \ b_{k_1})(b_{k_1+1} \ \dots) \dots$, then $\rho(a_i) = b_i$ will mean $\rho\sigma\rho^{-1} = \tau$. □

Proposition. $|\text{ccl}_{S_n}(\sigma)| = |\text{ccl}_{A_n}(\sigma)|$ *or* $|\text{ccl}_{S_n}(\sigma)| = 2|\text{ccl}_{A_n}(\sigma)|$.

Proof. Note that $C_{A_n}(\sigma) = C_{S_n}(\sigma) \cap A_n$ and that $C_{S_n}(\sigma) \leq S_n$. Thus either all of the permutations in $C_{S_n}(\sigma)$ are even, or exactly half of them are even. As a result, $|C_{A_n}(\sigma)| = |C_{S_n}(\sigma)|$ or $|C_{A_n}(\sigma)| = \frac{1}{2}|C_{S_n}(\sigma)|$. Using Orbit-Stabiliser we get the required result. □

Definition (Splitting)**.** If $|\text{ccl}_{S_n}(\sigma)| = 2|\text{ccl}_{A_n}(\sigma)|$, we say that the conjugacy class of σ splits in A_n.

Proposition. $\text{ccl}_{S_n}(\sigma)$ *splits in A_n if and only if there are no odd permutations which commute with σ.*

Proof. If $|\text{ccl}_{S_n}(\sigma)| = 2|\text{ccl}_{A_n}(\sigma)|$, then $C_{S_n}(\sigma) = C_{A_n}(\sigma)$. But we also have that $C_{A_n}(\sigma) = C_{S_n}(\sigma) \cap A_n$, so $C_{S_n}(\sigma) \subseteq A_n$.

Conversely, if $C_{S_n}(\sigma) \subseteq A_n$, then $C_{A_n}(\sigma) = C_{S_n}(\sigma) \cap A_n$ and so $\text{ccl}_{S_n}(\sigma)$ splits. □

10.4 Simplicity of A_5

Lemma. $C_{S_5}((1\ 2\ 3\ 4\ 5)) = \langle(1\ 2\ 3\ 4\ 5)\rangle$.

Proof. $|\text{ccl}_{S_5}((1\ 2\ 3\ 4\ 5))| = \dfrac{5 \times 4 \times 3 \times 2 \times 1}{5} = 24$, as it is all of the 5 cycles in S_5. By orbit stabilier, we have that $|C_{S_5}((1\ 2\ 3\ 4\ 5))| = 120/24 = 5$. Clearly $\langle(1\ 2\ 3\ 4\ 5)\rangle \subseteq C_{S_5}((1\ 2\ 3\ 4\ 5))$ and $|\langle(1\ 2\ 3\ 4\ 5)\rangle| = 5$, and we have the required result. □

Theorem. *A_5 is simple.*

Proof. The conjugacy classes in A_5 are as follows

Cycle Type	Odd element in C_{S_5}	Size of ccl_{S_5}	Size of ccl_{A_5}
$1,1,1,1$	Yes, (1 2)	1	1
$2,2,1$	Yes, (1 2)(3 4) commutes with (1 2)	15	15
$3,1,1$	Yes, (1 2 3) commutes with (4 5)	20	20
5	No	24	12 and 12

A normal subgroup of A_5 must be the following

- Contain e.
- Be a union of conjugacy classes.
- Have an order that divides $|A_n| = 60$.

As a result, the only normal subgroups are $\{e\}$ and A_5. □

11 Matrix Groups

In this section, $\mathbb{F}$ represents any field. Typically $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$. Let $M_n(\mathbb{F})$ represent the set of all $n \times n$ matrices for reprsenting linear maps $\mathbb{F}^n \to \mathbb{F}^n$.

Definition (General Linear Group). $\mathrm{GL}_n(\mathbb{F}) = \{A \in M_n(\mathbb{F}) : \det A \neq 0\}$

Definition (Special Linear Group). $\mathrm{SL}_n(\mathbb{F}) = \{A \in M_n(\mathbb{F}) : \det A = 1\} = \ker\det \leq \mathrm{GL}_n(\mathbb{F})$

Definition (Orthogonal Group). $O_n = O_n(\mathbb{R}) = \{A \in M_n(\mathbb{F}) : A^T A = I\}$

Proposition. $O_n \leq \mathrm{GL}_n(\mathbb{R})$

Proposition. $\det : O_n \to \{\pm 1\}$ *is a surjective homomorphism.*

Proof. Homomorphism is clear. $\det I = 1$, $\det \begin{pmatrix} -1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix} = -1$. □

Definition (Special Orthogonal Group). $SO_n = SO_n(\mathbb{R}) = \ker\det \leq O_n$.

11.1 Möbius Maps

Proposition. $\varphi : \mathrm{SL}_2(\mathbb{C}) \to \mathcal{M}$ *defined by*

$$\varphi\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = f = \left(z \mapsto \frac{az+b}{cz+d}\right)$$

is a surjective homomorphism.

Proof. Homomorphism can be checked by comparing entries.

If $f(z) = \dfrac{az+b}{cz+d}$ is a Möbius map, then $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{C})$, as $ad - bc \neq 0$. Let $D^2 = ad - bc$. Then $\varphi\left(\dfrac{1}{D}\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = f$. □

Proposition. $\ker\varphi = \{\pm I\}$

Proof. If $\varphi\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = \mathrm{id}$, then $\dfrac{az+b}{cz+d} = z$ for all $z \in \mathbb{C}$. So $a = d, b = c = 0$. As determinant of the matrix is 1, $a^2 = 1$ and $a = \pm 1$, $\ker\varphi = \{\pm I\}$. □

Proposition. $\mathcal{M} \cong \mathrm{SL}_2(\mathbb{C})/\{\pm I\}$.

Definition (Projective Special Linear Group). $PSL_2(\mathbb{C}) = \mathrm{SL}_2(\mathbb{C})/\{\pm I\}$.

11.2 Actions

Proposition. $\mathrm{GL}_n(\mathbb{F}), \mathrm{SL}_n(\mathbb{F}) \circlearrowleft \mathbb{F}^n$ *and* $O_n, SO_n \circlearrowleft \mathbb{R}^n$.

11.3 Change of Basis

Proposition. *$\mathrm{GL}_n(\mathbb{F})$ acts on $M_n(\mathbb{F})$ by conjugation. The orbit of $A \in M_n(\mathbb{F})$ is the set of matrices representing the same linear map with respect to different bases.*

Proof. The action is clear. A and B are in the same orbit if and only if there exists matrix P such that $PAP^{-1} = B$, for some $P \in \mathrm{GL}_n(\mathbb{F})$. By the definition of the change of base matrix this means that B represents the same linear map as A, with the basis given by the columns of P. □

11.4 Geometry of Orthogonal Groups

Proposition. *$P \in O_n$ if and only if the columns of P are orthonormal.*

Proof. $(P^T P)_i j = P^T_{ik} P_{kj} = P_{ki} P_{kj} = \delta_{ij}$. □

Proposition. *$P \circlearrowleft M_n(\mathbb{R})$ by conjugation. Two matrices are in the same orbit if and only if they represent the same linear map with respect to orthonormal bases.*

Proposition. $P \in O_n \iff \forall \mathbf{x}, \mathbf{y} \in \mathbb{R}^n, P\mathbf{x} \cdot P\mathbf{y} = \mathbf{x} \cdot \mathbf{y}$.

Definition (Reflection)**.** A reflection in the (hyper)plane with unit normal $\mathbf{a} \in \mathbb{R}^n$ is the linear map $R_{\mathbf{a}} : \mathbb{R}^n \to \mathbb{R}^n$, where

$$\mathbf{x} \mapsto \mathbf{x} - 2(\mathbf{x} \cdot \mathbf{a})\mathbf{a}$$

Proposition. $R_{\mathbf{a}} \in O_n$.

Proposition. $PR_{\mathbf{a}}P^{-1} = R_{P\mathbf{a}}$.

Proposition. $\det(R_{\mathbf{a}}) = -1$.

Proof. -1 is an eigenvalue as $R_{\mathbf{a}}(\mathbf{a}) = -\mathbf{a}$. 1 is an eigenvalue as for any $\mathbf{x}$ where $\mathbf{x} \cdot \mathbf{a} = 0$, $R_{\mathbf{a}}(\mathbf{x}) = \mathbf{x}$. So -1 has geometric multiplicity 1, 1 has geometric multiplicity $n-1$. $\det(R_{\mathbf{a}})$ is the product of the eigenvalues so it is -1. □

Theorem. *All elements of SO_2 are of the form $\begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}$, and all matrices of this form are in SO_2.*

Proof. Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SO_2$. Then $ad - bc = 1$, $A^T = A^{-1}$ so $\begin{pmatrix} a & c \\ b & d \end{pmatrix} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$. Thus $a = d$, $b = -c$. So $ad - bc = 1 \implies a^2 + b^2 = 1$. Without loss of generality, let $a = \cos\theta$, $b = \sin\theta$ for a unique $\theta \in [0, 2\pi)$. Converse implication is just calculation. □

Theorem. *The elements of $O_2 \backslash SO_2$ are reflections in lines through the origin.*

Proof. Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in O_2 \backslash SO_2$. Then $ad - bc = -1$, $A^T = A^{-1}$, so $\begin{pmatrix} a & c \\ b & d \end{pmatrix} = \begin{pmatrix} -d & b \\ c & -a \end{pmatrix}$, so $a = -d$, $b = c$. As a result, $a^2 + b^2 = 1$. Without loss of generality, set $a = \cos\theta$, $b = \sin\theta$, so $A = \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix}$.

Now $A \begin{pmatrix} \sin(\theta/2) \\ -\cos(\theta/2) \end{pmatrix} = \begin{pmatrix} -\sin(\theta/2) \\ \cos(\theta/2) \end{pmatrix}$, and $A \begin{pmatrix} \cos(\theta/2) \\ \sin(\theta/2) \end{pmatrix} = \begin{pmatrix} \cos(\theta/2) \\ \sin(\theta/2) \end{pmatrix}$. So A is the reflection in the line perpendicular to $\begin{pmatrix} \sin(\theta/2) \\ \cos(\theta/2) \end{pmatrix}$. □

Theorem. *Every element in O_2 is the composition of at most 2 reflections.*

Proof. Every element in $O_2 \backslash SO_2$ is a reflection. Now for $A \in SO_2$, $A = A \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$, and $A \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ are both in $O_2 \backslash SO_2$. □

Theorem. *For all $A \in SO_3$, 1 is an eigenvalue of A.*

Proof. $\det(A - I) = \det\big(A - AA^T\big) = \det(A)\det\big(I - A^T\big) = \det\big(I - A^T\big) = \det\big((I - A)^T\big) = \det(I - A) = -\det(A - I)$. So $\det(A - I) = 0$. $\square$

Theorem. *Every element in SO_3 is conjugate to an element of the form*

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix}$$

Proof. From above, we have $\mathbf{v}_1 \in \mathbb{R}^3$ such that $A\mathbf{v}_1 = \mathbf{v}_1$ and $|\mathbf{v}_1| = 1$. Extending $\mathbf{v}_1$ to an orthonormal basis $\{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$, we have that $A\mathbf{v}_i \cdot \mathbf{v}_1 = A\mathbf{v}_i \cdot A\mathbf{v}_1 = \mathbf{v}_i \cdot \mathbf{v}_1 = \delta_{i1}$. So $A\mathbf{v}_2$ and $A\mathbf{v}_3$ are in $\operatorname{span}\{\mathbf{v}_2, \mathbf{v}_3\}$.

As a result, we know that A has the form $\begin{pmatrix} 1 & 0 & 0 \\ 0 & a & b \\ 0 & c & d \end{pmatrix}$. A restricted to $\operatorname{span}\{\mathbf{v}_2, \mathbf{v}_3\}$ will be an element of SO_2, so we get that $A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix}$ with respect to the basis $\{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$.

The change of base matrix P will be in O_3, as $\{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$ is an orthonormal basis. It may or may not be in SO_3, if not, the change of base matrix with respect to $\{-\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$ will be in SO_3. $\square$

Theorem. *Every element of O_3 is the composition of at most 3 reflections.*

Proof. If $A \in SO_3$, then there exists $P \in SO_3$ such that $PAP^{-1} = B$, where $B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix}$. Since $\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$ is the composition of at most 2 reflections, so is B. Say $B = B_1B_2$. Then $A = PB_1P^{-1}PB_2P^{-1}$.

If $A \in O_3 \backslash SO_3$, then $\det A = -1$, and $A = A\begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. Then $A\begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ is in SO_3 and can be written as 2 reflections, and $\begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ is a reflection. $\square$

12 Symmetries of Platonic Solids

12.1 Tetrahedron

Let G be the group of symmetries of the tetrahedron. Clearly G acts transitively on the vertices, and the only symmetry that fixes all of the vertices is the identity, so the action of G on the vertices is also faithful.

Now, labelling the vertices of the tetrahedron as $1, 2, 3, 4$, we get that $\operatorname{Orb}(1) = \{1, 2, 3, 4\}$, and $\operatorname{Stab}(1)$ is the symmetries which fix 1. This is precisely the symmetries of the triangle $\{2, 3, 4\}$. So $\operatorname{Stab}(1) \cong D_6$. As a result, $|G| = 24$. Clearly G is a subgroup of S_4, and as $|G| = |S_4|$, we must in fact have $G = S_4$.

Now letting G^+ represent the group of symmetries consisting only of rotations. $\operatorname{Orb}(1) = \{1, 2, 3, 4\}$ and $\operatorname{Stab}(1)$ is the rotations of the triangle $\{2, 3, 4\}$. So $|G^+| = 12$. As $G^+ \leq G = S_4$, we must in fact have $G^+ = A_4$. Clearly all 3 cycles are there, and a $2 - 2$ cycle is a rotation through opposing edges.

12.2 Cube

Let G be the group of symmetries of the cube. Clearly G acts transitively on the vertices. So we get that $|\operatorname{Orb}(1)| = 8$. In addition, we have that $\operatorname{Stab}(1)$ contains the identity, 2 rotations (These are rotations through 1 and the opposing vertex. Considering the triangle formed by the vertices connected to 1, we see that there are two non-trivial rotations through this axis) and 3 reflections (for each edge connecting 1, reflect across plane through that edge and the opposing edge). So $|\text{Stab}(1)| = 6$. Thus $|G| = 48$.

Now let G^+ be the group of symmetries consisting only of rotations. Again this acts transitively on the vertices. Now Stab(1) contains only the rotations, so $|G| = 24$. Letting G^+ act on the four diagonals of the cube, we can define $\rho : G^+ \to S_4$. By rotations through the mid points of opposing edges, we see that $\operatorname{Im}\rho$ contains all 2-cycles, and by rotations though the mid points of opposing faces, we see that $\operatorname{Im}\rho$ contains all 4-cycles. As the 2-cycles generate S_4, we see that we must have $G^+ \cong S_4$.

Proposition. $O_3 \cong SO_3 \times C_2$.

Proof. $SO_3 = \ker\det$, and consider $\varphi : O_3 \to SO_3$ defined by

$$\varphi(A) = \begin{cases} A & \text{if } A \in SO_3 \\ -A & \text{if } A \notin SO_3 \end{cases}$$

This is a surjective homomorphism, with $\ker\varphi = \{\pm I\}$.

Then, $\ker\det \cap \ker\varphi = \{I\}$, $\ker\varphi \ker\det = \{\pm A : A \in SO_3\} = O_3$ and $-IA = A(-I)$, $AI = IA$, so $\ker\det \times \ker\varphi \cong O_3$. Thus $O_3 \cong SO_3 \times C_2$. $\square$

In the above, C_2 is generated by $-I$, which represents the map $\mathbf{v} \mapsto -\mathbf{v}$. Thus if $\mathbf{v} \mapsto -\mathbf{v}$ is a symmetry of a platonic solid, the group of symmetry will also split. Thus $G \cong G^+ \times C_2 \cong S_4 \times C_2$.

12.3 Platonic Solids

Cubes and Tetrahedra are Platonic solids, which means that their group of symmetries acts transitively on

(vertex, incident edge, incident face)

.

What this means is that choosing any vertex, an edge incident to it, and a face incident to the vertex, there is a symmetry which will map any other triple to it.

There are three more platonic solids, the octahedron, dodecahedron and the icosahedron. By inscribing the cube/octahedron in the other, we see that they must have the same group of symmetries. Similarly if we inscribe the icosahedron/dodecahedron into the other, they must have the same group of symmetries. We call them "dual".

Consequently only three groups are groups of symmetries of a platonic solid.