Groups

Hasan Baig

Michaelmas 2020

Contents

1 Basic Notation **2**
1.1 Basic Definitions . . . 2
1.2 Subgroups . . . 2
1.3 Homomorphisms, Isomorphisms . . . 4
1.4 Direct Products . . . 5

2 Important Examples **5**
2.1 Cyclic Group C_n . . . 5
2.2 Dihedral Group D_{2n} . . . 6
2.3 Symmetric Group . . . 6
2.4 Möbius Maps . . . 9

3 Lagrange's Theorem **9**

4 Quotients of Groups **11**
4.1 Basic Definitions . . . 11
4.2 First Isomorphism Theorem . . . 12
4.3 Correspondence Theorem . . . 13
4.4 Second Isomorphism Theorem . . . 13
4.5 Third Isomorphism Theorem . . . 13

5 Group Actions **14**
5.1 Basic Definitions . . . 14
5.2 Orbits and Stabilisers . . . 14
5.3 Symmetry Groups of Polyhedra . . . 15
5.4 Left Multiplication Actions . . . 16
5.5 Conjugation Actions . . . 17

6 The Möbius Group revisited **21**
6.1 Möbius Group acting on $\hat{\mathbb{C}}$ . . . 21
6.2 Cross-Ratios . . . 24

7 Matrix Groups **25**
7.1 Basic Definitions . . . 25
7.2 Möbius maps via matrices . . . 25
7.3 Change of Basis . . . 26
7.4 Symmetries of the cube revisited . . . 29

8 Groups of Order 8 **30**

1 Basic Notation

1.1 Basic Definitions

Definition. A **group** is set G together with a way of combining its elements $(*)$ satisfying:

(i) (closure) $g * h \in G (\forall g, h \in G)$

(ii) (identity) $(\exists e \in G)$ s.t. $e * g = g * e = g (\forall g \in G)$

(iii) (inverses) $(\forall g \in G)(\exists g^{-1}) \in G$ s.t. $g * g^{-1} = g^{-1} * g = e$

(iv) (associativity) $(\forall g, h, k \in G) g * (h * k) = (g * h) * k$.

Remarks.

- Formally, we say a set G is a group if there is a binary operation $* : G \times G \to G$ satisfying "identity", "inverses" and "assoc."
- Assoc. means can write $g * h * k$ without specifying which composition should be done first.

Prop. Let G be a group.

i) The identity element is unique.

ii) $\forall g \in G$, the inverse of g is unique

iii) If $gh = g$ then $hg = g$.

iv) If $gh = e$ then $hg = e$.

v) $(gh)^{-1} = h^{-1} g^{-1}$.

vi) $(g^{-1})^{-1} = g$

Proof.

i) Suppose e, e' both identity elements, show $e = e'$.

ii) Suppose $gh = e$ and $gk = e$, show $h = k$

iii) Left multiply by g^{-1}

iv) Conjugate by g, (left g^{-1})

v) Left multiply RHS by gh

vi) Left multiply by g

Definition. A group G is **abelian** if $\forall g, h \in G, gh = hg$.

Definition. A group G is **finite** if it has finitely many elements. The number of elements of G is the order of G, written $|G|$.

1.2 Subgroups

Definition. Let $(G, *)$ be a group. A subset $H \subseteq G$ is called a **subgroup** of G if $(H, *)$ is a group. We write $H \leq G$.

Remark. To check $H \subseteq G$ a subgroup, can just check closure, identity, inverses.

Lemma. Let G be a group. $H \subset G$ is a subgroup iff H is non-empty and $\forall a.b \in H, ab^{-1} \in H$

Proof. Trivial (check axioms)

Prop. The subgroups of $(\mathbb{Z}, +)$ are precisely the subsets of the form $n\mathbb{Z} \subseteq \mathbb{Z}(n \in \mathbb{N})$, where $n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$

Proof. Firstly show each is a subgroup by quick subgroup check.
If $H \leq \mathbb{Z}$ and non-trivial then show smallest positive element, show $n\mathbb{Z} \subseteq H$ and suppose for contradiction another element.

Prop.

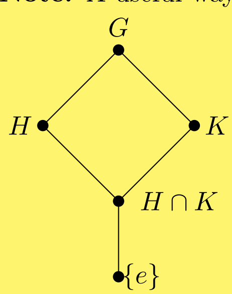
(i) Let H, K be subgroups of a group G. Then $H \cap K \leq G$.

(ii) If $K \leq H$ and $H \leq G$, then $K \leq G$.

(iii) If $K \subseteq H, H \leq G$ and $K \leq G$, then $K \leq H$.

Proof. Quick subgroup check works for all 3.

Note. A useful way to think about subgroups is via a diagram as follows, for example:



"Lattice of subgroups"
(Ascending edge or sequence of edges means the lower subgroup is contained in the upper)

Definition. Let $X \neq \varnothing$ be a subset of a group G. The **subgroup generated by X**, denoted $\langle X \rangle$, is the intersection of all subgroups containing X.
(Equivalently, it is the smallest subgroup containing X - i.e. if $X \subseteq H \leq G$, then $\langle X \rangle \leq H$).

Note. $\langle X \rangle$ contains e, $X \subseteq \langle X \rangle$, $\langle X \rangle$ contains all products of elements of X and their inverses

Prop. Let $X \subseteq G, X \neq \varnothing$. Then $\langle X \rangle$ is the set of elements of G of the form $x_1^{\alpha_1} x_2^{\alpha_2} x_3^{\alpha_3} \dots x_k^{\alpha_k}$ where $x_i \in X$ (not necessarily all distinct), $\alpha_i = \pm 1$, and $k \geq 0$ (when $k = 0$, the element is by definition e).

Proof. Let T be the set of such elements. $T \subseteq \langle X \rangle$, T a subgroup and $X \subseteq T$ so $T = \langle X \rangle$

1.3 Homomorphisms, Isomorphisms

Definition. Let $(G, *_G), (H, *_H)$ be groups. A function $\varphi : H \to G$ is a (group) **homomorphism** if for all $a, b \in H$,

$$\varphi(a *_H b) = \varphi(a) *_G \varphi(b)$$

A homomorphism φ is said to be **injective** if whenever $\varphi(a) = \varphi(b)$ in G, then $a = b$ in H.
A homomorphism φ is said to be **surjective** if $\forall g \in G, \exists h \in H$ s.t. $\varphi(h) = g$.
A homomorphism φ is said to be **bijective** if injective and surjective.

Prop. Let $\varphi : H \to G$ be a homom.

i) $\varphi(e_H) = e_G$
ii) $\varphi(h^{-1}) = \varphi(h)^{-1} \, \forall h \in H$
iii) if $\psi : G \to K$ is another homom., then $\psi \circ \varphi : H \to K$ is also a homom.

Proof.

i) Consider $\varphi(e_h *_H e_H)$
ii) Consider $\varphi(h) *_G \varphi(h)^{-1}$
iii) Let ψ and φ be the homomorphisms and reason from definitions

Definition. A bijective homomorphism $\varphi : H \to G$ is called an **isomorphism**. We say H, G are isomorphic and we write $H \cong G$ if $\exists$ isomorphism $H \to G$.

Prop. Let $\varphi : H \to G$ be an isomorphism. Then $\varphi^{-1} : G \to H$ is also an isomorphism.

Proof. $\varphi^{-1}(a *_G b) = \varphi^{-1}(\varphi(\varphi^{-1}(a) *_G \varphi^{-1}(b)))$ and use that φ a homomorphism

Definition. Let $\varphi : H \to G$ be a homom.
The **image** of φ is $\text{Im}(\varphi) = \{g \in G : g = \varphi(h) \text{ for some } h \in H\}$.
The **kernel** of φ is $\ker(\varphi) = h \in H : \varphi(h) = e_G$.

Prop. $\text{Im}(\varphi)$ is a subgroup of G and $\ker(\varphi)$ is a subgroup of H

Proof. Quick subgroup test works for both

Prop. Let $\varphi : H \to G$ be a homomorphism.

i) φ is surjective iff $\text{Im}(\varphi) = G$
ii) φ is injective iff $\ker(\varphi) = \{e\}$

Proof.

(i) By definition
(ii) Suppose φ injective. Have $\varphi(e_H) = e_G$, so e_H only element sent to e_G so $\ker(\varphi) = \{e_H\}$.
Suppose $\ker(\varphi) = \{e_H\}$ then show $\varphi(a) = \varphi(b) \implies a = b$

1.4 Direct Products

Definition. The **direct product** of two groups G, H is the set $G \times H$ with the operation of component-wise composition:

$$(g_1, h_1) * (g_2, h_2) = (g_1 *_G g_2, h_1 *_H h_2).$$

Remark. $G \times H$ contains subgroups isomorphic to G and H:

$$G \times \{e_H\} \text{ and} \{e_G\} \times H$$

Everything in (isomorphic copy of) G commutes with everything in (copy of) H

Theorem (Direct Product Theorem)**.** Let $H, K \leq G$ s.t.

i) $H \cap K = \{e\}$
ii) $\forall h \in H, \forall k \in K, hk = kh$
iii) $\forall g \in G, \exists h \in H, k \in K$ s.t. $g = hk$
Then $G \cong H \times K$

Proof. Let $\varphi : H \times K \to G$ be defined in natural way.
Show injective by $hk = e \implies h = k^{-1} \in H \cap K$

2 Important Examples

2.1 Cyclic Group C_n

Definition. Let G be a group and $X \subseteq G (X \neq \varnothing)$. If $\langle X \rangle = G$, then X is called a **generating set** of G.

Definition. G is **cyclic** if $\exists a \in G$ s.t. $\langle a \rangle = G$. In this case, $\forall b \in G$, $\exists k \in \mathbb{Z}$ s.t. $b = a^k$ (a is a generator of G)

Theorem. A cyclic group G is isomorphic to $\mathbb{Z}$ or to C_n for some $n \in \mathbb{N}$

Proof. Let $G = [b]$
Suppose $\exists n > 0$ s.t. $b^n = e$, take smallest such n and define $\varphi : C_n = [a] \to G$ by $\varphi(a^k) = b^k$. Show this is an isomorphism.
If no such n, define $\varphi : \mathbb{Z} \to G$ by $\varphi(k) = b^k$. Show this an isomorphism (suppose non-trivial kernel leads to contradiction for injective)

Definition. The **order of an element** $g \in G$ is the smallest $n \in \mathbb{N}$ s.t. $g^n = e$ (written $\text{ord}(g) = n$). If there is no such n, we say g has infinite order and write $\text{ord}(g) = \infty$.

Prop. Cyclic groups are abelian.

Proof. Trivial.

2.2 Dihedral Group D_{2n}

Definition. The **dihedral group** D_{2n} is the group of symmetries of a regular n-gon (the group operation is composition of symmetries).

Note. To show the elements of D_{2n} are those you expect, consider mapping of vertex v_1 and choice of v_2 giving $2n$ choices.

2.3 Symmetric Group

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

Theorem. $\mathrm{Sym}(X)$ forms a group wrt. compsitions.

Proof. Check axioms individually

Definition. If $|X| = n$, we write S_n for (the isomorphism class of) $Sym(X)$. S_n is called the **symmetric group** on n elements.

Note. $|S_n| = n(n-1)(n-2)\dots(2)(1) = n!$

Definition. A permutation of the form $\sigma = (a_1\, a_2\, \dots\, a_k)$ is a **k-cycle**.
If $k = 2$, i.e. $\sigma = (a_1\, a_2)$, then we call it a transposition.

Definition. Two cycles are **disjoint** if no number appears in both.

Definition. G a group. $g, h \in G$ **commute** if $gh = hg$ in G.

Lemma. Disjoint cycles commute.

Proof. Consider 4 cases of whether x in τ or σ disjoint cycles.

Theorem. Any $\sigma \in S_n$ can be written as a composition of disjoint cycles, and this expression is unique up to reordering cycles, and "cycling"" of cycles. ("Disjoint cycle decomposition"").

Proof. Consider $1, \sigma(1), \sigma^2(1), \sigma^3(1), \dots$. Show 2 in list must be equal by finiteness. This gives first cycle. Repeat with next number in $\{1, 2, \dots, n\}$ which hasn't already appeared. σ bijection so no number that has already appeared can reappear. Continue until exhausted all of set.
Uniqueness: suppose have 2 such decompositions

$$\sigma = (a_1 \, \dots \, a_{k_1})(a_{k_1+1} \, \dots a_{k_2}) \dots (a_{k_{m-1}+1} \, \dots a_{k_m}) = (b_1 \, \dots \, b_{l_1}) \dots (b_{l_{s-1}+1} \dots b_{l_s})$$

each element in set appears exactly once then $a_1 = b_t$ some t. Other numbers in cycle uniquely determined. Thus have

$$(a_1 \, \dots \, a_{k_1}) = (b_t \dots)$$

Disjoint cycles commute so have:

$$(a_1 \, \dots \, a_{k_1}) \dots = (b_t \, \dots) \dots$$

Continue in this way to see that all other cycles match.

Definition. The set of cycle lengths of the disjoint cycle decomposition of σ is its **cycle type**.

Theorem. The order of $\sigma \in S_n$ is the least common multiple of the cycle lengths in its cycle type.

Proof. Order of a k-cycle is k. Suppose $\sigma = \tau_1 \tau_2 \dots \tau_r$, τ_i disjoint cycles.
Have $\sigma^m = \tau_1^m \tau_2^m \dots \tau_r^m$, since disjoint cycles commute.
Let each τ_i be a k_i-cycle, then if $\sigma^m = e$, we have $\tau_1^m = \tau_2^{-m} \dots \tau_r^{-m}$
Elements in set permuted by LHS and RHS are disjoint so both sides must be $= e$. Thus $k_1 | m$. This holds for any k_i
Hence, $\mathrm{lcm}(k_1, \dots, k_r) | \mathrm{ord}(\sigma)$. Letting $l = \mathrm{lcm}(k_1, \dots, k_r)$, we can show $\sigma^l = e$ (by considering disjoint cycle decomposition). Hence $\mathrm{ord}(\sigma) | l \implies \mathrm{ord}(\sigma) = l$.

Prop. Let $\sigma \in S_n$. Then σ is a product of transpositions.

Proof. Sufficies to do this for a cycle.

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

Note. This is not unique but the parity of number of transpositions is well-defined.

Theorem. Writing $\sigma \in S_n$ as a product of transpositions in different ways, σ is either always a product of an even no. of transpositions or always a product of an odd no. of transpositions.

Proof. Write $\#(\sigma)$ for the number of cycles in σ in disjoint cycle decomposition.
See what happens to $\#(\sigma)$ when multiplying by $(c\,d)$:
If a cycle contains neither c nor d, unaffected.
If c, d in same cycle (considering disjoint decomp.), say $c\,a_2\,a_3\,\ldots\,a_{k-1}\,d\,a_{k+1}\,\ldots\,a_l)$, then:

$$(c\,a_2\,\ldots\,a_{k-1}\,\ldots\,a_l)(cd) = (c\,a_{k+1}\,\ldots\,a_l)(d\,a_2\,\ldots\,a_{k-1})$$

So $\#(\sigma\tau) = \#(\sigma) + 1$.
If c, d in different cycles (possible 1-cycles):

$$(c\,a_2\,\ldots\,a_k)(d\,b_2\,\ldots\,b_l)(c\,d) = (c\,b_2\,\ldots\,b_l\,d\,a_2\,\ldots\,a_k)$$

So $\#(\sigma\tau) = \#(\sigma) - 1$.
So for any σ, any transposition τ,

$$\#(\sigma) \equiv \#(\sigma\tau) + 1 \bmod 2$$

If $\sigma = \tau_1 \ldots \tau_k = \tau_1' \ldots \tau_l'$, we know $\#(\sigma)$ uniquely determined from σ (unique disjoint decomposition)
Also have $\sigma = e \cdot \tau_1 \ldots \tau_k = e \cdot \tau_1' \ldots \tau_l'$ So applying transpositions to e, we see:

$$\#(e) + k \equiv \#(e) + l \bmod 2$$

So $n + k \equiv n + l \bmod 2$ so $k \equiv l \bmod 2$, as desired.

Definition. Writing $\sigma \in S_n$ as a product of transpositions, $\sigma = \tau_1 \ldots \tau_k$, the **sign** of σ is defined as $\text{sign}(\sigma) = (-1)^k$.
If $\text{sign}(\sigma) = 1$, we say σ is an **even** permutation, and if $\text{sign}(\sigma) = 1$, we say σ is an **odd** permutation.

Theorem. For $n \geq 2$, $\text{sign} : S_n \to \{\pm 1\}$ is a surjective homomorphism

Proof. Know well-defined from above. Then have $\text{sign}(\sigma\sigma') = (-1)^{k+l} = (-1)^k \cdot (-1)^l$ to show homomorphism. consider e and $(1\,2)$ to show surjective.

Definition. The **kernel** of the homomorphism $\text{sign} : S_n \to \{\pm 1\}$ is called the alternating group, A_n.

Prop. $\sigma \in S_n$ is even iff its disjoint cycle decomposition contains an even number if even-length cycles. Even length cycles give sign -1, odd-length cycles give sign 1.

Proof. Let n be number of even-length cycles, m number of odd-length cycles.

2.4 Möbius Maps

Definition. A **Möbius map** is a function $f : \hat{\mathbb{C}} \to \hat{\mathbb{C}}$ of the form $f(z) = \frac{az+b}{cz+d}$ with: $(a, b, c, d \in \mathbb{C}), ad - bc \neq 0$, and:

$$f\left(\frac{-d}{c}\right) = \infty$$

$$f(\infty) = \frac{a}{c} \text{ if } c \neq 0$$

$$f(\infty) = \infty \text{ if } c = 0$$

Lemma. Möbius maps are bijections $\hat{\mathbb{C}} \to \hat{\mathbb{C}}$.

Proof. Inverse of $f(z) = \frac{az+b}{cz+d}$ is $f^{-1}(z) = \frac{dz-b}{-cz+a}$ (can check both ways work)

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

Proof. Can check axioms individually.

Remark. Can use conventions: "$\frac{1}{\infty} = 0$", "$\frac{1}{0} = \infty$", "$\frac{a\infty}{c\infty} = \frac{a}{c}$

Prop. Every Möbius map can be written as a composition of maps of the following forms:

i) $f(z) = az \ (a \neq 0)$
ii) $f(z) = z + b$
iii) $f(z) = \frac{1}{z}$

Proof. $c = 0$ case trivial,
$c \neq 0$:

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

3 Lagrange's Theorem

Definition. Let H be a subgroup of a group $G, g \in G$. A set of the form $gH = \{gh : h \in H\}$ is called a **left coset** of H in G and a set of the form $Hg = \{hg : h \in H\}$ is a **right coset** of H in G. $(gH, Hg \subseteq G)$.

Theorem (Lagrange's Theorem)**.** Let $H \leq G$ be a subgroup of a finite group G.

i) $|H| = |gH| \, \forall g \in G$
ii) for $g_1, g_2 \in G$, either $g_1H = g_2H$ or $g_1H \cap g_2H = \varnothing$
iii) $G = \bigcup_{g \in G} gH$

In particular,

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

Where $G : H$ is the index of H in G ($|G : H|$ is the number of distinct cosets of H in G)

Proof.

i) The function $H \to gH$ given by $h \mapsto gh$ defines a bijection (inverse $gh \mapsto g^{-1}gh = h$)
ii) Suppose non-empty intersection then show this implies equality (LHS $\subseteq$ RHS and vice versa)
iii) Given $g \in G$, then $g \in gH$ so LHS $\subseteq$ RHS but also have RHS $\subseteq$ LHS So cosets partition G, implying $|G| = |G : H||H|$

Remark. Used left cosets but could have used right cosets similarly to get an analagous result.

Prop.

$$g_1H = g_2H \iff g_1^{-1}g_2 \in H$$

Proof. Trivial from definitions.

Definition. Taking an element from distinct cosets of H in G: $g_1, g_2, \dots, g_{|G:H|}$, then $G = \bigcup_{i=1}^{|G:H|} g_iH$. The g_i are called **coset representatives** of H in G

Corollary. Let G be a finite group and $g \in G$. Then $\text{ord}(g) | |G|$.

Proof. Take $H = \langle g \rangle$. Then $\text{ord}(g) = |H|$ which divides $|G|$ by Lagrange

Corollary. Let G be a finite group, $g \in G$. Then $g^{|G|} = e$.

Proof. From previous corollary, $|G| = \text{ord}(g) \cdot n$, some $n \in \mathbb{N}$.
So $g^{|G|} = g^{\text{ord}(g) \cdot n} = \left(g^{\text{ord}(g)}\right)^n = e^n = e$

Corollary. Groups of prime order are cyclic and are generated by every non-identity element.

Proof. Consider $\langle g \rangle$ for some non-identity element g. $|\langle g \rangle| = p$ as divides p and contains e, g. Hence group cyclic.

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

Proof. Have $\mathbb{Z}_n^*$ with multiplication a group order $\varphi(n)$ and so follows from corollary.

Prop. If $|G| = 4$, then $G \cong C_4$, or $C_2 \times C_2$.

Proof. Possible element orders: $1, 2, 4$
If there is an element order 4, then group is C_4 (generated by element)
If there isn't then non-identity elements all order 2. Take 2 distinct elements order 2 say b and c and show G isomorphic to $C_2 \times C_2$ by direct product theorem.

4 Quotients of Groups

4.1 Basic Definitions

Definition. A subgroup N of G is **normal** if $\forall g \in G, gN = Ng$. We write $N \trianglelefteq G$. Equivalently:

$$\forall g \in G \, \forall n \in N, g^{-1}ng \in N$$

$$\forall g \in G, g^{-1}Ng = N$$

(here $g^{-1}Ng = \{g^{-1}ng : n \in N\}$).

Prop. The following are equivalent (TFAE):

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

$$\forall g \in G \, \forall n \in N, \, g^{-1}ng \in N$$

$$\forall g \in G, \, g^{-1}Ng = N$$

Proof. Can show equivalence trivially.

Prop.
i) Any subgroup of an abelian group is normal.
ii) Any subgroup of index 2 is normal.

Proof.
i) G abelian $\implies g^{-1}ng = n \forall g \in G, \forall n \in N$
ii) Cosets partition group so cosets are H and $G \backslash H$ for both left and right cosets cases so $gH = Hg$ so H normal in G

Prop. If $\varphi : G \to H$ a homomorphism, then $\ker \varphi \trianglelefteq G$.

Proof. Already know it is a subgroup, trivial to show normal. (consider $\varphi(g^{-1}kg)$

Prop. If $|G| = 6$, then $G \cong C_6$ or D_6.

Proof. By Langrange, possible element orders are $1, 2, 3, 6$.
Is there an element order 6?
If yes: $G \cong C_6$
If no: there is an element order 3, say r. (By Cauchy or if only order 2 then 6 a power of 2).
Hence $|G : \langle r \rangle| = 2$ so normal and consider cases for conjugation by order 2 element (must exist by considering sets of $\langle g \rangle$).

Prop. Let $N \trianglelefteq G$. The set of (left) cosets of N in G forms a group under the operation $g_1 N \cdot g_2 N = g_1 g_2 N$

Proof. Can check well-definedness, 3 axioms.

Definition. If $N \trianglelefteq G$, the group of (left) cosets of N in G is called the **quotient group** of G by N, written G/N.

Remark. Normality not transitive i.e. $N \trianglelefteq H$ and $H \trianglelefteq G \not\Rightarrow N \trianglelefteq G$

Theorem. Given $N \trianglelefteq G$, the function $\pi : G \to G/N$, $\pi(g) = gN$ is a surjective homomorphism with $\ker \pi = N$

Proof. Homomorphism follows previous prop. Surjective trivial.

Note. This together with the fact that kernels are normal subgroups shows "normal subgroups are exactly kernels of homomorphisms"

4.2 First Isomorphism Theorem

Theorem (1^{st} Isomorphism Theorem)**.** Let $\varphi : G \to H$ be a homomorphism. Then $G/\ker\varphi \cong \text{Im } \varphi$

Proof. Define $\overline{\varphi} : G/\ker\varphi \to \text{Im } \varphi$ via

$$g \ker\varphi \mapsto \varphi(g)$$

Well-defined: show 2 representations of same coset of $\ker\varphi$ map to same thing.
Homomorphism: follows from φ being a homomorphism.
Surjective: all elements in $\text{Im } \varphi$ are of the form $\varphi(g)$ for some $g \in G$ so clearly surjective.
Injective: if $\overline{\varphi}(g \ker\varphi) = e = \varphi(g)$ in $\text{Im } (\varphi)$, then $g \in \ker\varphi$, so $g \ker\varphi = \ker\varphi$

4.3 Correspondence Theorem

Theorem (Correspondence Theorem)**.** Let $N \trianglelefteq G$. The subgroups of G/N are in bijective correspondence with subgroups of G containing N.

Proof. Let $N \subseteq M \leq G$ and consider the quotient map

$$\pi : G \to G/N$$

$$\pi(M) = \{mN : m \in M\} = M/N \leq G/N$$

Then show any $H \leq G/N$ can be written as $H = M/N$, for some M by just showing the preimage is a group containing N and then let $\pi^{-1}(H) = M$.

$$\pi^{-1}(M/N) = \{m \in G : mN \in M/N\} = M$$

So map between the subgroups of G/N and subgroups of G containing N is invertible and therefore they biject

Note. This correspondence preserves lots of structure: indices, normality, containment.

4.4 Second Isomorphism Theorem

Corollary (2^{nd} Isomorphism Theorem)**.** Let $H \leq G$, $N \trianglelefteq G$. Then $H \cap N \trianglelefteq H$ and $H/H \cap N \cong HN/N$

Proof. Consider function $\varphi : H \to HN/N$, $\varphi(h) = hN$. This is a well-defined surjective homomorphism. Find the kernel then result follows by 1^{st} isomorphism theorem.

4.5 Third Isomorphism Theorem

Corollary (3^{rd} Isomorphism Theorem)**.** Let $N \leq M \leq G$ s.t. $N \trianglelefteq G, M \trianglelefteq G$. Then $M/N \trianglelefteq G/N$ and $(G/N)/(M/N) \cong G/M$

Proof. Define $\varphi : G/N \to G/M$ by $\varphi(gN) = gM$.
Well-defined since $N \leq M$, surjective homomorphism. Find the kernel then result follows by 1^{st} isomorphism theorem.

Definition. A group G is simple if its only normal subgroups are $\{e\}$ and G.

5 Group Actions

5.1 Basic Definitions

Definition. Let G be a group, X be a set. An **action** of G on X is a function $\alpha : G \times H \to X$, $\alpha(g, x) = \alpha_g(x) = g(x)$, satisfying:

$$g(x) \in X \, \forall g \in G \, \forall x \in X$$

$$e(x) = x \, \forall x \in X$$

$$g(h(x)) = gh(x) \, \forall g, h \in G \, \forall x \in X$$

Notation: $G \curvearrowright X$

Lemma. $\forall g \in G, \alpha_g : X \to X, x \mapsto g(x)$ is a bijection

Proof. Have inverse $\alpha_{g^{-1}} : X \to X$, $x \mapsto g^{-1}(x)$

Prop. Let G be a group, X a set. Then $\alpha : G \times X \to X$ ($\alpha(g, x) = g(x)$) is an action iff $\rho : G \to \text{Sym}(X)$ with $\rho(g) = \alpha_g$ is a homomorphism

Proof. $\implies$: Have α an action.By previous lemma, α_g is a bijection $X \to X$, so $\alpha_g \in \text{Sym}(X)$.
So $\rho(gh) = \alpha_{gh} = \alpha_g \alpha_h = \rho(g)\rho(h)$, so ρ homomorphism.
$\impliedby$: Given $\rho : G \to \text{Sym}(X)$ a homomorphism, can define $\alpha : G \times X \to X$ by $\alpha(g, x) = \alpha_g(x) = \rho(g)(x)$ and can show α is an action.

Definition. The **kernel of an action** $\alpha : G \times X \to X$ is the kernel of the homom. $\rho : G \to \text{Sym}(X)$. These are all the elements of G that act as the identity of $\text{Sym}(X)$

Note. $G/\ker\rho \cong \text{ Im } \rho \leq \text{Sym}(X)$ (by 1^{st} isomorphism theorem) so in particular if $\ker \rho = \{e\}$, then $G \leq \text{ Sym}(X)$

Definition. An action G on X is **faithful** if $\ker \rho = \{e\}$

5.2 Orbits and Stabilisers

Definition. Let G act on X, $x \in X$.
The orbit of x is:

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

The stabiliser of x is:

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

Definition. An action is **transitive** if $\text{Orb}(x) = X$.

Lemma. For any $x \in X$, $\text{stab}(x)$ is a subgroup of G

Proof. Quick subgroup check works.

Lemma. Let G act on X. Then the orbits partition X

Proof. If an element in X in 2 orbits, show the orbits must be equal (by showing subsets of one another)

Theorem (Orbit-Stabiliser)**.** Let G act on X, G finite. Then for any $x \in X$,

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

Proof. Showing points in orbit of x in bijection with cosets of $\text{Stab}(x)$:

$$g(x) = h(x) \iff h^{-1}g(x) = x \iff h^{-1}g \in \text{ Stab}(x) \iff g \text{ Stab}(x) = h \text{ Stab}(x)$$

So $|\text{Orb}(x)| = |G : \text{Stab}(x)| = |G|/|\text{Stab}(x)|$ by Lagrange.

5.3 Symmetry Groups of Polyhedra

Prop. Symmetries of tetrahedron isomorphic to S_4.

Proof. Let G be the group of symmetries of the tetrahedron.
Clearly G acts transitively on the vertices, and no non-identity symmetry fixes all vertices, so get $\rho : G \to S_4$ injective.
$\text{Orb}(1) = \{1, 2, 3, 4\}$, $\text{Stab}(1) =$ symmetries of a triangle.
$|G| = |\text{Orb}(1)| \cdot |\text{Stab}(1)| = 4 \cdot 6 = 24$ so $G \cong S_4$

Prop. Let G^+ be the symmetry group of rotations of cube. $G^+ \cong S_4$

Proof. Consider it acting on vertices and use orbit stabiliser to show $|G^+| = 24$, consider it acting on 4 diagonals and show you can get $(1\,2)$ and $(1\,2\,3\,4)$ by considering rotation angle π axis diagonal or rotation angle $\frac{\pi}{2}$ axis vertical through center respectively. Thus can generate all transpositions so can generate group.

Theorem (Cauchy's Theorem)**.** Let G be a finite group, p a prime s.t. $p||G|$. Then G has an element of order p.

Proof. We will construct an action onto a subset of G^p and, considering orbits of this, we will deduce there must exist such an element.
Let $p||G|$. Consider $G^p = G \times G \times \dots \times G$, i.e. the group formed of p-tuples of elements of G, with coordinate wise composition where

$$(g_1, g_2, \dots, g_p) * (h_1, h_2, \dots, h_p) = (g_1h_1, g_2h_2, \dots, g_ph_p)$$

Consider the subset $X \subseteq G^p$ where $X = \{(g_1, g_2, \dots, g_p) \in G^p : g_1g_2 \dots g_p = e\}$
Note that if $g \in G$ has order p, then $(g, g, \dots, g) \in X$.
And if $(g, g, \dots, g) \in X$, $g \neq e$ then g has order p (since p prime).
Now take a cyclic group $C_p = \langle a \rangle$, and let C_p act on X by "cycling".

$$a(g_1, \dots, g_p) = (g_2, g_3, \dots, g_p, g_1)$$

We can check this is an action.
Orbits partition X, sum of sizes of distinct orbits must be $|X|$. But we know $|X| = |G|^{p-1}$ (can choose first $p-1$ elements and last fixed as inverse).
Hence as $p||G|$, $p||X|$.
Considering the orbits size 1 and orbits size p. Since $|\text{Orb}(e, e, \dots, e)| = 1$, there must be other orbits of size 1 (at least $p-1$ such). Orbits size 1 are just tuples of 1 element repeated so from before, we have an element order p.

5.4 Left Multiplication Actions

Lemma. Let G be a group. G acts on itself by left multiplication. This action is faithful and transitive.

Proof. Can check satisfies definition of action trivially.
Faithful: $g(x) = x \, \forall x \in G$, then $ge = e$ so $g = e$
Transitive: given $x, y \in G$, by setting $g = yx^{-1}$ we have $g(x) = gx = yx^{-1}x = y$

Definition. The left multiplication action of a group on itself is called the **left regular action**.

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

Proof. Let G act on G by the left regular action. This gives a homomorphism:

$$\rho : G \to \text{ Sym}(G)$$

with $\ker \rho = \{e\}$ since the action is faithful. so,by the 1^{st} Isomorphism Theorem,:

$$G = G/\ker \rho = \text{ Im } \rho \leq \text{ Sym}(G)$$

Prop. Let $H \leq G$. Then G acts on the set of left-cosets by left multiplication, and the action is transitive.

Proof. Can check satisfies definition of an action trivially.
Transitive: given g_1H, g_2H, have $(g_1g_2^{-1})(g_2H) = g_1g_2^{-1}g_2H = g_1H$

Notes.
- this is the left regular action if $H = \{e\}$
- this induces actions of G on its quotient groups G/N

5.5 Conjugation Actions

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

Note. Can view conjugate elements as doing the same things just from a different perspective. Think about changing bases in a vector space. The conjugate matrices do the same thing just viewed from different 'lenses'.

Prop. A group G acts on itslf by conjugation.

Proof. Can check satisfies definition of an action trivially.

Definition. The kernel of the conjugation action of G on itself is the **center** $Z(G)$ of G:

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

"elements that commute with everything"

Definition. An orbit of the conjugation action of G on itself is called a **conjugacy class**:

$$\mathrm{ccl}(h) = \{ghg^{-1} : g \in G\}.$$

Definition. Stabilisers of the conjugation action of G on itself are called **centralisers**:

$$\mathrm{C}_G(h) = \{g \in G : ghg^{-1} = h\}$$

"elements that commute with h".

Prop.

$$Z(G) = \bigcap_{h \in G} C_G(h)$$

Proof. Can show subsets of each other.

Definition. If $H \leq G, g \in G$, then the **conjugate of H** by g is:

$$gHg^{-1} = \{ghg^{-1} : h \in H\}$$

Prop. Let $H \leq G, g \in G$. Then gHg^{-1} is also a subgroup of G.

Proof. Check axioms individually.

Note. gHg^{-1} is isomorphic to H (trivial proof, isomorphism is $h \mapsto ghg^{-1}$)

Prop. A group G acts by conjugation on the set of its subgroups. The singleton orbits are the normal subgroups.

Proof. Can check satisfies definition of an action trivially.
Singleton orbits are the normal subgroups as $N \trianglelefteq G \iff \forall g \in G\, gNg^{-1} = N$

Prop. Normal subgroups are those subgroups that are unions of conjugacy classes.

Proof. Let $N \trianglelefteq G$. Then if $h \in N$, then $ghg^{-1} \in N\, \forall g \in G$. So $\text{ccl}(h) \subseteq N$.
So N is a union of ccls of its elements, i.e.

$$N = \bigcup_{h \in N} \text{ccl}(h)$$

(RHS $\subseteq$ LHS as ccl of each h subset of N. LHS $\subseteq$ RHS as given $h \in N$, h is in its own ccl.)
And conversely, if H a subgroup that is a union of ccls, then:

$$\forall g \in G,\, \forall h \in H,\, ghg^{-1} \in H \implies H \trianglelefteq G$$

Lemma. Given a k-cycle $(a_1\ \ldots\ a_k)$ and $\sigma \in S_n$, we have:

$$\sigma(a_1\ \ldots\ a_k)\sigma^{-1} = (\sigma(a_1)\, \sigma(a_2)\ \ldots\ \sigma(a_k))$$

Proof.

$$\begin{aligned}\sigma(a_1\ \ldots\ a_k)\sigma^{-1} : &\sigma(a_1) \mapsto a_1 \mapsto a_2 \mapsto \sigma(a_2)\\ &\sigma(a_2) \mapsto a_1 \mapsto a_2 \mapsto \sigma(a_2)\\ &\vdots\\ &\sigma(a_k) \mapsto a_1 \mapsto a_2 \mapsto \sigma(a_2)\end{aligned}$$

So $\sigma(a_1\ \ldots\ a_k)\sigma^{-1}$ and $(\sigma(a_1)\, \sigma(a_2)\ \ldots\ \sigma(a_k))$ do the same thing on $\{\sigma(a_1), \sigma(a_2), \ldots, \sigma(a_k)\}$.
For any $a \notin \{\sigma(a_1), \sigma(a_2), \ldots, \sigma(a_k)\}$, $(\sigma(a_1)\, \sigma(a_2)\ \ldots\ \sigma(a_k))$ leaves a unchanged, and $\sigma(a_1\ \ldots\ a_k)\sigma^{-1}$ does too as $\sigma^{-1}(a) \notin \{a_1, \ldots, a_k\}$

Prop. Two elements of S_n are conjugate (in S_n i.e. via conjugation by an element $\in S_n$) iff they have the same cycle type.

Proof. Two elements that are conjugate clearly have same cycle type as by writing in disjoint cycle notation:

$$\rho\sigma\rho^{-1} = \rho\sigma_1\rho^{-1}\rho\sigma_2\rho^{-1}\dots\rho\sigma_m\rho^{-1}$$

And previous lemma shows each $\rho\sigma_i\rho^{-1}$ a cycle length σ_i and the $\rho\sigma_i\rho^{-1}$ are distinct since ρ is a bijection.
Previous lemma shows that same cycle type $\implies$ conjugate as if:

$$\sigma = (a_1\ \dots\ a_k)(a_{k_1+1}\ \dots\ a_{k_2})(a_{k_2+1}\ \dots)\dots$$

$$\tau = (b_1\ \dots\ b_k)(b_{k_1+1}\ \dots\ b_{k_2})(b_{k_2+1}\ \dots)\dots$$

Then ρ defined by $\rho(a_i) = b_i$ has $\rho\sigma\rho^{-1} = \tau$.

Method. Determining conjugacy classes of S_4:

cycle type	example element	size of ccl	size of C_{S_4}	sign
1,1,1,1	e	1	24	+1
2,1,1	(1 2)	6	4	-1
2,2	(1 2)(3 4)	3	8	+1
3,1	(1 2 3)	8	3	+1
4	(1 2 3 4)	6	4	-1

Notes.
- Determine size of ccl by combinatorics.
- Determine size of C_{S_4} by $|S_4|/|\text{ccl}|$ (orbit-stabiliser)

From the information above, can deduce the normal subgroups of S_4 as order divides 24 and order is size of union of ccls ie sum of sizes of ccls and must have e.

Warning. If 2 elements are conjugate in S_n that does NOT mean they are conjugate in A_n.

Method. Determining possible sizes of a ccl in A_n:
The size of a conjugacy class in A_n of an element in A_n is either the same size as the ccl in S_n or half the size of the ccl in S_n.

$$|S_n| = |\text{ccl}_{S_n}(\sigma)| \cdot |C_{S_n}(\sigma)|$$

$$|A_n| = |\text{ccl}_{A_n}(\sigma)| \cdot |C_{A_n}(\sigma)|$$

But $|S_n| = 2|A_n|$ and $|\text{ccl}_{A_n}(\sigma)| \leq |\text{ccl}_{S_n}(\sigma)|$ and $|C_{A_n}(\sigma)| \leq |C_{S_n}(\sigma)|$
Hence

$$|\text{ccl}_{A_n}(\sigma)| = \frac{1}{2}|\text{ccl}_{S_n}(\sigma)| \text{ and } |C_{A_n}(\sigma)| = |C_{S_n}(\sigma)|$$

Or

$$|\text{ccl}_{A_n}(\sigma)| = |\text{ccl}_{S_n}(\sigma)| \text{ and } |C_{A_n}(\sigma)| = \frac{1}{2}|C_{S_n}(\sigma)|$$

Definition. When $|\text{ccl}_{A_n}(\sigma)| = \frac{1}{2}|\text{ccl}_{S_n}(\sigma)|$, we say that the conjugating class of σ **splits** in A_n.

Prop. The ccl of $\sigma \in A_n$ splits in A_n iff no odd permutations commute with σ

Proof.

$$|\text{ccl}_{A_n}(\sigma)| = \frac{1}{2}|\text{ccl}_{S_n}(\sigma)| \iff |C_{A_n}(\sigma)| = |C_{S_n}(\sigma)|$$

We have:

$$C_{A_n}(\sigma) = A_n \cap C_{S_n}(\sigma)$$

$A_n \cap C_{S_n}(\sigma) = C_{S_n}(\sigma)$ iff $C_{S_n}(\sigma)$ contains ONLY even elements ie no odd elements. Hence, we have this iff no odd permutation commutes with σ.

Note. Hence to determine the size of a ccl in A_n, determine the size in S_n. It remains the same if an odd permutation commutes with your element. If no such odd permutation exists, then divide size of ccl in S_n by 2.

Method. Showing no odd permutation commutes with an element in A_n:
One way of doing this is by determining exactly what $C_{S_n}(\sigma)$ is.
e.g. $C_{S_4}(1\,2\,3) = \langle(1\,2\,3)\rangle$ since $|C_{S_4}(1\,2\,3)|$ and all of $\langle(1\,2\,3)\rangle$ clearly commutes with $(1\,2\,3)$

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

Proof. Show size of ccl is 24. Thus size of centraliser is 5. RHS contained in centraliser and same size hence centraliser is RHS.

Theorem. A_5 is simple.

Proof. Normal subgroups must be unions of ccls, must contain e and must order must divide $|A_5| = 60$.
Show sizes of ccls in A_5 are $1, 15, 20, 12, 12$. Hence only ways to get a number dividing 60 whilst ensureing we have '1' in our sum are:

$$1 = 1$$

And

$$1 + 15 + 20 + 12 + 12 = 60$$

Hence the normal subgroups of A_5 are $\{e\}$ and A_5

6 The Möbius Group revisited

6.1 Möbius Group acting on $\hat{\mathbb{C}}$

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

Prop. The action $\mathcal{M}$ on $\hat{\mathbb{C}}$ is faithful, and so $\mathcal{M} \leq \mathrm{Sym}(\hat{\mathbb{C}})$

Proof. Consider $\rho : \mathcal{M} \to \mathrm{Sym}(\hat{\mathbb{C}})$ given by $\rho(f)(z) = f(z)$.
Then if $\rho(f) = \mathrm{id}$. permutation of $\hat{\mathbb{C}}$ then f is the identity in $\mathcal{M}$. So ρ injective and the action is faithful.

Definition. A **fixed point** of a Möbius map $f : \hat{\mathbb{C}} \to \hat{\mathbb{C}}$ is a point $z \in \hat{\mathbb{C}}$ s.t. $f(z) = z$.

Theorem. A Möbius map with ≥ 3 fixed points is the identity

Proof. Suppose $f = \frac{az+b}{cz+d}$ has ≥ 3 fixed points.
If ∞ not a fixed point then $\frac{az+b}{cz+d} = z$ for ≥ 3 complex numbers, ie:

$$cz^2 + (d-a)z - b = 0$$

Has ≥ 3 roots in $\mathbb{C}$. But a quadratic has ≤ 2 roots, so must have $c = b = 0, d = a$ i.e. $f(z) = z$.
If ∞ a fixed point, then $c = 0$. Hence consider:

$$(a-d)z + b = 0$$

Instead which must have ≥ 2 roots in $\mathbb{C}$. Similarly above has ≤ 1 roots unless $a = d, b = 0$ hence this is the case and so $f(z) = z$

Corollary. If two Möbius maps coincide on 3 distinct points in $\hat{\mathbb{C}}$, then they are equal.

Proof. If f and g are 2 such permutations coinciding on z_1, z_2, z_3, then $g^{-1}f(z_i) = z_i$ for $i = 1, 2, 3$.
So $g^{-1}f$ fixes ≥ 3 points.
So $g^{-1}f = \mathrm{id}$. from previous theorem so $f = g$.

Remark. We can interpret this as "knowing what a Möbius map does on 3 points in $\hat{\mathbb{C}}$ uniquely determines it."

Theorem. There is a unique Möbius map sending any 3 distinct pints of $\hat{\mathbb{C}}$ to any 3 distinct points of $\hat{\mathbb{C}}$, i.e. given $z_1, z_2, z_3 \in \hat{\mathbb{C}}$ (distinct) and $w_1, w_2, w_3 \in \hat{\mathbb{C}}$ (distinct), $\exists! f$ s.t. $f(z_i) = w_i$ for $i = 1, 2, 3$

Proof. We show unique map sending to $(0, 1, \infty)$ initially:
Suppose first that $w_1 = 0$, $w_2 = 1$, $w_3 = \infty$.
Then $f(z) = \frac{(z_2 - z_3)(z - z_1)}{(z_2 - z_1)(z - z_3)}$ satisfies $f(z_i) = w_i \forall i$.
Special cases:

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

Thus can find f_1 sending (z_1, z_2, z_3) to $(0, 1, \infty)$
and f_1 sending (w_1, w_2, w_3) to $(0, 1, \infty)$
Then $f = f_2^{-1} f_1$ will send (z_1, z_2, z_3) to (w_1, w_2, w_3) as required ($f \in \mathcal{M}$ since $\mathcal{M}$ is a group).
Uniqueness follows from previous corollary.

Theorem. Every non-identity $f \in \mathcal{M}$ has 1 or 2 fixed points. If f has 1 fixed point, then it is conjugate to $x \mapsto z + 1$.
If f has 2 fixed points, then it's conjugate to a map of the form $z \mapsto az$, for some $a \in \mathbb{C} \backslash \{0\}$

Proof. Have if $f \neq$ id. then f has ≤ 2 fixed points.
If $f(z) = \frac{az+b}{cz+d}$, by considering the quadratic: $cz^2 + (d - a)z - b = 0$ (arising from $f(z) = z$) which must have ≥ 1 solutions, we see there's at least one fixed point.

- If f has exactly 1 fixed point z_0, choose $z_1 \in \mathbb{C}$ not fixed by f.
  Then $(z_1, f(z_1), z_0)$ are all distinct (easy check) so there is $g \in \mathcal{M}$ s.t. $(z_1, f(z_1), z_0) \mapsto (0, 1, \infty)$
  Consider gfg^{-1}. We have:
  $$\begin{aligned} gfg^{-1} : 0 &\mapsto z_1 \mapsto f(z_1) \mapsto 1 \\ \infty &\mapsto z_0 \mapsto z_0 \mapsto \infty \end{aligned}$$
  So $gfg^{-1}(0) = 1$, $gfg^{-1}(\infty) = \infty$, so gfg^{-1} must be equal to $z \mapsto az + 1$ ($a \in \mathbb{C}$) (trivial check)
  If $a \neq 1$, then this has $\frac{1}{1-a} \neq \infty$ as a fixed point. ※since ∞ must be the only fixed point of gfg^{-1} as same number fixed points as f.
  So $a = 1$, and then f conjugate (via g) to $z \mapsto z + 1$
- If f has exactly 2 fixed points: let g be any Möbius map sending $(z_0, z_1) \mapsto (0, \infty)$ So
  $$\begin{aligned} gfg^{-1} : 0 &\mapsto z_0 \mapsto z_0 \mapsto 0 \\ \infty &\mapsto z_1 \mapsto z_1 \mapsto \infty \end{aligned}$$
  So gfg^{-1} fixes 0 and ∞ so must have the form $z \mapsto az$ where $a = gfg^{-1}(1)$ (trivial check)

Remark. We can use this to efficiently work out f^n for $f \in \mathcal{M}$

Note. Equation of circle in $\mathbb{C}$ center $b \in \mathbb{C}$, radius $r > 0$:

$$|z - b| = r \iff z\overline{z} - \overline{b}z - b\overline{z} + b\overline{b} - r^2 = 0$$

Equation of a straight line in $\mathbb{C}$:

$$a\text{Re}(z) + b\text{Im}(z) = c \iff \overline{\frac{a+ib}{2}}z + \frac{a+ib}{2}\overline{z} - c = 0$$

Under stereographic projection to the Reimann sphere, lines can also be considered circle

Definition. A **circle** in $\hat{\mathbb{C}}$ is the set of points satisfying the equation

$$Az\overline{z} + \overline{B}z + B\overline{z} + C = 0$$

with $A, C \in \mathbb{R}$, $B \in \mathbb{C}$, and $|B|^2 > AC$.
We consider $\infty \in \hat{\mathbb{C}}$ to be a solution $\iff A = 0$

Note. Can show the set of points satisfying such an equation is always either circle in $\mathbb{C}$ or line$\cup\{\infty\}$

Theorem. Möbius maps send circles in $\hat{\mathbb{C}}$ to circles in $\hat{\mathbb{C}}$

Proof. Since $\mathcal{M}$ generated by $z \mapsto az$, $z \mapsto z + b$, $z \mapsto \frac{1}{z}$, it suffices to check for these maps. Writing $S(A, B, C)$ for the circle satisfying

$$Az\overline{z} + \overline{B}z + B\overline{z} + C = 0 \tag{1}$$

Can check that under $z \mapsto az$:

$$S(A, B, C) \mapsto S(\frac{A}{\overline{a}a}, \frac{B}{\overline{a}}, C)$$

under $z \mapsto z + b$:

$$S(A, B, C) \mapsto S(A, B - Ab, C + Ab\overline{b} - B\overline{b} - \overline{B}b)$$

under $z \mapsto \frac{1}{z}$:
solutions to (1) becomes solutions to $Cw\overline{w} + Bw + \overline{B}\overline{w} + A = 0$ so:

$$S(A, B, C) \mapsto S(C, \overline{B}, A)$$

Remark. A circle is determined by 3 points on it, and a Möbius map determined by where it sends 3 points so easy to find a Möbius map sending a given circle to another circle (just consider 3 points on each and find map between them)

6.2 Cross-Ratios

Definition. If $z_1, z_2, z_3, z_4 \in \hat{\mathbb{C}}$ distinct, then their **cross-ratio** $[z_1, z_2, z_3, z_4]$ is defined to be $f(z_4)$ where $f \in \mathcal{M}$ is the unique Möbius map s.t.

$$f(z_1) = 0,\ f(z_2) = 1,\ f(z_3) = \infty$$

Note. $[0, 1, \infty, w] = w\ \forall w \in \hat{\mathbb{C}} \backslash \{0, 1, \infty\}$

Equation. We have the following formula for computing the cross-ratio:

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

With special cases interpreted accordingly when $z_i = \infty$ for some i e.g.

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

This formula follows from the proof that we have unique Möbius map sending any 3 distinct points to 3 distinct points.

Prop. Double transpositions of the z_i fix the cross-ratio, i.e.

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

Proof. By inspection of formula

Theorem. Möbius maps preserve the cross-ratio, i.e. $\forall g \in \mathcal{M}$, $\forall z_1, z_2, z_3, z_4 \in \hat{\mathbb{C}}$ distinct,

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

Proof. Consider $f : (z_1, z_2, z_3) \mapsto (0, 1, \infty)$.
Then consider fg^{-1} acting on the $g(z_i)$ to show:

$$\begin{aligned} [g(z_1), g(z_2), g(z_3), g(z_4)] &= (f \circ g^{-1})(g(z_4)) \\ &= f(z_4) \\ &= [z_1, z_2, z_3, z_4] \end{aligned}$$

Note. This leads onto a nice geometric corollary:

Corollary. Four distinct points $z_1, z_2, z_3, z_4 \in \hat{\mathbb{C}}$ lie on a circle iff $[z_1, z_2, z_3, z_4] \in \mathbb{R}$

Proof. Consider $f : (z_1, z_2, z_3) \mapsto (0, 1, \infty)$. Since circles sent to circles, all points on circle sent to real axis.

7 Matrix Groups

7.1 Basic Definitions

Definition. $GL_n(\mathbb{F}) = \{A \in M_{n\times n}(\mathbb{F}) : A \text{ is invertible}\}$ is the **general linear group** over $\mathbb{F}$

Note. $\det : GL_n(\mathbb{F} \to \mathbb{F}^*$ is a surjective homomorphism

Definition. The **special linear group**, $SL_n(\mathbb{F}) \leq GL_n(\mathbb{F})$ is the kernel of the det homomorphism.

Definition. $O_n = O_n(\mathbb{R}) = \{A \in GL_n(\mathbb{R}) : A^T A = I\}$ is the **orthogonal group**.

Note. Can check axioms to show indeed subgroup of $GL_n(\mathbb{R})$

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

Proof. If $A \in O_n$, then $A^T A = I$. Can reason from there using properties of determinant.

Definition. The **special orthogonal group** $SO_n = SO_n(\mathbb{R})$ is the kernel of the det homomorphism, i.e.

$$SO_n = \{A \in O_n : \det A = 1\}$$

7.2 Möbius maps via matrices

Prop. The function $\varphi : SL_2(\mathbb{C}) \to \mathcal{M}$
$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto f$ where $f(z) = \frac{az+b}{cz+d}$ is a surjective homomorphism with kernel $\{I, -I\}$

Proof. Homomorphism: check works M_1 and M_2
Surjective: show every map has corresponding matrix
Kernel: $b = c = 0$ considering 0 and ∞. $a = d$ considering 1 so have $\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$
Considering determinant gives desired kernel

Corollary.

$$\mathcal{M} \cong SL_2(\mathbb{C})/\{I, -I\}$$

Proof. By 1[st] isomorphism theorem

Remark. Quotient $SL_2(\mathbb{C})/\{I, -I\}$ known as the projective special linear group $PSL_2(\mathbb{C})$

7.3 Change of Basis

Remark. Representing the same linear map with respect to 2 different bases gives 2 matrices A and B where $B = P^{-1}AP$, some matrix P, the change of basis matrix.

Prop. $GL_n(\mathbb{F})$ acts on $M_{n\times n}(\mathbb{F})$ by conjugation. The orbit of a matrix $A \in M_{n\times n}(\mathbb{F})$ is the set of matrices representing the same linear map A wrt different bases.

Proof. Can check satisfies definition of an action trivially.
A and B in the same orbit
$\iff A = PBP^{-1}$ for some $P \in GL_n(\mathbb{F})$
$\iff B = P^{-1}AP\,(P \in GL_n(\mathbb{F}))$
$\iff$ B represents the same linear map as A but wrt the basis obtained via the change of basis corresponding to P

Note. From V& M, have every matrix in $M_{2\times 2}(\mathbb{C})$ is conjugate to a matrix in Jordan Normal Form i.e. to one of the following types of matrix:

$$\begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix} (\lambda_1 \neq \lambda_2), \begin{bmatrix} \lambda & 0 \\ 0 & \lambda \end{bmatrix}, \text{ or } \begin{bmatrix} \lambda & 1 \\ 0 & \lambda \end{bmatrix}$$

See vectors and matrices notes for which form any given matrix conjugate to. No 2 matrices above are conjugate to one another (except swapping λ_1, λ_2 from $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix} \begin{bmatrix} 0 & \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} \lambda_2 & 0 \\ 0 & \lambda_1 \end{bmatrix}$

Prop. $P \in O_n \iff$ the columns of P form an orthonormal basis.

Proof. Have

$$(P^TP)_{ij} = \mathbf{p}_i^T\mathbf{p}_j = \mathbf{p}_i \cdot \mathbf{p}_j$$

Hence $P \in O_n \iff P^TP = \delta_{ij} \iff \mathbf{p}_i \cdot \mathbf{p}_j = \delta_{ij} \iff$ the columns of P form an orthonormal basis.

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

Proof. $\implies$:

$$P\mathbf{x} \cdot P\mathbf{y} = (P\mathbf{x})^T(P\mathbf{y}) = \mathbf{x}^T P^T P\mathbf{y} = \mathbf{x}^T I\mathbf{y} = \mathbf{x}^T\mathbf{y} = \mathbf{x} \cdot \mathbf{y}$$

$\impliedby$:
If $P\mathbf{x} \cdot P\mathbf{y} = \mathbf{x} \cdot \mathbf{y}\, \forall \mathbf{x}, \mathbf{y} \in \mathbb{R}^n$, then taking the standard basis $\mathbf{e}_i, \mathbf{e}_j$ we have:

$$P\mathbf{e}_i \cdot P\mathbf{e}_j = \mathbf{e}_i \cdot \mathbf{e}_j = \delta_{ij}$$

So the vectors $P\mathbf{e}_1, \dots, P\mathbf{e}_n$ are orthonormal.
These are the columns of P, so $P \in O_n$ by previous prop.

Corollary. For $P \in O_n$, $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$, we have:

i) $|P\mathbf{x}| = |\mathbf{x}|$
ii) $P\mathbf{x}\angle P\mathbf{y} = \mathbf{x}\angle\mathbf{y}$ (angle)

Proof.

i) Follows from previous prop, taking $\mathbf{y} = \mathbf{x}$
ii) Angles defined using inner product,

$$\cos(\mathbf{x}\angle\mathbf{y}) = \frac{\mathbf{x} \cdot \mathbf{y}}{|\mathbf{x}||\mathbf{y}|} = \frac{P\mathbf{x} \cdot P\mathbf{y}}{|P\mathbf{x}||P\mathbf{y}|} = \cos(P\mathbf{x}\angle P\mathbf{y})$$

Since $\cos : [0, \pi] \to [-1, 1]$ is injective, $\mathbf{x}\angle\mathbf{y} = P\mathbf{x}\angle P\mathbf{y}$.

Definition. If $\mathbf{a} \in \mathbb{R}^n$ with $|\mathbf{a}| = 1$, then the **reflection in the plane normal to a** is the linear map:

$$R_{\mathbf{a}} : \mathbb{R}^n \to \mathbb{R}^n$$

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

Lemma. $R_{\mathbf{a}}$ lies in O_n

Proof. Show by showing $R_{\mathbf{a}}(\mathbf{x}) \cdot R_{\mathbf{a}}(\mathbf{y}) = \mathbf{x} \cdot \mathbf{y}$

Lemma. Given $P \in O_n$, $PR_{\mathbf{a}}P^{-1} = R_{P\mathbf{a}}$

Proof.

$$\begin{aligned} PR_{\mathbf{a}}P^{-1}(\mathbf{x}) &= P(P^{-1}(\mathbf{x}) - 2(P^{-1}(\mathbf{x}) \cdot \mathbf{a})\mathbf{a}) \\ &= \mathbf{x} - 2(P^{-1}(\mathbf{x}) \cdot \mathbf{a})(P\mathbf{a}) \end{aligned}$$

But $P^{-1} = P^T$ and $(P^T(\mathbf{x}) \cdot \mathbf{a}) = \mathbf{x}^T P\mathbf{a} = \mathbf{x} \cdot P\mathbf{a}$
So $PR_{\mathbf{a}}P^{-1} = \mathbf{x} - 2(\mathbf{x} \cdot P\mathbf{a})(P\mathbf{a})$
So $PR_{\mathbf{a}}P^{-1} = R_{P\mathbf{a}}$ as desired

Prop.

$$R_{\mathbf{a}} \in O_n \backslash S_n$$

Proof. Have $\det R_{\mathbf{a}}$ is the product of evals, evals are -1 and 1 (multiplicity $n-1$)

Theorem. Every element of SO_2 is of the form $\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$ for some $\theta \in [0, 2\pi)$ and conversely, every such element lies in SO_2.

Proof. Have $A^T = A^-1$ which leads us to $a = d$, $b = -c$.
Determinant $\implies a^2 + c^2 = 1$ so let $a = \cos\theta$, $c = \sin\theta$ for unique $\theta \in [0, 2\pi)$. Conversely, have determinant of such matrix is 1 and it is in O_2 (orthogonal columns) so in SO_2

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

Proof. Have $A^T = A^{-1}$ which leads us to $a = -d$, $b = c$.
Determinant $\implies a^2 + c^2 = 1$ so let $a = \cos\theta$, $c = \sin\theta$ for unique $\theta \in [0, 2\pi)$.
Can check $A \begin{bmatrix} \sin\frac{\theta}{2} \\ -\cos\frac{\theta}{2} \end{bmatrix} = -\begin{bmatrix} \sin\frac{\theta}{2} \\ -\cos\frac{\theta}{2} \end{bmatrix}$ and $A \begin{bmatrix} \cos\frac{\theta}{2} \\ \sin\frac{\theta}{2} \end{bmatrix} = \begin{bmatrix} \cos\frac{\theta}{2} \\ \sin\frac{\theta}{2} \end{bmatrix}$
So A is the reflection in the plane orthogonal to the unit vector: $\begin{bmatrix} \sin\frac{\theta}{2} \\ -\cos\frac{\theta}{2} \end{bmatrix}$
Conversely, any reflection in a line through the origin will have this form, so in $O_2 \backslash SO_2$

Corollary. Every element of O_2 is the composition of at most two reflections.

Proof. If A has determinant -1 then is a reflection.
Else $A = A \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$, which is product of 2 reflections.

Theorem. If $A \in SO_3$, then $\exists \mathbf{v} \in \mathbb{R}^3$ s.t. $|\mathbf{v}| = 1$ and $A\mathbf{v} = \mathbf{v}$

Proof. Suffices to show 1 is an eval.
Have $\det(A - I) = \det\left(A - AA^T\right)$ which leads to $\det(A - I) = \det(I - A)$ which leads to $\det(A - I) = -\det(A - I)$
So $\det(A - I) = 0$ as required.
(Then normalise an evec to get $\mathbf{v}$ with $|\mathbf{v}| = 1$)

Corollary. Every $A \in SO_3$ is conjugate (in SO_3) to a matrix of the form:

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

Proof. From previous theorem, have a $\mathbf{v}_1$ which maps to itself. Now extend to orthonormal basis and consider dot products of form $A\mathbf{v}_i \cdot A\mathbf{v}_1$ to show $A\mathbf{v}_2$ and $A\mathbf{v}_3$ lie in $\langle \mathbf{v}_2, \mathbf{v}_3 \rangle$.
So A maps $\langle \mathbf{v}_2, \mathbf{v}_3 \rangle$ to itself. Thus consider restriction of A to $\langle \mathbf{v}_2, \mathbf{v}_3 \rangle$. The 2×2 matrix still has determinant 1 since A will be a matrix of form:

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & a & b \\ 0 & c & d \end{bmatrix}$$

so $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ must be of form $\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$ from a previous theorem.
Indeed $P \in O_3$ since $\{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$ an orthonormal basis.
If $P \notin SO_3$, then can use basis $\{-\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$ instead.

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

Proof. If $A \in SO_3$, we have $\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$ is a composition of at most 2 reflections. Thus so is B where:

$$PAP^{-1} = B = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{bmatrix}$$

Let $B = B_1B_2$, product of reflections.
Then we have $A = PBP^{-1} = (PB_1P^{-1})(PB_2P^{-1})$ And the conjugate of a reflection is a reflection.
If $\det A = -1$ then let:

$$A = A \begin{bmatrix} -1 & & \\ & 1 & \\ & & 1 \end{bmatrix} \cdot \begin{bmatrix} -1 & & \\ & 1 & \\ & & 1 \end{bmatrix}$$

First product has determinant 1, second product is reflection in $y - z$ plane so ≤ 3 reflections total as desired.

7.4 Symmetries of the cube revisited

Can think of the symmetries of the cube as a subgroup of O_3.
Have $O_3 \cong SO_3 \times C_2$ (example sheet 4, but can show using direct products)
Where $\mathbf{v} \mapsto -\mathbf{v}$ generates C_2. So if $\mathbf{v} \mapsto -\mathbf{v}$ a symmetry of our platonic solid, then its group of symmetries will also split as the direct product $G^+ \times C_2$ (can show by direct product)
So we have that the symmetry group of the cube is $G^+ \times C_2 \cong S_4 \times C_2$ by results from section 5.

8 Groups of Order 8

Definition. The set $\{\pm\mathbf{1}, \pm\mathbf{i}, \pm\mathbf{j}, \pm\mathbf{k}\}$ forms a group called the **Quaternions**, Q_8. Where:

$$\mathbf{1} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \mathbf{i} = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \mathbf{j} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \mathbf{k} = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$$

Note. Can check:

- $g^4 = \mathbf{1} \, \forall g \in Q_8$
- $(-\mathbf{1})^2 = \mathbf{1}$
- $\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -\mathbf{1}$
- $\mathbf{i} \cdot \mathbf{j} = \mathbf{k}$, $\mathbf{j} \cdot \mathbf{k} = \mathbf{i}$, $\mathbf{k} \cdot \mathbf{i} = \mathbf{j}$
- $\mathbf{j} \cdot \mathbf{i} = -\mathbf{k}$, $\mathbf{k} \cdot \mathbf{j} = -\mathbf{i}$, $\mathbf{i} \cdot \mathbf{k} = -\mathbf{j}$

Lemma. If a finite group has all non-identity elements of order 2, then it is isomorphic to $C_2 \times C_2 \times \cdots \times C_2$

Proof. Can easily show such a G must be abelian ($ghg^{-1}h^{-1} = ghgh = e$) and that $|G| = 2^n$ (Cauchy)
If $|G| = 2$, $G \cong C_2$
If $|G| > 2$, then chose a_2 order 2 in G and $a_2 \notin \langle a_1 \rangle$ and show $\langle a_1, a_2 \rangle \cong \langle a_1 \rangle \times \langle a_2 \rangle \cong C_2 \times C_2$.
Continue in this was taking $a_3, \ldots$ until we have all $|\langle a_1, a_2, \ldots, a_k \rangle| = 2^k = |G|$

Theorem. A group of order 8 is isomorphic to (exactly) one of:

$$C_8,\ C_4 \times C_2,\ C_2 \times C_2 \times C_2,\ D_8 \text{ or } Q_8$$

Proof. Firstly, groups are not isomorphic. Abelian ones differ in maximal order of element. Only 1 element order 2 in Q_8 but 4 such in D_8.

(i) Order of elements divide 8 so order of any element is 1, 2, 4 or 8

(ii) Consider first if element order 8, leads to $G \cong C_8$

(iii) Else if all non-identity order 2, then $G \cong C_2 \times C_2 \times C_2$

(iv) Remaining groups have element h order 4 so $\langle h \rangle \trianglelefteq G$ (index 2)

(v) for $g \notin \langle h \rangle$, $g^2 \in \langle h \rangle$ (consider map to $g\langle h \rangle$)

(vi) $g^2 = h$ or $g^2 = h^3$ leads to g order 8 ※

(vii) If $g^2 = e$, $ghg^{-1} \in \langle h \rangle$ (normal) and must be order 4.
- If $ghg^{-1} = h$, have direct product $C_4 \times C_2$
- If $ghg^{-1} = h^{-1}$, recognise as D_8

(viii) If $g^2 = h^2$ (note does NOT mean $g = h$), still have $ghg^{-1} = h$ or h^3
- If $ghg^{-1} = h$, have gh order 2 so have direct product $\langle h \rangle \times \langle gh \rangle \cong C_4 \times C_2$
- If $ghg^{-1} = h^{-1}$, define homomorphism:
  $e \mapsto \mathbf{1}$
  $h \mapsto \mathbf{i}$
  $g \mapsto \mathbf{j}$
  $gh \mapsto \mathbf{k}$
  And powers defined from these. Clearly φ bijective, and can check its a homom. so φ an isomorphism, so $G \cong Q_8$.

Remark. Q_8 has all subgroups normal but is not abelian.