Higher Algebra

Jeremy Le — UNSW MATH3711 25T1

Contents

Part I

Group Theory

1 The Mathematical Language of Symmetry

Definition 1.1 (Isometry)**.** A function $f : \mathbb{R}^n \to \mathbb{R}^n$ is an isometry if $\|f(x) - f(y)\| = \|x - y\|$ for all $x, y \in \mathbb{R}^n$. i.e. preserves distances.

Definition 1.2 (Symmetry)**.** Let $F \subseteq \mathbb{R}^n$, a symmetry of F is a (surjective) isometry $T : \mathbb{R}^n \to \mathbb{R}^n$ such that $T(F) = F$.

Properties 1.3. Let S, T be symmetries of $F \subseteq \mathbb{R}^n$. Then $S \cdot T : \mathbb{R}^n \to \mathbb{R}^n$ is also a symmetry of F.

Proof. Given $x, y \in \mathbb{R}^n$.

$$\begin{aligned} \|STx - STy\| &= \|Tx - Ty\| && (S \text{ is an isometry}) \\ &= \|x - y\|. && (T \text{ is an isometry}) \end{aligned}$$

Therefore ST is an isometry. Clearly ST is surjective as both S and T are surjective. Also,

$$\begin{aligned} ST(F) &= S(F) && (T(F) = F) \\ &= F. && (S(F) = F) \end{aligned}$$

So ST is a symmetry of F.

Properties 1.4. If $G =$ set of symmetries of $F \subseteq \mathbb{R}^n$, then G satisfies:

i) Composition is associative, $ST(R) = S(TR)$ for all $S, T, R \in G$.

ii) $\mathrm{id}_{\mathbb{R}^n} \in G \quad (\mathrm{id}_{\mathbb{R}^n}(x) = x \quad$ for all $x \in \mathbb{R}^n)$. Also, $\mathrm{id}_G T = T$ and $T \,\mathrm{id}_G = T$ for all $T \in G$.

iii) If $T \in G$, then T is bijective and $T^{-1} \in G$.

Proof. If $Tx = Ty$, then $\|Tx - Ty\| = 0$. So $\|x - y\| = 0, x = y$, therefore T is injective. By definition T is surjective, hence, T is bijective and therefore T^{-1} is surjective.

To prove T^{-1} is an isometry.

$$\begin{aligned} \left\|T^{-1}x - T^{-1}y\right\| &= \left\|TT^{-1}x - TT^{-1}y\right\| \\ &= \|\mathrm{id}\, x - \mathrm{id}\, y\| \\ &= \|x - y\|. \end{aligned}$$

To prove symmetry, $T^{-1}F = F$:

$$T^{-1}F = T^{-1}(T(F)) = F.$$

Thus $T^{-1} \in G$.

Definition 1.5 (Group)**.** A group is a set G equipped with a "multiplication map" $\mu : G \times G \to G$ such that

1) Associativity: $(gh)k = g(hk)$ for all $g, h, j \in G$.
2) Existence of identity: There exists $1 \in G$ such that $1g = g$ and $g1 = g$ for all $g \in G$.
3) Existence of inverses: $\forall g \in G,$ there exists $h \in G$ such that $gh = 1$ and $hg = 1$. Denoted by g^{-1}.

Properties 1.6. Basic facts about groups.

- "**Generalised Associativity**". When multiplying three or more elements, the bracketing does not matter. E.g. $(a(b(cd)))e = (ab)(c(de))$.

  Proof. Mathematical Induction as for matrix multiplication.

- **Cancellation Law**. If $gh = gk$ then $h = k$ for all $g, h, k \in G$.

  Proof. $gh = gk \implies g^{-1}(gh) = g^{-1}(gk) \implies (g^{-1}g)h = (g^{-1}g)k \implies 1h = 1k \implies h = k$.

2 Matrix Groups and Subgroups

Recall $\mathrm{GL}_n(\mathbb{R})$ and $GL_n(\mathbb{C})$ which represent the set of real/complex invertible $n \times n$ matrices.

Proposition 2.1. $\mathrm{GL}_n(\mathbb{R})$ and $GL_n(\mathbb{C})$ are groups when endowed with matrix multiplication.

Proof. Product of real invertible matrices is in $\mathrm{GL}_n(\mathbb{R})$.

i) matrix multiplication is associative.
ii) identity matrix $I_n : I_n m = m$ and $mI_n = m$ for all $m \in \mathrm{GL}_n(\mathbb{R})$
iii) if $m \in \mathrm{GL}_n(\mathbb{R})$ then m^{-1}. $mm^{-1} = I$ and $m^{-1}m = I$.

Proposition 2.2. Let $G =$ group.

1) Identity is unique i.e. suppose $1, e$ are both identities then $1 = e$.

   Proof. $1 = 1 \cdot e = e$.

2) Inverses are unique.

   Proof. If $g \in G, gh = hg = 1$ and $gk = kg = 1$ then $h = k$.

3) For $g, h \in G$ we have $(gh)^{-1} = h^{-1}g^{-1}$.

   Proof. $(gh)(h^{-1}g^{-1}) = ghh^{-1}g^{-1} = g1g^{-1} = gg^{-1} = 1$. Similarly, $(h^{-1}g^{-1}(gh) = 1)$.

Definition 2.3 (Subgroup)**.** Let G be a group with multiplication μ. A subset $H \subseteq G$ is called a subgroup of G (denoted $H \leq G$) if it satisfies:

i) $1_G \in H$ (contains identity),

ii) if $g, h \in H$ then $gh \in H$ (closed under multiplication),

iii) if $g \in H$ then $g^{-1} \in H$ (closed under inverse).

Proposition 2.4. H is a group with the induced multiplication map $\mu_H : H \times H \to H$ by $\mu_H(g, h) = \mu(g, h)$.

Proof. (ii) tells us that μ_H makes sense. μ_H is associative because μ is. H has an identity from (i). H has inverses from (iii).

Proposition 2.5. Set of orthogonal matrices $O_n(\mathbb{R}) = \{M \in \mathrm{GL}_n(\mathbb{R}) : M^T = M^{-1}\} \leq \mathrm{GL}_n(\mathbb{R})$ forms a group. Namely the set of symmetries of an $n-1$ sphere, i.e. an n dimensional circle.

Proof. Check axioms.

i) $I_n \in O_n(\mathbb{R})$

ii) If $M, N \in O_n(\mathbb{R})$ then $(MN)^T = N^T M^T = N^{-1}M^{-1} = (MN)^{-1}$, so $MN \in O_n(\mathbb{R})$.

iii) If $M \in O_n(\mathbb{R})$ then $(M^{-1})^T = (M^T)^{-1} = (M^{-1})^{-1}$ so $M^{-1} \in O_n(\mathbb{R})$.

Proposition 2.6. Basic subgroup facts.

i) Any group G has two trivial subgroups: itself and $1 = \{1_G\}$.

ii) If $J \leq H$ and $H \leq G$ then $J \leq G$.

Here are some notations. For $g \in G$ where G is a group.

i) If n positive integer, define $g^n = g \cdot g \cdots g$ (n times)

ii) $g^0 = 1$

iii) n positive: $g^{-n} = (g^{-1})^n$ or $(g^n)^{-1}$.

iv) For $m, n \in \mathbb{Z}$, $g^m \cdot g^n = g^{m+n}$ and $(g^m)^n = g^{mn}$.

Definition 2.7. The order of a group G, denoted $|G|$ is the cardinality of G. For $g \in G$, the order of g is the smallest positive integer n such that $g^n = 1$. If no such integer exists, order is ∞.

3 Permutation Groups

Definition 3.1 (Permutations)**.** Let S be a set. Let $\mathrm{Perm}(S)$ be the set of permutations of S. This is the set of bijections of form $\sigma : S \to S$.

Proposition 3.2. $\mathrm{Perm}(S)$ is a group when endowed with composition of functions.

Proof. Composition of bijections is a bijection. The identity is id_S and group inverse is the inverse function.

Definition 3.3 (Symmetric Group)**.** Let $S = \{1, \ldots, n\}$. The symmetric group S_n is $\mathrm{Perm}(S)$.

Two notations are used. With the two line notation, represent $\sigma \in S_n$ by

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix}$$

($\sigma(i)$'s are all distinct, hence σ is one to one and bijective). Note this shows $|S_n| = n!$.

With the cyclic notation, let $s_1, s_2, \ldots, s_k \in S$ be distinct. We define a new permutation $\sigma \in \mathrm{Perm}(S)$ by $\sigma(s_i) = s_{i+1}$ for $i = 1, 2, \ldots, k-1, \sigma(s_k) = \sigma(s_1)$ and $\sigma(s) = s$ for $s \notin \{s_1, s_2, \ldots, s_k\}$. Denoted $(s_1 s_2 \ldots s_k)$ and called a k-cycle.

Example 3.4. For $n = 4$,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} \in S_4 \quad \text{means} \quad \begin{matrix} \sigma(1) = 2, & \sigma(2) = 3 \\ \sigma(3) = 1, & \sigma(4) = 4. \end{matrix}$$

In cyclic notation this is $(123)(4)$ or (123) where the cycle is $1 \to 2 \to 3 \to 1$.

Note that a 1-cycle is the identity and the order of a k-cycle is k. So $\sigma^k = 1$ and $\sigma^{-1} = \sigma^{k-1}$.

Definition 3.5 (Disjoint Cycles)**.** Cycles $s_1 \ldots s_k$ and $t_1 \ldots t_k$ are disjoint if $\{s_1, \ldots, s_k\} \cup \{t_1, \ldots, t_k\} = \emptyset$.

Definition 3.6 (Commuativity)**.** In any group, two elements g, h commute if $gh = hg$.

Proposition 3.7. Disjoint cycles commute.

Proposition 3.8. Any permutation σ of a finite set S is a product of disjoint cycles.

Example 3.9. $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 6 & 1 & 5 & 3 \end{pmatrix} \in S_6$ does $1 \to 2 \to 4 \to 1$, $3 \to 6 \to 3$ and $5 \to 5$.
Thus $\sigma = (124)(36)$ since (5) is the identity.

Proposition 3.10. Let σ be a permutation of a finite set S. Then S is a disjoint union of subsets, say $S_1, \ldots, S_r$, such that σ permutes the elements of each S_i cyclically.

Definition 3.11 (Transposition)**.** A transposition is a $2-$cycle i.e. (ab).

Proposition 3.12. i) The k-cycle $(s_1 s_2 \ldots s_k) = (s_1 s_k)(s_1 s_{k-1}) \ldots (s_1 s_3)(s_1 s_2)$

Example 3.13. $(3625) = (35)(32)(36) = (36)(62)(25)$

Proof. The RHS produces the mapping below which is equivalent to the LHS.

$$\begin{aligned} s_1 &\to s_2 \\ s_2 &\to s_1 \to s_3 \\ s_3 &\to s_1 \to s_4 \\ &\vdots \\ s_{k-1} &\to s_1 \to s_k \\ s_k &\to s_1. \end{aligned}$$

ii) Any permutations in S_n is a product of transpositions.

Proof. We can write any $\sigma \in S_n$ as product of (disjoint) cycles. By part i), each cycle is a product of transpositions. So we can write σ as product of transpositions.

4 Generators and Dihedral Groups

Lemma 4.1. Let $\{H_i\}_{i\in I}$ be a (non-empty) collection of subgroups of G. Then $\bigcap_{i\in I} H_i \leq G$.

Proof.

1) Why is $1 \in \bigcap_{i\in I} H_i$? Because $1 \in H_i$ for all i.

2) Closed under multiplication? If $g, h \in \bigcap_{i\in I} H_i$, then $g, h \in H_i$ for all $i \implies gh \in H_i$ for all $i \implies gh \in_{i\in I} H_i$.

3) Closed under taking inverse? If $g \in \bigcap_{i\in I} H_i$ then $g \in H_i$ for all i as H_i are subgroups, every element has an inverse. So an inverse exists for all elements in H_i for all i.

Proposition - Definition 4.2. Let G be a group and $S \subseteq G$. Let $\mathcal{J}$ be the set of subgroups $J \leq G$ containing S.

i) [Definition] The subgroup generated by S, $\langle S\rangle$ is $\bigcap J \in \mathcal{J} \leq J \leq G$. i.e. it's the intersection of all subgroups of G containing S.

Proof. Lemma 4.1 implies $\langle S\rangle$ is a subgroup of G.

ii) [Proposition] $\langle S\rangle$ is the set of elements of the form $g = s_1 s_2 \dots s_n$ where $n \geq 0$ and $s_i \in S \cup S^{-1}$. Define $g = 1$ when $n = 0$.

Proof. Let $H = \{s_1 \dots s_n : s_i \in S \cup S^{-1}\}$. First, $H \subseteq \langle S\rangle$. Need to prove that $s_i \cdots s_n \in$ every J. Each $s_i \in J$ because $s_i = s$ or s^{-1} for some $s \in S \leq J$ and J closed under inversion. Therefore, $s_1 \dots s_n \in J$ by closure under multiplication. Hence $s_1 \dots s_n \in \bigcap_{J\in\mathcal{J}} J = \langle S\rangle$.

Second, $\langle S\rangle \subseteq H$. Need to prove H is a subgroup containing S. Closure under multiplication: $(s_1 \dots s_n)(t_1 \dots t_m) = s_1 \dots s_n t_1 \dots t_m$ also closure under inversion: $(s_1 \dots s_n)^{-1} = s_1^{-1} \dots s_n^{-1} \in H$ since $s_i^{-1} \in S$ for all i. Identity: $s, s^{-1} \in S \neq \emptyset \implies ss^{-1} = 1 \in H$.

Definition 4.3 (Finitely Generated)**.** A group G is finitely generated $f.g.$ if $G = \langle S\rangle$ for a finite subset $S \subseteq G$. G is cyclie if we can take $|S| = 1$.

Example 4.4. Take $G \in \mathrm{GL}_2(\mathbb{R})$ with $\sigma = \begin{pmatrix} \cos\left(\frac{2\pi}{n}\right) & -\sin\left(\frac{2\pi}{n}\right) \\ \sin\left(\frac{2\pi}{n}\right) & -\cos\left(\frac{2\pi}{n}\right) \end{pmatrix}$ and $\tau = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Find the subgroup generated by $\{\sigma, \tau\}$.

Notice both σ, τ are symmetries of any n-gon. Any element of $\langle \sigma, \tau\rangle$ has form

$$\sigma^{i_1}\tau^{j_1}\sigma^{i_2}\tau^{j_2}\dots\sigma^{i_r}\tau^{j_r} \quad \text{for } i_1, \dots, i_r, j_1, \dots, j_r \in \mathbb{Z}.$$

We have relations: $\sigma^n = 1, \tau^2 = 1$ and $\tau\sigma\tau^{-1} = \sigma^{-1}$. We use these relations to push all σ's to the left and all τ's to the right to achieve the form $\sigma^i\tau^j$ where $0 \leq i < n$ and $j = 0, 1$.

Proposition - Definition 4.5. $\langle \sigma, \tau \rangle$ = dihedral group of $2n$, denoted D_n (sometimes D_{2n}).

$$D_n = \{1, \sigma, \ldots, \sigma^{n-1}, \tau, \sigma\tau, \sigma^2\tau, \ldots, \sigma^{n-1}\tau\} \text{ and } |D_n| = 2n.$$

Proof. Need to show $2n$ elements are all distinct. $\det(\sigma^i) = 1$ (because $\det(\sigma) = 1$), $\det(\tau) = -1$ and $\det(\sigma^i\tau) = -1$. We conclude, $\{1, \sigma, \ldots, \sigma^{n-1}\} \cap \{\tau, \sigma\tau, \ldots, \sigma^{n-1}\tau\} = \emptyset$ because $\sigma^k = \begin{pmatrix} \cos\left(\frac{2k\pi}{n}\right) & -\sin\left(\frac{2k\pi}{n}\right) \\ \sin\left(\frac{2k\pi}{n}\right) & \cos\left(\frac{2k\pi}{n}\right) \end{pmatrix}$ are distinct. If $\sigma^i\tau = \sigma^j\tau$ then $\sigma^i = \sigma^j$ then $i = j$.

5 Alternating and Abelian Groups

Definition 5.1 (Symmetric Functions)**.** Let $f(x_1, \ldots, x_n)$ be a function of n variables. Let $\sigma \in S_n$. We define function $(\sigma f)(x_1, \ldots, x_n) = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$. We say that f is symmetric if $\sigma f = f$ for all $\sigma \in S_n$.

Example 5.2. Suppose $f(x_1, x_2, x_3) = x_1^3 x_2^2 x_3$ and $\sigma = (12)$ then $\sigma f(x_1, x_2, x_3) = x_2^3, x_1^2 x_3$. Not symmetric because $x_1^3 x_2^2 x_3 \neq x_2^3 x_1^2 x_3$. But $f(x_1, x_2) = x_1^2 x_2^2$ is symmetric in two variables.

Definition 5.3 (Difference Product)**.** The difference product in (n variables) is

$$\Delta(x_1, \ldots, x_n) = \Pi_{i<j}(x_i - x_j).$$

Lemma 5.4. Let $f(x_1, \ldots, x_n)$ be a function in n variables. Let $\sigma, \tau \in S_n$, then $(\sigma\tau) \cdot f = \sigma \cdot (\tau f)$.

Proof.

$$\begin{aligned}
(\sigma \cdot (\tau f))(x_1, \ldots, x_n) &= (\tau f)(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) && \text{(by definition)} \\
&= f(y_{\tau(1)}, \ldots, y_{\tau(n)}) && \text{(where } y_i = x_\sigma(i)) \\
&= f(x_{\sigma(\tau(1))}, \ldots, x_{\sigma(\tau(n))}) \\
&= f(x_{(\sigma\tau)(1)}, \ldots, x_{(\sigma\tau)(n)}) \\
&= ((\sigma\tau) \cdot f)(x_1, \ldots, x_n).
\end{aligned}$$

Note, the second and third step follows because $x_{\sigma(1)}$ is not necessarily x_1, so τ is applied to x_1 first, then σ can be applied.

Proposition - Definition 5.5. For $\sigma \in S_n$ write $\sigma = \tau_1\tau_2 \ldots \tau_m$ where τ_i are transpositions. Then

$$\sigma \cdot \Delta = \begin{cases} \Delta & \text{if } m \text{ even (call } \sigma \text{ an even permutation)} \\ -\Delta & \text{if } m \text{ odd (call } \sigma \text{ an odd permutation)} \end{cases}$$

Proof. Sufficent to prove for a single transposition (i.e. $m = 1$) because by the above Lemma,

$$\sigma\Delta = \tau_1(\tau_2 \ldots (\tau_{m-1}(\tau_m\Delta)) \ldots) = \tau_1((-1)^{m-1}\Delta) = (-1)^m\Delta.$$

Let's assume $\sigma = (ij), i < j$. There are 3 cases:

i) $x_i - x_j \implies x_j - x_i$ (factor of -1).

ii) $x_r - x_s$ where i, j, r, s all distinct $\implies x_r - x_s$ (factor of +1).

iii) $x_r - x_s$ where one of r, s is equal to i or j. There are several subcases:

(a) $r < i < j$: $x_r - x_i \implies x_r - x_j$ but also $x_r - x_j \implies x_r - x_i$, no change (factor of $+1$).

(b) $i < r < j$: $(x_i - x_r)(x_r - x_j) \implies (x_j - x_r)(x_r - x_i)$ (factor of $+1$).

(c) $i < j < r$: similar to (a) (factor of $+1$).

So only change in i). Multiplying the three cases together yields $\sigma \cdot \Delta = -\Delta$.

Corollary - Definition 5.6 (Alternating Group)**.** The alternating group (on n symbols) is

$$A_n = \{\sigma \in S_n : \sigma \text{ is even}\}.$$

This is a subgroup of S_n. Also A_n is generated by $\{\tau_1\tau_2 : \tau_1, \tau_2 \text{ are transposition}\}$.

Example 5.7. $A_3 = \{1, (123), (132)\}, S_3 \setminus A_3 = \{(12), (13), (23)\}. |A_n| = n!/2$ except for $n = 1, A_1 = S_1 = \{1\}$.

Definition 5.8 (Abelian Group)**.** A group G is abelian if any two elements commute.

In abelian groups, often switch to additive notation:

i) product $gh \implies g + h$

ii) identity $1 \implies 0$

iii) power $g^n \implies ng$

iv) inverse $g^-1 \implies -g$

This notation follows from $\mathbb{Z}$ endowed with addition which forms an abelian group.

6 Cosets and Lagrange's Theorem

Let $H \leq G$ be a subgroup. This will apply to all statements in this section unless mentioned otherwise.

Definition 6.1 (Coset)**.** A left coset of H in G is a set of the form $gH = \{gh : h \in H\} \subseteq G$ for some $g \in G$. The set of left cosets is denoted byt G/H.

Example 6.2. Let $H = A_n \leq S_n = G$ for $n \geq 2$. Let τ be any transposition. We claim that $\tau A_n = \{\text{odd permutations}\}$.

$\subseteq$: $\tau A_n = \{\tau\sigma : \sigma \text{ even}\}$, they are all odd.

$\supseteq$: Suppose σ is odd, then $\sigma = \tau \cdot (\tau^{-1}\sigma) \in \tau A_n$.

Theorem 6.3. Define a relation on $G : g \equiv g'$ if and only if $g \in g'H$. Then $\equiv$ is an equivalence relation, the equivalence classes are the left cosets. Therefore $G = \dot{\bigcup}_{i \in I} g_i H$ (disjoint union).

Proof.

i) Reflexive. i.e. $g \in gH$ for all $g \in G$. True because $1 \in H$.

ii) Symmetry. Suppose $g \in g'H$, need to prove $g' \in gH$. Since $g \in g'H$ we have $g = g'H$ for some $h \in H$. $g' = gh^{-1}$ so $g' \in gH$ (as $h^{-1} \in H$).

iii) Transitivity. Suppose $g \in g'H$ and $g' \in g''H$. Then $g = g'h$ and $g' = g''h'$ for $h, h' \in H$. Therefore $g = (g''h)h = g''(h'h) \in g''H$ from associativity and $h'h \in H$.

Thus $\equiv$ is an equivalence relation and G is a disjoint union of equivalence classes.

Note $1H = H$ is always a coset of G and the coset containing $g \in G$ is gH.

Example 6.4. $H = A_n \leq S_n = G$ cosets are exactly S_n and τS_n where $S_n = A_n \dot{\bigcup} \tau A_n$.

Definition 6.5 (Index)**.** The index of H in G is the number of left cosets, i.e. $|G/H|$. Denoted by $[G : H]$.

Lemma 6.6. Let $g \in G$. Then H and gH have the same cardinality.

Proof. Bijection, $H \to gH, h \mapsto gh$. Surjective and injective (multiply on lefy by g^{-1}).

Theorem 6.7 (Lagrange's Theorem)**.** Assume G finite. Then $|G| = |H|[G : H]$ i.e. $|G/H| = |G|/|H|$.

Proof. Using Lemma 6.6, we have:

$$G = \bigcup_{i=1}^{[G:H]} g_i H \quad \text{(disjoint union)} \implies |G| = \sum_{i=1}^{[G:H]} |g_i H| = \sum_{i=1}^{[G:H]} |H| = [G : H]|H|.$$

Example 6.8. $A_n \leq S_n$. $[S_n : A_n] = 2 \implies |S_n| = 2|A_n| \implies n! = 2 * n!/2$.

All above statements hold for right cosets which have form $Hg = \{hg : h \in H\}$ denoted $H \backslash G$. The number of left cosets are equal the number of right cosets.

7 Normal Subgroups and Quotient Groups

Let G = group and $J, K \subseteq G$. Define the subset product $JK = \{jk : j \in J, k \in K\}$.

Proposition 7.1. Let G = group.

i) If $J' \subseteq J \subseteq G$ and $K \subseteq G$ then $KJ' \subseteq KJ$.

ii) If $H \leq G$, then $HH = H(= H^2)$.

iii) For $J, K, L \subseteq G$ then $(JK)L = J(KL) = \{jkl : j \in J, k \in K, \ell \in L\}$

Proposition - Definition 7.2 (Normal Subgroup)**.** Let $N \leq G$. We say N is a normal subgroup of G and write $N \trianglelefteq G$ if any of the following equivalent conditions hold:

i) $gN = Ng$ for all $g \in G$.

ii) $g^{-1}Ng = N$ for all $g \in G$.

iii) $g^{-1}Ng \subseteq N$ for all $g \in G$

Proof. (i) $\iff$ (ii), multiply both sides on the left by g^{-1}. (ii) $\implies$ (iii) by definition. (iii) $\implies$ (ii), assume $g^{-1}Ng \subseteq N$ for all $g \in G$, apply this with $g^{-1} : (g^{-1})Ng^{-1} \subseteq N \implies N \subseteq g^{-1}Ng$. Therefore $g^{-1}Ng = N$.

Theorem - Definition 7.3 (Quotient Group)**.** Let $N \trianglelefteq G$. Then subset product is a well-defined multiplication map on G/N which makes G/N into a group, called the quotient group. Also:

i) $(gN)(g'N) = (gg')N$

ii) $1_{G/N} = N$

iii) $(gN)^{-1} = g^{-1}N$.

Proof. Why is this well-defined? Why is the product of 2 cosets another coset?

Take cosets $gN = \{g\}N$ and $g'N$. Calculate

$$\begin{aligned}
(gN)(g'N) &= g(Ng')N && \text{(associative)}\\
&= g(g'N)N && (N \trianglelefteq G)\\
&= (gg')(NN) && \text{(associative)}\\
&= gg'N && (N^2 = N)
\end{aligned}$$

This is a coset. Also proves (i). For (ii), $(gN)N = g(NN) = gN \implies N(gN) = (Ng)N = (gN)N = gN$, N is an identity. For (iii), $(g^{-1}N)(gN) = g^{-1}(Ng)N = g^{-1}(gN)N = (g^{-1}g)(NN) = 1 \cdot N = N$.

8 Group Homomorphisms

Definition 8.1 (Homomorphism)**.** Given groups G, H. A function $\phi : H \to G$ is a homomorphism of groups if $\phi(hh') = \phi(h)\phi(h')$ for all $h, h' \in H$.

Proposition - Definition 8.2 (Isomorphisms and Automorphisms)**.** Let $\phi : H \to G$ be a group homomorphism. The following are equivalent:

- There exists a group homomorphism, $\psi : G \to H$ such that $\psi\phi = \mathrm{id}_H$ and $= \phi\psi = \mathrm{id}_G$
- ϕ is bijective.

We call ϕ is a group isomorphism. If $H = G$, ϕ is an automorphism.

Proposition 8.3. If $\phi : H \to G, \psi : K \to H$ are group homomorphism then $\phi \cdot \psi : K \to G$ is a homomorphism.

Proof. $(\phi \cdot \psi)(kk') = \phi(\psi(kk')) = \phi(\psi(k)\psi(k')) = \phi(\psi(k))\phi(\psi(k'))$

Proposition 8.4. Let $\phi : H \to G$ be a group homomorphism.

i) $\phi(1_H) = 1_G$.

ii) $\phi(h^{-1}) = \phi(h)^{-1}$ for all $h \in H$.

iii) if $H' \leq H$ then $\phi(H') \leq G$.

Proposition - Definition 8.5. Let G be a group with $g \in G$. Conjugation by g is the map $C_g : G \to G; h \mapsto ghg^{-1}$. Then C_g is an automorphism with inverse $C_{g^{-1}}$.

Proof. C_g is a homomorphism: $C_g(h_1h_2) = C_g(h_1)C_g(h_2)$. Check: $C_g(h_1h_2) = gh_1h_2g^{-1} = gh_1g^{-1}gh_2g^{-1} = C_g(h_1)C_g(h_2)$. Now check $C_{g^{-1}}$ is an inverse. $C_{g^{-1}}(C_g(h)) = C_{g^{-1}}(ghg^{-1}) = g^{-1}ghg^{-1}g = h$. Similarly $C_g(C_{g^{-1}})(h) = h$, therefore $(C_g)^{-1} = C_{g^{-1}}$.

Corollary - Definition 8.6. For $H \leq G$, a conjugate of H (in G) is a subgroup of G of the form $gHg^{-1} := c_g(H)$.

Definition 8.7 (Epimorphism and Monomorphism)**.** Let $\phi : H \to G$ be a group homomorphism. ϕ is an epimorphism if ϕ is surjective. ϕ is a monomorphism if ϕ is injective.

Example 8.8. Linear map $T : V \to W$ where V and W are vector spaces. Suppose T is a projection onto some subspace. What does $T^{-1}(w) = \{v \in V : T(v) = w\}$ looks like, for a given $w \in W$?

If $w \in L$, $T^{-1}(w) = \emptyset$
If $w \in L, T^{-1}(w) =$ plane containing w, orthogonal to $L = w + K$ where $K =$ kernel of $T = T^{-1}(0)$.

Definition 8.9. Let $\phi : H \to G$ be a group homomorphism. The kernel of ϕ is

$$\ker \phi = \phi^{-1}(1_G) = \{h \in H : \phi(h) = 1_G\}$$

Proposition 8.10. Let $\phi : H \to G$ be a group homomorphism.

i) If $G' \leq G$ then $\phi^{-1}(G') \leq H$.

ii) If $G' \trianglelefteq G$ then $\phi^{-1}(G') \trianglelefteq H$.

Proof. (Normality) Given $h \in \phi^{-1}(G')$ and$g \in H$. We need to prove $ghg^{-1} \in \phi^{-1}(G') \implies \phi(ghg^{-1}) \in G \implies \phi(g)\phi(h)\phi(g)^{-1} \in G$ true because $\phi(h) \in G'$ and $G' \trianglelefteq G$.

iii) $K = \ker \phi \trianglelefteq H$.

Proof. Follows from (ii) because $K = \phi^{-1}(\{1\})$ and $\{1\} \trianglelefteq G$.

iv) The non-empty fibres of ϕ, i.e. $\phi^{-1}(g)$ for all $g \in G$, are exactly the cosets of H.

Proof. Suppose $g \in G$, consider $\phi^{-1}(g)$. Assume $\phi^{-1}(g) \neq \phi$. Let $h \in \phi^{-1}(g)$.

Claim. $\phi^{-1}(g) = hK$.
Proof. $hK \subseteq \phi^{-1}(g)$ because $\phi(hK) = \phi(h)\phi(j) = g \cdot 1 = g$.
Converse: $\phi^{-1}(g) \subseteq hK$. Let $h' \in \phi^{-1}(g)$. Then $\phi(h') = g$, also $\phi(h) = g$. Therefore $\phi(h'h^{-1}) = \phi(gg^{-1}) = \phi(1) = 1$. So $h'h^{-1} \in K, h' \in Kh = hK$, thus $\phi^{-1}(g) = hK$.

v) ϕ is one to one if and only if $K = \{1\}$.

Proof. ($\implies$) trivial. ($\impliedby$) Assume $K = \{1\}$. By part (iv) fibres $\phi^{-1}(g)$ are cosets of $\{1\}$ hence contain single element.

Proposition - Definition 8.11. Let $N \trianglelefteq G$. The quotient monomorphism (of G by N) is the map $\pi : G \to G/N; g \mapsto gN$. Its an epimorphism with kernel N.

9 First Group Isomorphism Theorem

Theorem 9.1. Let $N \trianglelefteq G$ and $\pi : G \to G/N$ be quotient map. Suppose $\phi : G \to H$ is a homomorphism such that $N \leq \ker \phi$.

i) If $g, g' \in G$ lie in the same coset of N, i.e. $gN = g'N$, then $\phi(g) = \phi(g')$.

ii) The map $\psi : G/N \to H; gN \mapsto \phi(g)$ is a homomorphism (the induced homomorphism).

iii) ψ is the unique homomorphism $G/N \to H$ such that $\phi = \psi \circ \pi$.

iv) $\ker \psi = (\ker \phi)/N = \{gN : g \in \ker \phi\}$.

Lemma 9.2 (Universal Property of Quotient Morphism)**.** If $N \trianglelefteq \mathbb{Z}$ then $N = m\mathbb{Z}$ for some $m \in \mathbb{N}$.

Proof. If $N = 0 (= \{0\})$ then can take $m = 0$. Suppose $N \neq 0$. Must contain at least one nonzero element. Take $m =$ smallest positive element in N. $m\mathbb{Z} \subseteq N$ easy. $N \subseteq m\mathbb{Z}$. Let $n \in N$, we write $n = mq + r$ where $0 \leq r < m$. We know $n \in N, mq \in N$. Therefore $r = n - mq \in N$ but $r < m \implies r = 0$. Thus, $n = mq \in m\mathbb{Z}$.

Proposition 9.3. Let $H = \langle h \rangle$ be a cyclic group. Then there exists an isomorphism: $\phi : \mathbb{Z}/m\mathbb{Z} \to H$ where m is the order of $h$if this is finite and 0 if h has infinite order.

Proof. Define $\phi : \mathbb{Z} \to H; i \mapsto h^i$. ϕ is an epimorphism (because $h^{i+j} = h^i \cdot h^j and H = \langle h \rangle$ gives surjective.) Let $N = \ker \phi$. By lemma, $N = m\mathbb{Z}$ for some $m \geq 0$. Apply Universal Property Theorem, gives $\psi : \mathbb{Z}/m\mathbb{Z} \to H$. ψ surjective because ϕ is surjective. Injective if $i + m\mathbb{Z} \in \ker \psi$, then $\phi(i) = 1 \in H$ so $i \in \ker \phi = N = m\mathbb{Z}$. So $H \cong \mathbb{Z}/m\mathbb{Z}$. Check m gives correct order.

Theorem 9.4 (First isomorphism Theorem)**.** Let $\phi : G \to H$ be a homomorphism. The isomorphism π given by $G \to H$ induces $G/\ker \phi \to H$ (by Universal Property) induces $G/\ker \phi \to \operatorname{Im} \phi$.

10 Second and Third Isomorphism Theorems

Proposition 10.1 (Subgroups of Quotient Groups)**.** Let $N \trianglelefteq G$ and $\pi : G \to G/N$ be the quotient map.

i) If $N \leq H \leq G$ then $N \trianglelefteq H$.

ii) There is a bijection between subgroups $H \leq G$ that contain N and subgroups $\bar{H} \leq G/N$. $H \mapsto \pi(H) = \{nH : h \in H\} = H/N$ and $\bar{H} \leftarrow\!\shortmid \pi^{-1}(\bar{H})$.

Proof. Images and image images of subgroups are subgroups. If $\bar{H} \leq G/N$, then $\pi^{-1}(\bar{H})$ contains N (because $1_{G/N} \in \bar{H}$). Surjective: $\pi(\pi^{-1}(\bar{H})) = \bar{H}$ because π surjective. Injective: If $\pi(H_1) = \pi(H_2)$ then $H_1 = H_2$. This follows from $H_1 = \cup_{g \in H_1} gN$ (disjoint union of cosets).

iii) Normal subgroups correspond i.e. $H \trianglelefteq G$ iff $\bar{H} \trianglelefteq G/N$.

Theorem 10.2 (Second Isomorphism Theorem)**.** Suppose $N \trianglelefteq G$ and $N \leq H \trianglelefteq G$. Then $\frac{G/N}{H/N} \cong G/H$.

Proof. Since $\pi_N, \pi_{H/N}$ are both onto, $\phi = \pi_{H/N} \circ \pi_N$ is also onto. $\ker(\phi) = \{g \in G : \pi_N(g) \in \ker(\pi_{H/N} : G/N \to \frac{G/N}{H/N}\} = \{g \in G : \pi_N(g) \in H/N\} = \pi^{-1}(H/N) = H$ by Proposition 10.1. First

Isomorphism Theorem says $G/\ker(\phi) \cong \mathrm{Im}(\phi) \implies G/N \cong \frac{G/N}{H/N}$ which proves the theorem.

Theorem 10.3. Suppose $H \leq G, N \trianglelefteq G$. Then

i) $H \cap N \trianglelefteq H$, $HN \leq G$.

ii) $\frac{H}{H \cap N} \cong \frac{HN}{N}$.

11 Products of Groups

Recall given groups $G_1, \dots, G_n$, the set $G_1 \times G_2 \times \dots G_n = \{(g_1, \dots, g_n) : g_1 \in G_1, \dots g_n \in G_n\}$. More generally if $G_i, i \in I$ are groups then $\prod_{i \in I} G_i = \{(g_i)_{i \in I} : g_i \in G_i\}$.

Proposition - Definition 11.1 (Product)**.** The set $\prod_{i \in I} G_i$ is called the (direct) product of the G_i's, it is a group when endowed with co-ordinatewise multiplication. $(g_i)(g_i') = (g_i g_i')$

i) $1_G = (1_{G_i}) = (1_{G_1}, 1_{G_2}, 1_{G_3}, \dots)$

ii) $(g_i)^{-1} = (g_i^{-1})$

Example 11.2. Consider $\mathbb{Z}^2 = \mathbb{Z} \times \mathbb{Z}$. $(a, b) + (a', b') = (a + a', b + b')$, group law in each coordinate. $\mathbb{Z}^2 = \langle (1, 0), (0, 1) \rangle$ is finitely generated.

Proposition 11.3 (Canonical Injections and Projections)**.** Let $G_i, i \in I$ be groups and $r \in I$.

i) The canonical injection $\iota_r : G_n \to \prod_{i \in I} G_i; g \mapsto (g_i)_{i \in I}$ where $g_i = 1$ if $i \neq r$ or $g_i = g$ if $i = r$.

ii) The canonical project $\pi_r : \prod_{i \in I} G_i \to G_r; (g_i)_{i \in I} \mapsto g_r$.

iii) $\frac{G_1 \times G_2}{G_1 \times \{1\}} \cong G_2$ (Note: $G_n \times \{1\} \trianglelefteq G_1 \times G_2$).

Proof. $\pi_2 : G_1 \times G_2 \to G_2$. Apply First Isomorphism Theorem

Proposition 11.4 (Internal Characterisation of Product)**.** Let $G_1, \dots, G_n \leq G$. Assume $G = \langle G_1, \dots, G_n \rangle$. Assume:

i) If $i \neq j$ then elements of G_i and G_j commute

ii) For any i, $G_i \cap \langle U_{\ell \neq i} G_\ell \rangle = 1$.

Then there is an isomorphism $\phi : G_1 \times \dots G_n \to G; (g_1, \dots, g_n) \mapsto g_1 g_2 \cdots g_n$.

Proof. Check homomorphism:

$$\begin{aligned}
\phi((g_1, \dots, g_n)(h_1, \dots, h_n)) &= \phi((g_1 h_1, \dots g_n h_n)) \\
&= g_1 h_1 g_2 h_2 \cdots g_n h_n \\
&= g_1 \cdots g_n h_1 \cdots h_n && \text{(using (i))} \\
&= \phi(g_1 \dots g_n) \phi(h_1 \dots h_n)
\end{aligned}$$

Surjective? Yes because G is generated by $G_1, \dots, G_n$. Injective? Suppose $\phi((g_1, \dots, g_n)) = 1$, then

$g_1 \cdots g_n = 1 \implies g_1^{-1} \in G_1 = g_2 \cdots g_n \in \langle G_2 \cdots G_n \rangle$ by (ii) must be id. So $g_1 = 1$ and $g_2 \cdots g_n = 1$. Repeat the same argument to get all $g_i = 1$.

Corollary 11.5. Let G = finite group of exponent 2. i.e. LCM of all orders of group element is 2. Then $G \cong \mathbb{Z}/2\mathbb{Z} \times \cdots \mathbb{Z}/2\mathbb{Z}$.

Proof. G is finitely genereqated. Choose minimal generating set $\{g_1, \ldots, g_n\}$, each $\langle g_i \rangle \cong \mathbb{Z}/2\mathbb{Z}$. Want to prove that $G \cong \langle g_1 \rangle \times \ldots \langle g_n \rangle$. Condition (i): Need $g_i g_j = g_j g_i$ for $i \neq j$. $\text{ord}(g_i g_j) = 2$, so $g_i g_j g_i g_j = 1 \implies g_i g_j = g_j^{-1} g_i^{-1} = g_j g_i$. Condition (ii): e.g. $\langle g_1 \rangle \cap \langle g_2, \ldots, g_n \rangle = \{1\}$. If false, then $g_1 \in \langle g_2, \ldots, g_n \rangle$ but then our generating set is not minimal. By proposition $G \cong \langle g_1 \rangle \times \cdots \times \langle g_n \rangle$.

Theorem 11.6. Let G be a finitely generated abelian group. Then $G \cong$ product of cyclic groups. In fact $G \cong \mathbb{Z}/h_1\mathbb{Z} \times \mathbb{Z}/g_2\mathbb{Z} \times \cdots \times \mathbb{Z}/h_n\mathbb{Z} \times \mathbb{Z}^s$ where $h_1 \mid h_2 \mid h_3 \mid \cdots \mid h_n$ for some $n, r \in \mathbb{N}$.

12 Symmetries of Regular Polygons

AO_n, the set of surjective symmetries $T : \mathbb{R}^n \to \mathbb{R}^n$ forms a subgroup of $\text{Perm}(\mathbb{R}^n)$.

Proposition 12.1. Let $T \in AO_n$, then $T = T_{\mathbf{v}} \circ T'$, where $\mathbf{v} = T(\mathbf{0})$ and T' is an isometry with $T'(\mathbf{0}) = \mathbf{0}$.

Proof. Set $T' = T_{\mathbf{v}}^{-1} \circ T = T_{-\mathbf{v}} \circ T$ where $\mathbf{v} = T(\mathbf{0})$. T' is an isometry because T and $T_{\mathbf{v}}$ are isometries. Also $T'(\mathbf{0}) = T_{-\mathbf{v}}(T(\mathbf{0})) = T_{-\mathbf{v}}(\mathbf{v}) = \mathbf{v} - \mathbf{v} = 0$.

Theorem 12.2. Let $T : \mathbb{R}^n \to \mathbb{R}^n$ be an isometry such that $T(\mathbf{0}) = \mathbf{0}$. Then T is linear.

The centre of mass $V = \{\mathbf{v}^1, \ldots, \mathbf{v}^m\} \subseteq \mathbb{R}^n$ is $\mathbf{c}_V = \frac{1}{m}(\mathbf{v}^1 + \cdots + \mathbf{v}^m)$.

Corollary 12.3. Let $V = \{\mathbf{v}^1, \ldots, \mathbf{v}^m\}$ and let $T : \mathbb{R}^n \to \mathbb{R}^n$ be an isometry such that $T(V) = V$. Then $T(\mathbf{c}_V) = \mathbf{c}_V$.

Proof. Decomposte $T = T_{\mathbf{w}} \circ T'$ for some $\mathbf{w} \in \mathbb{R}^n$ and isometry T' with $T'(\mathbf{0}) = \mathbf{0}$. So T' is linear. Then

$$\begin{aligned}
T(\mathbf{c}_V) &= \mathbf{w} + T'(\mathbf{c}_V) = \mathbf{w} + T'\left(\frac{1}{m}\sum_i \mathbf{v}^i\right) \\
&= \mathbf{w} + \frac{1}{m}\sum_i T'(\mathbf{v}^i) && \text{(using linearity)} \\
&= \frac{1}{m}\sum_i \big(T'(\mathbf{v}^i) + \mathbf{w}\big) = \frac{1}{m}\sum_i T(\mathbf{v}^i) \\
&= \frac{1}{m}\sum_i \mathbf{v}^i && \text{(since } T(\mathbf{v}) = \mathbf{v}\text{)} \\
&= \mathbf{c}_V
\end{aligned}$$

Corollary 12.4. Let $G \leq AO_n$ be finite. Then there exists $\mathbf{c} \in \mathbb{R}^n$ such that $T\mathbf{c} = \mathbf{c}$ for any $T \in G$. If we translate to change coordinates so $\mathbf{c} = \mathbf{0}$, then $G < O_n$.

Proof. Pick any $\mathbf{w} \in \mathbb{R}^n$ and let $V = \{S\mathbf{w} : S \in G\} \subseteq \mathbb{R}^n$. V is finite because G is finite. Also $T(V) = \{TS\mathbf{w} : S \in G\} = \{S\mathbf{w} : S \in G\} = V$. Take $\mathbf{c} = \mathbf{c}_V$ then by the previous corollary $T(\mathbf{c}) = \mathbf{c}$ for all $T \in G$.

Proposition 12.5 (Symmetries of Regular Polygons)**.** The group of symmetries of a regular n-gon is in fact D_n.

13 Abstract Symmetry and Group Actions

Definition 13.1 (G-set, Group Action)**.** A G-set is a set S equipped with a map $\alpha : G \times S \to S; (g, s) \mapsto \alpha(g, s) = g.s$ is called a group action and satisfies the following axioms:

i) $g.(h.s) = (g.h).s$ for all $g, h \in G, s \in S$.

ii) $1_G.s = s$ for all $s \in S$.

Definition 13.2 (Permutation Representation)**.** A permutation representation of a group G on a set S is a homomorphism $\phi : G \to \mathrm{Perm}(S)$. This gives a G-set structure on S. Action is $g.s = (\phi(g))(s)$.

Proposition 13.3. Every G-set S arises from some permutation representation. Given G-set S, need to define homomorphism $\phi : G \to \mathrm{Perm}(S)$, take $\phi(g)(s) = g.s$.

Definition 13.4. Let S_1, S_2 be G-sets. A morphism of G-sets is a function $\psi : S_1 \to S_2$ such that $g.\psi(S) = \psi(g.s)$ for all $g \in G, s \in S_1$. Say that ψ is G-equivalent or that ψ is compatible with the G-action.

14 Orbits and Stabilisers

Let $G =$ group, $S = G-$set. Define relation $\sim$ on S by $s \sim t \iff$ there exists $g \in G$ such that $t = g.s$.

Proposition 14.1. This $\sim$ is an equivalence relation.

Proof. Reflexive: $1 \in G$. Symmetric: if $t = g.s$ then $s = g^{-1}.t$. Transitive: if $t = g.s$ and $u = g'.t$ then $u = g'.(g.s) = (g'g).s$.

Corollary - Definition 14.2 (Orbits)**.** The equivalence classes of $\sim$ are called G-orbits. Also, S is a disjoint union of orbits. The G-orbit containing $s \in S$ is denoted $G.s = \{g.s : g \in G\}$. S/G denotes the set of G-orbits of S.

Proposition - Definition 14.3 (G-stable)**.** Let S be a G-set. A subset $T \subseteq S$ is called G-stable if $g.t \in T$ for all $g \in G, t \in T$.

Proposition 14.4. Let $S = G$-set and $s \in S$. The orbit $G.s$ is the smallest G-stable subset of S containing s.

Proof. $G.s$ is G-stable. If T is a G-stable subset containing s then $G.s \subseteq T$. Check these.

Definition 14.5. We say G acts transitively on G-set S, if S consists of a single orbit. i.e. for all $t, s \in S$, there exists $g : g.s = t$.

Example 14.6. Let $G = \mathrm{GL}_n(\mathbb{R})_n(\mathbb{C})$. G acts on $S = M_n(\mathbb{C})$, the set of $n \times n$ matrices over $\mathbb{C}$, by conjugation, i.e. for all $A \in G = \mathrm{GL}_n(\mathbb{C}), M \in S, A.M = AMA^{-1}$. Let us check indeed this gives a group action. Check axioms. $(i) I_n.M = I_n M I^{-1} = M.(ii) A.(B.M) = A.(BMB^{-1}) = ABMB^{-1}A_1 = (AB)M(AB)^{-1} = (AB).M$. What are the orbits? $GM = \{AMA^{-1} : A \in \mathrm{GL}_n(\mathbb{C})\}$.

Definition 14.7 (Stabilisers)**.** Let $s \in S$. Then the stabiliser of s is $\mathrm{stab}_G(s) = \{g \in G : g.s = s\} \subseteq G$

Proposition 14.8. Let S be a G-set and let $s \in S$. Then $\mathrm{stab}_G(s) \leq G$.

15 Structure of G-orbits

Proposition 15.1. Let $H \leq G$. Then G/H is a G-set with the action $g'.(gH) = (g'g)H$ for all $g, g' \in G$

Proof. Checking axioms to show G/H is a G-set.

(i) $1.(gH) = gH$

(ii) $g''.(g'.(gH)) = (g''g')(gH)$. LHS $= g''.(g'gH) = g''g'g'H = (g''g')gH =$ RHS.

Theorem 15.2 (Structure of G-orbits)**.** Suppose G acts transitively on S. Let $s \in S$ and $H = \mathrm{stab}_G(s) \leq G$. Then there is an isomorphism of G-sets: $\psi : G/H \to S; gH \mapsto g.s$.

Proof. Well-defined: if $gH = g'H$ then $g' = gh$ for $h \in H$. So we need to check $g.s = g'.s$. RHS $= g'.s = (gh).s = g.(h.s) = g.s =$ LHS, for $h \in \mathrm{stab}(s)$.

Next we need to check its a morphism of G-sets. i.e. $\psi(g'(gH)) = g'.\psi(gH) \implies (g'g).s = g'.(g.s)$. Next surjective because action is transitive. Injective: if $\psi(gH) = \psi(g'H) \implies g.s = g'.s \implies s = (g^{-1}g').s$. So $g^{-1}g' \in \mathrm{stab}(s) = H$ so $g' \in gH, gH = g'H$.

Corollary 15.3. If G is finite then, $|G.s|$ divides $|G|$ by Lagrange's theorem.

Proposition 15.4. Let $S = G$-set, $s \in S, g \in G$. Then $\mathrm{stab}_G(g.s) = g.\mathrm{stab}_G(s).g^{-1}$.

Corollary 15.5. Let $H_1, H_2 \leq G$ be conjugate. (i.e. $H_2 = gH_1g^{-1}$ for some $g \in G$). Then $G/H_1 \cong G/H_2$ as G-sets.

Definition 15.6. If $S =$ a platonic solid (all faces same, and all regular polygons, and same number of faces at each vertex) and $G =$ group of rotation symmetries $=$ symmetries $\cap SO_3$.

Proposition 15.7. With notation as above, then $|G| =$ number of faces $\times$ number of edges on each face.

Proof. Let $F =$ set of faces, G acts on F. Gives a G-set structure to F. Let $f \in F$ be a face, then $G.f = F$ (i.e. action is transitive). By the theorem, $F \cong G/\mathrm{stab}_G(f)$. But $\mathrm{stab}_G(f) =$ rotations around axis through face. $\mathrm{stab}_G(f) =$ number of edges on each face which implies $|G| = |F||\mathrm{stab}_G(f)|$.

16 Counting Orbits and Cayley's Theorem

Let G be a group and S be a G-set.

Definition 16.1 (Fixed Point Set). The fixed point set of a subset $J \subseteq G$ is $S^J = \{s \in S : j.s = s \text{ for all } j \in J\}$.

Proposition 16.2. Let S be a G-set

i) If $J_1 \subseteq J_2 \subseteq G$ then $S^{J_2} \subseteq S^{j_1}$

ii) If $J \subseteq G$ then $S^J = S^{\langle J \rangle}$

Example 16.3. $G = \mathrm{Perm}(\mathbb{R}^2)$ acts naturally on $S = \mathbb{R}^2$. Let $\tau_1, \tau_2 \in G$ be reflections about lines L_1, L_2. Then $S^{\tau_i} = L_i$, $S^{\{\tau_1, \tau 2_2\}} = L_1 \cap L_2$ and $S^{\langle \tau_1, \tau_2 \rangle} = L_1 \cap L_2$.

Theorem 16.4. Let G be a finite group and S be a finite G-set. Let $|X|$ denote the cardinality of X. Then

$$\text{number of orbits of } S = \frac{1}{|G|} \sum_{g \in G} |S^g| = \text{average size of the fixed point set}$$

Proof. Let $S = \dot{\bigcup}_i S_i$ where S_i are G-orbits. Then $S^g = \dot{\bigcup}_i S_i^g$. LHS $= \sum_i$ number of orbits of S_i (since S_i's are union of G-orbits and S_i's are disjoint) while RHS $= \sum_i \frac{1}{|G|} \sum_{g \in G} |S_i^g|$. Thus it suffices to prove theorem for $S = S_i$ and then just sum over i. But S are disjoint union of G-orbits, so can assume $S = S_i = G$-orbit which by (Theorem 15.2), means $S \cong G/H$ for some $H \leq G$. So in this case

$$\begin{aligned}
\text{RHS} &= \frac{1}{|G|} \sum_{g \in G} |S^g| \\
&= \frac{1}{|G|} \times \text{number of } (g, s) \in G \times S : g.s = s \text{ by letting } g \text{ vary all over } G \\
&= \frac{1}{|G|} \sum_{s \in S = G/H} |\operatorname{stab}_G(s)|
\end{aligned}$$

Note by proposition 15.4, these stabilisers are all conjugates, and hence all have the same size. Since $|\operatorname{stab}_G(1.H)| = |H|, |\operatorname{stab}_G(s)| = |H|$ for all $s \in S$. Hence RHS $= \frac{1}{G}|G/H||H| = \frac{|H|}{|G|}\frac{|G|}{|H|} = 1$ and LHS = number of orbits of $S = 1$ as S is assumed to be a G-orbit.

Example 16.5. Birthday cake with 8 slices. Red/green candle on each slide. How many ways? Notice that: two arrangments are the same if you can rotate one to get the other.

$S = \{0, 1\}^8, |S| = 2^8 = 256$. $\sigma \in \mathrm{Perm}(S)$ acts by $\sigma(x_1, \ldots, x_8) = (x_2, x_3, \ldots, x_8, x_1)$. $G = \langle \sigma \rangle, |G| = 8$. We want to find number of G-orbits. By the theorem above, this is equal to $\frac{1}{8} \sum_{g \in G} |S^g|$. Trying each g:

$$
\begin{array}{llll}
g = 1 & \implies |S^1| = 2^8 & g = \sigma^4 & \implies |S^{\sigma^4}| = 2^4 \\
g = \sigma & \implies |S^{\sigma}| = 2 & g = \sigma^5 & \implies |S^{\sigma^5}| = 2 \\
g = \sigma^2 & \implies |S^{\sigma^2}| = 2^2 & g = \sigma^6 & \implies |S^{\sigma^6}| = 2^2 \\
g = \sigma^3 & \implies |S^{\sigma^3}| = 2 & g = \sigma^7 & \implies |S^{\sigma^7}| = 2
\end{array}
$$

$$\text{Final Answer: } \frac{1}{8}(256 + 16 + 4 + 4 + 4 + 4 \cdot 2) = \frac{1}{8}(288) = 36.$$

Definition 16.6 (Faithful Permutation Representation)**.** A permutation representation $\phi : G \to \operatorname{Perm} S$ is faithful if $\ker \phi = 1$.

Theorem 16.7 (Cayley)**.** Let G be a group. Then G is isomorphic to a subgroup of $\operatorname{Perm}(G)$. In particular, if $|G| = n < \infty$, then G is isomorphic to a subgroup of S_n.

Proof. Let G act oon itself: $g.h = gh$. This gives $\phi : G \to \operatorname{Perm}(G)$. If $g \in G$ has property that $gh = h$ for all $h \in G$ then $g = 1$. Clear, take $h = 1$.

Part II

Ring Theory

17 Rings

Definition 17.1 (Ring)**.** A ring is an abelian group R, with group addition together with ring multiplication map ($\mu : R \times R \to R$) satisfying:

i) associativity: $(rs)t = r(st)$ for all $r, s, t \in R$.

ii) there exists $1_R \in R$ such that $1r = r$ and $r1 = r$ for all $r \in R$.

iii) distributive law: $r(s + t) = rs + rt$ and $(r + s)t = rt + st$ for all $r, s, t \in R$.

Similar to a group, 1 is unique and $0r = 0$.

Example 17.2. $\mathbb{C}, \mathbb{Z}, \mathbb{R}, \mathbb{Q}$ are all rings.

Example 17.3. Let V be a vector space over $\mathbb{C}$. Define $\operatorname{End}_{\mathbb{C}}(V)$ be the set of linear maps $T : V \to V$. Then $\operatorname{End}_{\mathbb{C}}(V)$is a ring when endowed with ring additional equal to sum of linear maps, ring multiplication equal to composition of linear maps. $0 =$ constant map to $\mathbf{0}$ and $1 = \mathrm{id}_V$.

Proposition - Definition 17.4 (Subrings)**.** A subset of $S \subseteq R$ is a subring if:

i) $s + s' \in S$ for all $s, s' \in S$

ii) $ss' \in S$ for all $s, s' \in S$

iii) $-s \in S$ for all $s \in S$

iv) $0_R \in S$

v) $1_R \in S$.

Then S becomes a ring with restricted $+, \cdot, 0, 1$. Note the identity 1_R is the identity from R.

Example 17.5. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ are all substrings of $\mathbb{C}$. Also the set of Gaussian integers $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ is a subring.

Example 17.6. Matrices $M_n(\mathbb{R})$ and $N_n(\mathbb{C})$ both form rings. The set of upper triangular matrices form a subring.

Proposition 17.7. i) subrings of subrings are subrings

ii) intersection of subrings is a subring

Proposition - Definition 17.8 (Units)**.** Let $R =$ ring. An element $u \in R$ is called a unit or invertible if there exists $v \in R$ such that $uv = 1$ and $vu = 1$. Define $R^* = \{$ set of units in R$\}$ as a group (with multiplicative structure).

Example 17.9. $\mathbb{Z}^* = \{1, -1\}$