

Higher Algebra

Jeremy Le — UNSW MATH3711 25T1

Contents

1	The Mathematical Language of Symmetry	2
2	Matrix Groups and Subgroups	3
3	Permutation Groups	4
4	Generators and Dihedral Groups	5
5	Alternating and Abelian Groups	7
6	Cosets and Lagrange's Theorem	8

1 The Mathematical Language of Symmetry

Definition 1.1 (Isometry). A function $f : \mathbb{R}^n \rightarrow \mathbb{R}^n$ 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 $T : \mathbb{R}^n \rightarrow \mathbb{R}^n$ such that $T(F) = F$.

Properties 1.3. Let S, T be symmetries of $F \subseteq \mathbb{R}^n$. Then $S \cdot T : \mathbb{R}^n \rightarrow \mathbb{R}^n$ 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) $\text{id}_{\mathbb{R}^n} \in G$ ($\text{id}_{\mathbb{R}^n}(x) = x$ for all $x \in \mathbb{R}^n$). Also, $\text{id}_G T = T$ and $T \text{id}_G = T$ 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.

$$\begin{aligned} \|T^{-1}x - T^{-1}y\| &= \|TT^{-1}x - TT^{-1}y\| \\ &= \|\text{id } x - \text{id } y\| \\ &= \|x - y\|. \end{aligned}$$

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” $\mu : G \times G \rightarrow G$ such that

- 1) Associativity: $(gh)k = g(hk)$ for all $g, h, k \in G$.
- 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 $GL_n(\mathbb{R})$ and $GL_n(\mathbb{C})$ which represent the set of real/complex invertible $n \times n$ matrices.

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

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

- i) matrix multiplication is associative.
- ii) identity matrix $I_n : I_n m = m$ and $m I_n = m$ for all $m \in GL_n(\mathbb{R})$
- iii) if $m \in GL_n(\mathbb{R})$ 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. $(gh)(h^{-1}g^{-1}) = gh h^{-1}g^{-1} = g1g^{-1} = gg^{-1} = 1$. 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 $\mu_H : H \times H \rightarrow H$ 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 $O_n(\mathbb{R}) = \{M \in GL_n(\mathbb{R}) : M^T = M^{-1}\} \leq GL_n(\mathbb{R})$ 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 $\text{Perm}(S)$ be the set of permutations of S . This is the set of bijections of form $\sigma : S \rightarrow S$.

Proposition 3.2. $\text{Perm}(S)$ 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 $S = \{1, \dots, n\}$. The symmetric group S_n is $\text{Perm}(S)$.

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

Example 3.4. For $n = 4$,

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

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

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 $s_1 \dots s_k$ and $t_1 \dots t_k$ are disjoint if $\{s_1, \dots, s_k\} \cup \{t_1, \dots, t_k\} = \emptyset$.

Definition 3.6 (Commutativity). 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 $1 \rightarrow 2 \rightarrow 4 \rightarrow 1$, $3 \rightarrow 6 \rightarrow 3$ and $5 \rightarrow 5$.
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, \dots, 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 $(s_1 s_2 \dots s_k) = (s_1 s_k)(s_1 s_{k-1}) \dots (s_1 s_3)(s_1 s_2)$

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

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

$$\begin{array}{l} s_1 \rightarrow s_2 \\ s_2 \rightarrow s_1 \rightarrow s_3 \\ s_3 \rightarrow s_1 \rightarrow s_4 \\ \vdots \\ s_{k-1} \rightarrow s_1 \rightarrow s_k \\ s_k \rightarrow s_1. \end{array}$$

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 $i \implies gh \in \bigcap_{i \in I} H_i$.
- 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 $s_i \dots s_n \in$ 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 cyclic if we can take $|S| = 1$.

Example 4.4. Take $G \in \text{GL}_2(\mathbb{R})$ 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}).

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

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, $\{1, \sigma, \dots, \sigma^{n-1}\} \cap \{\tau, \sigma\tau, \dots, \sigma^{n-1}\tau\} = \emptyset$ 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 $f(x_1, \dots, x_n)$ be a function of n variables. Let $\sigma \in S_n$. We define function $(\sigma f)(x_1, \dots, x_n) = f(x_{\sigma(1)}, \dots, x_{\sigma(n)})$. 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

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

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

Proof.

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

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 $\sigma = \tau_1 \tau_2 \dots \tau_m$ 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. Sufficient to prove for a single transposition (i.e. $m = 1$) because by the above Lemma,

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

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 by 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 $G = \bigcup_{i \in I} g_i H$ (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, $H \rightarrow gH, h \mapsto gh$. Surjective and injective (multiply on left 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.