Graph Theory

Jeremy Le — UNSW MATH3711 25T1

Contents

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 $GL_n(\mathbb{R})$ 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 $mI_n = m$ for all $m \in GL_n(\mathbb{R})$

iii) if $m \in GL_n(\mathbb{R})$ then m^{-1}. $mm^{-1} = I$ and $m^{-1}m = I$.

$\square$

Proposition 2.2. Let $G =$ group.

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

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

2) Inverses are unique.

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

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, $(h^{-1}g^{-1}(gh) = 1)$. $\square$

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 $O_n(\mathbb{R}) = \{M \in GL_n(\mathbb{R}) : M^T = M^{-1}\} \leq GL_n(\mathbb{R})$ 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 ∞.