Abstract Algebra and Fundamental Analysis

Jeremy Le — UNSW MATH2701 24T3

Contents

1 Transformations and Groups

Definition 1.1. A *transformation* on $\mathbb{R}^n$ is a **bijection** from $\mathbb{R}^n$ to $\mathbb{R}^n$. We will denote $\mathscr{B}(\mathbb{R}^n)$ the set of all transformations on $\mathbb{R}^n$.

In particular, a transformation on the Euclidean plane $\mathbb{R}^2$ is called a **plane transformation**.

Definition 1.2 (Group)**.** A group is a set G equipped with a map

$$* : G \times G \to G, (g, h) \mapsto g * h = gh,$$

that satisfies the following axioms:

(G1) **Associativity**, i.e. $g, h, k \in G$, then $(gh)k = g(hk)$.

(G2) **Existence of identity**, i.e. there is an element denoted by e in G called the *identity* of G such that $eg = g = ge$ for any $g \in G$. (Such e is unique; notation: 1_G.)

(G3) **Existence of inverse**, i.e. for any $g \in G$, there is an element denoted by $h \in G$ called the inverse of g such that $gh = hg = e$. (h is also unique; notation: g^{-1}.)

A group G is called commutative or abelian if $gh = hg$ for all $g, h \in G$.

Proposition 1.3. *Examples of Transformation Groups*

(1) *The set $\mathscr{B}(\mathbb{R}^n)$ of all transformations on $\mathbb{R}^n$ together with the operation of composition forms a group.*

(2) *The set $\mathscr{T}(\mathbb{R}^n)$ of all translations on $\mathbb{R}^n$ together with the operation of composition forms a group.*

(3) *The set $\mathscr{C}(\mathbb{R}^n)$ of collineations of $\mathbb{R}^n$ together with the operation of composition forms a group.*

Definition 1.4 (Subgroup)**.** Let $(G, *)$ be a group. A nonempty subset $H \subseteq G$ is said to be a subgroup of G, denoted by $H \leq G$, if $(H, *)$ is a group.

Lemma 1.5 (Subgroup Lemma)**.** *A nonempty subset H of a group G is a subgroup if and only if the following two closure conditions are satisfied:*

(SG1) *Closure under multiplication, i.e. if $h, k \in H$, then $hk \in H$;*

(SG2) *Closure under inverse, i.e. if $h \in H$, then $h^{-1} \in H$.*

In particular, $1_H = 1_G \in H$.

Definition 1.6 (Group Isomorphisms)**.** For groups G, H, a map $f : G \to H$ is called a group homomorphism if $f(xy) = f(x)f(y)$ for all $x, y \in G$. A bijective group homomorphism is called an isomorphism. In this case, we say that G is isomorphic to H. Notation $G \cong H$.

2 Subgroups and the Group of Isometries

Lemma 2.1. *If S is a subset of a group $(G, *)$, then $\langle S \rangle = \bigcap_{S \subseteq H \leq G} H$. In other words, $\langle S \rangle$ is the **smallest** subgroup of G that contains all the elements of S.*

Definition 2.2. We call $\langle S \rangle$ the **subgroup of G generated by** S. A group generated by one element is called a **cyclic group**.

Notation:

- space: $\mathbb{R}^n$;
- points: $A, B, C, P, Q, R, \ldots$ with position vectors $\mathbf{a}, \mathbf{b}, \mathbf{c}, \mathbf{p}, \mathbf{q}, \mathbf{r} \ldots$;
- transformations: $\tau, \pi, \sigma, \delta, \ldots$;
- lines: $l, m, n, \ldots$; line equations in $\mathbb{R}^n : \mathbf{x} = \mathbf{a} + \lambda \mathbf{v}$ for all $\lambda \in \mathbb{R}$;
- planes in $\mathbb{R}^n = \mathbf{x} = \mathbf{a} + \lambda \mathbf{u} + \mu \mathbf{v}$ for all $\lambda, \mu \in \mathbb{R}$;
- **Hyperplanes** through $\mathbf{a} \in \mathbb{R}^n$ with normal $\mathbf{n} \in \mathbb{R}^n = \mathbf{0}$:
$$\mathbb{H}_{\mathbf{n},\mathbf{a}} = \{\mathbf{x} \in \mathbb{R}^n \mid (\mathbf{x} - \mathbf{a}) \cdot \mathbf{n} = 0\} = \langle \mathbf{n} \rangle^{\perp} + \mathbf{a}.$$
- For points P, Q in $\mathbb{R}^n$, we may also define the **perpendicular bisector** of the line segment $\bar{PQ}$ to be the hyperplane $\mathbb{H}$ that passes through the midpoint of $\bar{PQ}$ and perpendicular to $\bar{PQ}$. So $\mathbb{H}$ has the equation $(\mathbf{x} - \mathbf{m}) \centerdot (\mathbf{p} - \mathbf{q}) = 0$ where $\mathbf{m} = \frac{\mathbf{1}}{\mathbf{2}}(\mathbf{p} + \mathbf{q})$.
- It is clear that, for all $X \in \mathbb{H}$,
$$d(X, P) = \sqrt{\|\mathbf{x} - \mathbf{m}\|^2 + \|\mathbf{p} - \mathbf{m}\|^2} = \sqrt{\|\mathbf{x} - \mathbf{m}\|^2 + \|\mathbf{q} - \mathbf{m}\|^2} = d(X, Q).$$

The Euclidean space $\mathbb{R}^n$

- Length of a vector: $\|\mathbf{a} = \sqrt{\mathbf{a} \centerdot \mathbf{a}}\|$;
- Distance between two points $P, Q : d(P, Q) := \|\mathbf{p} - \mathbf{q}\|$;
- Projection of $\mathbf{a}$ on $\mathbf{b}$: $\mathrm{proj}_{\mathbf{b}}(\mathbf{a}) = \frac{\mathbf{a} \cdot \mathbf{b}}{\mathbf{b} \cdot \mathbf{b}} \mathbf{b}$;
- Angle between $\mathbf{a}$ and $\mathbf{b}$: $\cos(\theta) = \frac{\mathbf{a} \cdot \mathbf{b}}{\|\mathbf{a}\| \|\mathbf{b}\|}$;
- Orthogonality: $\mathbf{a} \perp \mathbf{b} \iff \mathbf{a} \centerdot \mathbf{b} = 0$;

Definition 2.3. An *isometry* on $\mathbb{R}^n$ is a map $\tau : \mathbb{R}^n \to \mathbb{R}^n$ which preserves distance between points: $d(P, Q) = d(\tau(P), \tau(Q)), \forall P, Q \in \mathbb{R}^n$.

Lemma 2.4. *The set of isometries which fix the zero vector is equal to the set of (linear) maps that represent multiplication by an orthogonal matrix.*

Theorem 2.5. *An isometry can be decomposed into a translation multiplied by a linear transformation, which can be represented by an orthogonal matrix. In other words, for every $\tau \in \mathscr{I}(\mathbb{R}^n)$, there exist an orthogonal $n \times n$ matrix Q and a vector $\mathbf{b} \in \mathbb{R}^n$ such that $\tau = T_{Q,\mathbf{b}} = T_{I,\mathbf{b}} \circ T_{Q,\mathbf{0}}$. In particular, an isometry is a **transformation**.*

Theorem 2.6. *The group of Isometries*

(1) *The set $\mathscr{I}(\mathbb{R}^n)$ of all isometries forms a subgroup of the group $\mathscr{B}(\mathbb{R}^n)$ of all transformations.*

(2) *The group $\mathscr{I} = \mathscr{I}(\mathbb{R}^n)$ contains two subgroups: the group $\mathscr{T}$ of translations and the group $\mathscr{O}$ of all orthogonal linear transformations. Moreover, we have $\mathscr{I} = \mathscr{T}\mathscr{O} := \{\tau\sigma \mid \tau \in \mathscr{T}, \sigma \in \mathscr{O}\}$.*

3 Reflections and Isometries

Definition 3.1. Let $\mathbb{H}$ be a hyperplane. The reflection $\sigma_{\mathbb{H}}$ in $\mathbb{H}$ is the mapping defined by:

$$\sigma_{\mathbb{H}}(P) = \begin{cases} P & \text{if } P \in \mathbb{H}; \\ P' & \text{if } P \text{ is off } \mathbb{H} \text{ and } \mathbb{H} \text{ is the perpendicular bisector of } \bar{PP'}. \end{cases}$$

(in the sense that $d(P, X) = d(P', X)$ for all $X \in \mathbb{H}$.)

Proposition 3.2. *Let $\mathbb{H}$ be a hyperplane.*

(1) *A reflection $\sigma_{\mathbb{H}}$ is an isometry satisfying $\sigma_{\mathbb{H}}^2 = 1$.*

(2) *$\sigma_{\mathbb{H}}$ fixes a line $m \nsubseteq \mathbb{H}$ if and only if $m \perp \mathbb{H}$.*

(3) *$\sigma_{\mathbb{H}}$ fixes a line **pointwise** if and only if $m \subseteq \mathbb{H}$.*

Theorem 3.3. *If $\mathbb{H} = \mathbb{H}_{\mathbf{n},\mathbf{a}}$, then there exist $Q = I - \frac{2}{\mathbf{n}.\mathbf{n}}\mathbf{n}\mathbf{n}^T \in O_n(\mathbb{R})$ and $\mathbf{b} = 2\frac{\mathbf{a}.\mathbf{n}}{\mathbf{n}.\mathbf{n}}\mathbf{n}$ such that*

$$\sigma_{\mathbb{H}}(\mathbf{x}) = Q\mathbf{x} + \mathbf{b}.$$

Corollary 3.4. *In $\mathbb{R}^2$, if line ℓ has equation $aX + bY + c = 0$, then the reflection σ_ℓ in ℓ has equation:*

$$\begin{aligned} \sigma_\ell(\mathbf{x}) &= \frac{1}{a^2+b^2}\begin{bmatrix} b^2 - a^2 & -2ab \\ -2ab & a^2 - b^2 \end{bmatrix}\mathbf{x} + \frac{1}{a^2+b^2}\begin{bmatrix} -2ac \\ -2bc \end{bmatrix} \\ &= \begin{pmatrix} x \\ y \end{pmatrix} - 2\frac{(ax+by+c)}{a^2+b^2}\begin{pmatrix} a \\ b \end{pmatrix}. \end{aligned}$$

Definition 3.5 (Points in Generic Position)**.** We say that m points $P_1(\mathbf{p_1}), P_2(\mathbf{p_2}), \ldots, P_m(\mathbf{p}_m)$ in $\mathbb{R}^n$ are in **generic position** if the vectors $\mathbf{p}_i - \mathbf{p}_1$, for $i = 2, 3, \ldots, m$, are linearly independent. In particular, $n+1$ points in $\mathbb{R}^n$ are in generic position if every hyperplane contains at most n of the $n+1$ points.

Theorem 3.6. **(1)** *An isometry on $\mathbb{R}^n$ that fixes $n+1$ points in generic position is the identity map.*

(2) *An isometry on $\mathbb{R}^n$ that fixes n points in generic position is a reflection **or** the identity.*

(3) *An isometry that fixes $n-1$ but not n points in generic position is a product of two **reflections**.*

(4) *Every isometry (in $\mathbb{R}^n$) is a product of **at most** $n+1$ reflections.*

4 Translations and Rotations on $\mathbb{R}^2$

Theorem 4.1. *An isometry τ in $\mathbb{R}^n$ is a **translation** if and only if τ is the product of two reflections in parallel hyperplanes.*

Corollary 4.2. *A plane isometry is a translation if and only if it is a product of two reflections in parallel lines.*

Definition 4.3. A **rotation** on $\mathbb{R}^2$ about a point C, through angle θ, is the transformation that fixes C and otherwise sends a point P to a point P', where $d(C,P) = d(C,P')$, and the angle from $\vec{CP}$ to $\vec{CP'}$ is θ (in anti-clockwise direction) if $\theta > 0$, and clockwise if $theta < 0$). We denote this transformation by $\rho_{C,\theta}$.

Theorem 4.4. *A plane isometry is a **rotation** if and only if it is the product of two reflections in intersecting lines. Further we have*

- **(1)** *if lines l, m intersect at C, and the directed angle from l to m is $\frac{\theta}{2} \in (-\frac{\pi}{2}, \frac{\pi}{2}]$, then $\sigma_m \sigma_l = \rho_{C,\theta}$;*
- **(2)** *if lines p, q, r are concurrent, then there exists a line l such that $\sigma_r \sigma_q \sigma_p = \sigma_l$.*

Corollary 4.5. **(1)** *A non-identity rotation (on $\mathbb{R}^2$) fixes exactly one point.*

- **(2)** *A rotation with centre C fixes every circle with centre C.*
- **(3)** *The set of all rotations about a particular point (i.e., with centre at a particular point) is a subgroup of the group $\mathscr{I}(\mathbb{R}^2)$ of isometries; further still, it is a **commutative** subgroup. In other words,*

$$\mathscr{R}_C := \{\rho_{C,\theta} : \theta \in \mathbb{R}\} \leq \mathscr{I}(\mathbb{R}^2) \text{ and } \rho\rho' = \rho'\rho, \forall \rho, \rho' \in \mathscr{R}_C.$$

Theorem 4.6 (Equation of a rotation). **(1)** *The rotation $\rho_{\mathbf{0},\theta} : \mathbb{R}^2 \to \mathbb{R}^2$ about the origin $\mathbf{0}$ and through angle θ is the linear isomorphism $T_{Q,\mathbf{0}}(\mathbf{x}) = Q\mathbf{x}$, where Q is the following matrix:*

$$Q = \begin{bmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{bmatrix}.$$

- **(2)** *If $\mathbf{c}$ is the position vector of C, then $\rho_{C,\theta} = T_{\mathbf{c}}(\rho_{\mathbf{0},\theta})T_{-\mathbf{c}}$. Hence, $\rho_{\mathbf{C},\theta}$ has the equation $\rho_{C,\theta}(\mathbf{x}) = Q\mathbf{x}+\mathbf{b}$, where Q defines $\rho_{\mathbf{0},\theta}$ as in (1) and $\mathbf{b} = (I-Q)\mathbf{c}$. At the group level, we have $\mathscr{R}_C = T_{\mathbf{c}}\mathscr{R}_{\mathbf{0}}T_{-\mathbf{c}}$. Call the group $\mathscr{R}_C$ is **conjugate** to the group $\mathscr{R}_{\mathbf{0}}$.*