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: $\left\|\mathbf{a} = \sqrt{\mathbf{a} \centerdot \mathbf{a}}\right\|$;
- 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 $m \not\subseteq \mathbb{H}$ 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 $Q = I - \frac{2}{\mathbf{n.n}}\mathbf{n}\mathbf{n}^T \in O_n(\mathbb{R})$ and $\mathbf{b} = 2\frac{\mathbf{a.n}}{\mathbf{n.n}}\mathbf{n}$ 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.*

Corollary 3.7. *The group $\mathscr{I}(\mathbb{R}^n)$ is generated by reflections $\mathbb{H}_{\mathbf{n},\mathbf{a}}$ for all $\mathbf{0} \neq \mathbf{n}, \mathbf{a} \in \mathbb{R}^n$.*

Corollary 3.8. **(1)** *A plane isometry that fixes three vertices of a triangle is the identity map.*

(2) *Every plane isometry $\tau \in \mathscr{I}(\mathbb{R}^2)$ is a product of at most three reflections in three lines.*

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 $\mathscr{R}_{\mathbf{0}}$.*

Half-turn A rotation of the form $\rho_C := \rho_{C,\pi}$ is called a half-turn. A half-turn has the equation

$$\mathbf{x}' = -\mathbf{x} + 2\mathbf{c},$$

where $\mathbf{c}$ is the position vector of C.

Definition 4.7. A figure $F_1 \subseteq \mathbb{R}^n$ is **congruent** to a figure $F_2 \subseteq \mathbb{R}^n$ if one can be mapped onto the other by an isometry; i.e. if there exists an isometry τ such that $\tau(F_1) = F_2$. **Notation:** $F_1 \cong F_2$ means F_1 is congruent to F_2.

Theorem 4.8. *If $\triangle ABC \cong \triangle A'B'C'$ in $\mathbb{R}^2$ (same side lengths), then there exists a **unique** plane isometry τ such that*

$$\tau(A) = A', \tau(B) = B', \tau(C) = C'.$$

5 Classification of Plane Isometries

Definition 5.1. A plane isometry τ is called a **glide reflection** with axis c (a line) if there exist distinct lines a, b which are perpendicular to c such that $\tau = \sigma_c\sigma_b\sigma_a (= \sigma_b\sigma_a\sigma_c)$.

Proposition 5.2. **(1)** *A glide reflection is a composition of a reflection in line a and a halfturn centred at a point off a.*

(2) *A glide reflection is a translation followed by a reflection.*

(3) *A glide reflection fixes no points.*

(4) *A glide reflection fixes exactly one line, the axis, c.*

(5) *The midpoint of any point and its image under a glide reflection lies on its axis (c).*

Theorem 5.3. *Distinct lines p, q, r are neither concurrent, nor parallel, if and only if $\sigma_r\sigma_q\sigma_p$ is a glide reflection.*

Definition 5.4. An isometry that is a product of an even (resp., odd) number of reflections is said to be even (resp., odd) isometry.

Theorem 5.5. *1. The set $\mathscr{E}$ of even isometries in $\mathbb{R}^n$ forms a subgroup of $\mathscr{I}$.*

2. If $\mathscr{E}'$ denotes the set of odd isometries, then $\mathscr{E} \cap \mathscr{E}' = \emptyset$.

3. If $\sigma = \sigma_{\mathbb{H}}$ is a reflection, then $\mathscr{E}' = \sigma\mathscr{E} := \{\sigma\pi | \pi \in \mathscr{E}\}$.

4. We also have $\sigma\mathscr{E} = \mathscr{E}\sigma$ and $\mathscr{I} = \mathscr{E} \bigsqcup \sigma\mathscr{E}$.

Corollary 5.6. *For any non-identity plane isometries, it is either even or odd. All even isometries are either translations or rotations. All odd isometries are reflections or glide reflections.*

Theorem 5.7. *A product of 4 reflections in $\mathbb{R}^2$ is a product of 2 reflections.*

Definition 5.8. Let $\Omega \subseteq \mathbb{R}^n$ be a geometric figure (or a subset). A **symmetry** of Ω si an isometry τ such that $\tau(\Omega) = \Omega$.

All the symmetries of Ω form a group $\mathrm{sym}(\Omega)$, the **symmetry group** of Ω.

6 Similarities

Definition 6.1. A transformation $\alpha : \mathbb{R}^n \to \mathbb{R}^n$ is called a **similarity of ratio** $r > 0$ if

$$d(\alpha(P), \alpha(Q)) = rd(P, Q), \text{ for all } P, Q \in \mathbb{R}^n.$$

Proposition 6.2. **(1)** *An isometry is a similarity of ratio 1.*

(2) *A similarity fixing two points is an isometry.*

(3) *A similarity fixing $n+1$ points in generic position is the identity.*

(4) *The set of all similarities in $\mathbb{R}^n$ forms a group, denote this set by $\mathscr{S}$ or $\mathscr{S}(\mathbb{R}^n)$.*

Definition 6.3. A **stretch of ratio** $r > 0$ about point C is a transformation $\delta_{C,r}$ that fixes C and otherwise sends a point P to a point P', where P' is the unique point on the **ray** from C through P such that $d(C, P') = r \cdot d(C, P)$.

Theorem 6.4. *Decomposition of a similarity If α is a similarity of ratio $r > 0$, and P is any **fixed** point, then $\alpha = \tau\delta_{P,r} = \delta_{P,r}\tau'$, for some isometries tau, τ'. Moreover, we have*

$$\mathscr{S} = \bigsqcup_{r>0} \mathscr{I} S_{P,r} = \bigsqcup_{r>0} S_{P,r}\mathscr{I} \text{ (disjoint unions)},$$

where $\mathscr{I} S_{P,r} = \{\tau S_{P,r} \mid \tau \in \mathscr{I}\}$ and $\S_{P,r}\mathscr{I} = \{S_{P,r}\tau \mid \tau \in \mathscr{I}\}$.

Corollary 6.5. *A similarity is a **collineation** that preserves betweenness, midpoints, angles, perpendicularity, etc.*

Definition 6.6. **(1)** A **point reflection** about $C(\mathbf{c})$ is the isometry $\rho_C : \mathbb{R}^n \to \mathbb{R}^n$ defined by

$$\rho_C(\mathbf{x}) = -(\mathbf{x} - \mathbf{c}) + \mathbf{c} = -\mathbf{x} + 2\mathbf{c}.$$

(2) A **dilation** about the point C is a stretch transformation $\delta_{C,r}(r > 0)$ about C, or it is a stretch transformation followed by a point reflection both about C (i.e., $\rho_C\delta_{C,r}$).

Lemma 6.7. **(1)** *A point reflection is an isometry.*

(2) *The product of two point reflections is a translation.*

(3) *The product of a translation and a point reflection is a point reflection.*

Proposition 6.8. *All point reflections generate a subgroup $\mathscr{H}(of \mathscr{I})$. Moreover, $\mathscr{H}$ is a (disjoint) union of the set $\mathscr{T}$ of all translations and the set of all point reflections: for a fixed C,*

$$\mathscr{H} = \mathscr{T} \sqcup \rho_C\mathscr{T} = \mathscr{T} \sqcup = \mathscr{T}\rho_C = \mathscr{T} \sqcup \{\rho_P \mid P \in \mathbb{R}^n\}.$$

Proposition 6.9. *The dilation $\tau = \rho_C\delta_{C,r}(r > 0)$ has the following equation:*

$$\tau(\mathbf{x}) = (-r)\mathbf{x} + (1 + r)\mathbf{c}.$$

Lemma 6.10. *Let $R^\times = \{r \in \mathbb{R} \mid r \neq 0\}$. For any $r, s \in \mathbb{R}^\times$, and any point $P(\mathbf{p})$, we have*

(1) $\delta_{P,-r} = \rho_O\delta_{P,r}$;

(2) $\delta_{P,1} = 1, \delta_{P,-1} = \rho_P$;

(3) $\delta_{P,r}\delta_{P,s} = \delta_{P,rs}$;

(4) $\delta_{P,r}^{-1} = \delta_{P,r^{-1}}$.

Proposition 6.11. *The set $\{\delta_{C,r} \mid r \in \mathbb{R}^\times (:= \mathbb{R} - 0)\}$ forms a group that is isomorphic to the group $(\mathbb{R}^\times, \cdot)$.*