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 $(\mathbf{x}-\mathbf{m})\,\mathbf{.}\,(\mathbf{p}-\mathbf{q}) = 0$ 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: $\|\mathbf{a} = \sqrt{\mathbf{a}\,\mathbf{.}\,\mathbf{a}}\|$;
- 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: $\mathbf{a} \perp \mathbf{b} \iff \mathbf{a}\,\mathbf{.}\,\mathbf{b} = 0$;

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 $\mathscr{I} = \mathscr{T}\mathscr{O} := \{\tau\sigma \mid \tau \in \mathscr{T}, \sigma \in \mathscr{O}\}$.*