

# Abstract Algebra and Fundamental Analysis

Jeremy Le — UNSW MATH2701 24T3

## Contents

<b>1</b>	<b>Algebra (Geometry)</b>	<b>2</b>
1.1	Transformations and Groups . . . . .	2
1.2	Subgroups and the Group of Isometries . . . . .	3
1.3	Reflections and Isometries . . . . .	4
1.4	Translations and Rotations on $\mathbb{R}^2$ . . . . .	5
1.5	Classification of Plane Isometries . . . . .	6
1.6	Similarities . . . . .	7
1.7	Dilatations . . . . .	8
1.8	Classification of Plane Similarities . . . . .	8
1.9	Normal Subgroups . . . . .	9
1.10	Collineations . . . . .	9
1.11	Darboux's Theorem . . . . .	9
1.12	Affine Transformations . . . . .	10
1.13	The Real Projective Line $\mathbb{R}P^1$ , Plane $\mathbb{R}P^2$ and Space $\mathbb{R}P^n$ . . . . .	11
1.14	The Principle of Duality in $\mathbb{R}P^2$ . . . . .	11
1.15	Desargues' Theorem and Pappus' Theorem . . . . .	12
1.16	Projective Transformations in $\mathbb{R}P^n$ . . . . .	12
1.17	Projective Plane Transformations . . . . .	13
<b>2</b>	<b>Analysis</b>	<b>14</b>
2.1	Asymptotics . . . . .	14
2.2	Inequalities . . . . .	15
2.2.1	Basic Inequalities . . . . .	15
2.2.2	Role of Convexity . . . . .	15
2.2.3	The Cauchy-Schwarz and Hölder Inequalities . . . . .	15
2.3	Norms and Convex Bodies . . . . .	16
2.3.1	$p$ -norms . . . . .	16
2.3.2	Convex Bodies . . . . .	16
2.4	Duality . . . . .	17
2.4.1	Dual Norms . . . . .	17
2.4.2	Polar Bodies . . . . .	17
2.4.3	Seperating Hyperplanes . . . . .	17
2.4.4	Mahler Volume . . . . .	17
2.5	Prime Numbers . . . . .	18
2.5.1	Infinitude of Primes . . . . .	18
2.5.2	Elementary Estimates for the Growth of $\pi(x)$ . . . . .	18
2.5.3	Statement of the Prime Number Theorem . . . . .	18

# 1 Algebra (Geometry)

## 1.1 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  $\mathcal{B}(\mathbb{R}^n)$  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

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

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

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

(3) *The set  $\mathcal{C}(\mathbb{R}^n)$  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  $f : G \rightarrow H$  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  $G \cong H$ .

## 1.2 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:  $A, B, C, P, Q, R, \dots$  with position vectors  $\mathbf{a}, \mathbf{b}, \mathbf{c}, \mathbf{p}, \mathbf{q}, \mathbf{r}, \dots$ ;
- transformations:  $\tau, \pi, \sigma, \delta, \dots$ ;
- lines:  $l, m, n, \dots$ ; 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  $\overline{PQ}$  to be the hyperplane  $\mathbb{H}$  that passes through the midpoint of  $\overline{PQ}$  and perpendicular to  $\overline{PQ}$ . So  $\mathbb{H}$  has the equation  $(\mathbf{x} - \mathbf{m}) \cdot (\mathbf{p} - \mathbf{q}) = 0$  where  $\mathbf{m} = \frac{1}{2}(\mathbf{p} + \mathbf{q})$ .
- 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:  $\|\mathbf{a}\| = \sqrt{\mathbf{a} \cdot \mathbf{a}}$ ;
- Distance between two points  $P, Q$ :  $d(P, Q) := \|\mathbf{p} - \mathbf{q}\|$ ;
- Projection of  $\mathbf{a}$  on  $\mathbf{b}$ :  $\text{proj}_{\mathbf{b}}(\mathbf{a}) = \frac{\mathbf{a} \cdot \mathbf{b}}{\mathbf{b} \cdot \mathbf{b}} \mathbf{b}$ ;
- Angle between  $\mathbf{a}$  and  $\mathbf{b}$ :  $\cos(\theta) = \frac{\mathbf{a} \cdot \mathbf{b}}{\|\mathbf{a}\| \|\mathbf{b}\|}$ ;
- Orthogonality:  $\mathbf{a} \perp \mathbf{b} \iff \mathbf{a} \cdot \mathbf{b} = 0$ ;

**Definition 2.3.** An *isometry* on  $\mathbb{R}^n$  is a map  $\tau : \mathbb{R}^n \rightarrow \mathbb{R}^n$  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  $\tau \in \mathcal{I}(\mathbb{R}^n)$ , 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  $\mathcal{I}(\mathbb{R}^n)$  of all isometries forms a subgroup of the group  $\mathcal{B}(\mathbb{R}^n)$  of all transformations.*
- (2) *The group  $\mathcal{I} = \mathcal{I}(\mathbb{R}^n)$  contains two subgroups: the group  $\mathcal{T}$  of translations and the group  $\mathcal{O}$  of all orthogonal linear transformations. Moreover, we have  $\mathcal{I} = \mathcal{T}\mathcal{O} := \{\tau\sigma \mid \tau \in \mathcal{T}, \sigma \in \mathcal{O}\}$ .*

### 1.3 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:

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

(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  $Q = I - \frac{2}{\mathbf{n} \cdot \mathbf{n}} \mathbf{n} \mathbf{n}^T \in O_n(\mathbb{R})$  and  $\mathbf{b} = 2 \frac{\mathbf{a} \cdot \mathbf{n}}{\mathbf{n} \cdot \mathbf{n}} \mathbf{n}$  such that

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

**Corollary 3.4.** In  $\mathbb{R}^2$ , if line  $\ell$  has equation  $aX + bY + c = 0$ , then the reflection  $\sigma_{\ell}$  in  $\ell$  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  $P_1(\mathbf{p}_1), P_2(\mathbf{p}_2), \dots, P_m(\mathbf{p}_m)$  in  $\mathbb{R}^n$  are in **generic position** if the vectors  $\mathbf{p}_i - \mathbf{p}_1$ , for  $i = 2, 3, \dots, m$ , 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  $\mathcal{I}(\mathbb{R}^n)$  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  $\tau \in \mathcal{I}(\mathbb{R}^2)$  is a product of at most three reflections in three lines.

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

**Theorem 4.1.** *An isometry  $\tau$  in  $\mathbb{R}^n$  is a **translation** if and only if  $\tau$  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  $\theta$ , 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  $\theta$  (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  $\mathcal{I}(\mathbb{R}^2)$  of isometries; further still, it is a **commutative** subgroup. In other words,*

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

**Theorem 4.6** (Equation of a rotation). (1) *The rotation  $\rho_{\mathbf{0},\theta} : \mathbb{R}^2 \rightarrow \mathbb{R}^2$  about the origin  $\mathbf{0}$  and through angle  $\theta$  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,  $\rho_{C,\theta}$  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  $\mathcal{R}_C = T_{\mathbf{c}}\mathcal{R}_0T_{-\mathbf{c}}$ . Call the group  $\mathcal{R}_C$  is **conjugate** to the group  $\mathcal{R}_0$ .*

**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  $\tau$  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  $\tau$  such that*

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

## 1.5 Classification of Plane Isometries

**Definition 5.1.** A plane isometry  $\tau$  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  $\mathcal{E}$  of even isometries in  $\mathbb{R}^n$  forms a subgroup of  $\mathcal{I}$ .*

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

3. *If  $\sigma = \sigma_H$  is a reflection, then  $\mathcal{E}' = \sigma \mathcal{E} := \{\sigma \pi \mid \pi \in \mathcal{E}\}$ .*

4. *We also have  $\sigma \mathcal{E} = \mathcal{E} \sigma$  and  $\mathcal{I} = \mathcal{E} \sqcup \sigma \mathcal{E}$ .*

**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  $\Omega$  is an isometry  $\tau$  such that  $\tau(\Omega) = \Omega$ .

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

## 1.6 Similarities

**Definition 6.1.** A transformation  $\alpha : \mathbb{R}^n \rightarrow \mathbb{R}^n$  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  $\mathcal{S}$  or  $\mathcal{S}(\mathbb{R}^n)$ .*

**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  $\alpha$  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  $\tau, \tau'$ . Moreover, we have*

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

where  $\mathcal{S} S_{P,r} = \{\tau S_{P,r} \mid \tau \in \mathcal{S}\}$  and  $S_{P,r} \mathcal{S} = \{S_{P,r} \tau \mid \tau \in \mathcal{S}\}$ .

**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  $\rho_C : \mathbb{R}^n \rightarrow \mathbb{R}^n$  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  $\mathcal{H}$  (of  $\mathcal{S}$ ). Moreover,  $\mathcal{H}$  is a (disjoint) union of the set  $\mathcal{T}$  of all translations and the set of all point reflections: for a fixed  $C$ ,*

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

**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  $\mathbb{R}^\times = \{r \in \mathbb{R} \mid r \neq 0\}$ . 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  $(\mathbb{R}^\times, \cdot)$ .*

## 1.7 Dilatations

**Definition 7.1.** A collineation  $\delta$  on  $\mathbb{R}^n$  is called a **dilatation** if, for every line  $\ell$  in  $\mathbb{R}^n$ ,  $\ell \parallel \delta(\ell)$ .

**Proposition 7.2.** The set  $\mathcal{D}(\mathbb{R}^n)$  of all dilatations in  $\mathbb{R}^n$  forms a subgroup of  $\mathcal{C}(\mathbb{R}^n)$ .

**Lemma 7.3.** A dilatation that fixes two points is the identity map. Hence, for dilatations  $\delta_1, \delta_2$  and distinct point  $A, B$ , if  $\delta_1(A) = \delta_2(A)$  and  $\delta_1(B) = \delta_2(B)$ , then  $\delta_1 = \delta_2$ .

**Lemma 7.4.** (1) If  $A, B, C$  are collinear, distinct, with  $\frac{CB}{CA} = r \neq 0$ , then  $\delta_{C,r}(A) = B$ .

(2) For collinear points  $A, B, P, P'$ , if  $\frac{AP}{PB} = \frac{AP'}{P'B}$ , then  $P = P'$ .

(3) Let  $\tau$  be a dilatation and let  $\tau(P) = P'$  for every point  $P$ . If there exist points  $A, B$  such that  $\overrightarrow{AB}$  and  $\overrightarrow{A'B'}$  have the same (resp., opposite) direction, then, for any points  $C, D$ ,  $\overrightarrow{CD}$  and  $\overrightarrow{C'D'}$  have the same (resp., opposite) direction.

**Corollary 7.5.** If points  $A, B, C$  are sent to  $A', B', C'$  under a dilatation, then

$$\frac{AB}{A'B'} = \frac{BC}{B'C'} = \frac{CA}{C'A'}.$$

**Theorem 7.6.** A dilatation is either a translation or a dilation. Hence, every dilatation is a similarity.

## 1.8 Classification of Plane Similarities

**Definition 8.1.** We say that figure  $f_1 \subseteq \mathbb{R}^n$  and figure  $f_2 \subseteq \mathbb{R}^n$  are **similar** if there is a similarity  $\alpha$  such that  $\alpha(f_1) = f_2$ .

**Theorem 8.2.** If  $\triangle ABC \sim \triangle A'B'C'$  in  $\mathbb{R}^2$ , then there exists a **unique** plane similarity  $\alpha$  such that

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

**Theorem 8.3** (Equations of Similarities). If  $\alpha$  is a similarity in  $\mathbb{R}^n$ , then there exist  $Q \in O_n(\mathbb{R})$ ,  $\mathbf{b} \in \mathbb{R}^n$  and  $r \in \mathbb{R}_{>0}$  such that

$$\alpha(\mathbf{x}) = rQ\mathbf{x} + \mathbf{b}, \quad \text{for all } \mathbf{x} \in \mathbb{R}^n.$$

**Lemma 8.4.** A similarity without a fixed point is an isometry.

**Definition 8.5.** (1) A **stretch reflection** in  $\mathbb{R}^2$  is a non-identity stretch about some point  $C$  followed by a reflection about a line through  $C$ .

(2) A **stretch rotation** in  $\mathbb{R}^2$  is a non-identity stretch about some point  $C$  followed by a non-identity rotation about  $C$ .

**Theorem 8.6.** A non-identity plane similarity is exactly one of the following:

Isometry,    Stretch of ratio  $r \neq 1$ ,    Stretch reflections,    Stretch rotation.

**Theorem 8.7.** In the equation of similarities, the algebraic classification is as follows:

1.  $\alpha$  is an isometry if  $r = 1$ ;
2.  $\alpha$  is a stretch (of ratio  $r \neq 1$ ) if  $r \neq 1$  and  $Q = I$ ;
3.  $\alpha$  is a stretch reflection if  $r \neq 1, Q \neq I$  and  $\det(Q) = -1$ ;
4.  $\alpha$  is a stretch rotation if  $r \neq 1, Q \neq I$  and  $\det(Q) = 1$ ;



## 1.9 Normal Subgroups

**Definition 9.1.** A subgroup  $K$  of a group  $G$  is called a **normal subgroup** if  $g^{-1}Kg \leq K$  (equivalently,  $g^{-1}Kg = K$ , or  $gK = Kg$ ) for all  $g \in G$ . **Notation:**  $K \trianglelefteq G$ .

**Theorem 9.2.** Suppose  $\alpha \in \mathcal{S}$  is a similarity, and  $G \in \{\mathcal{I}, \mathcal{E}, \mathcal{D}, \mathcal{H}, \mathcal{T}\}$ . Then  $\alpha\tau\alpha^{-1} \in G$ , for all  $\tau \in G$ . In other words, each of the groups  $\mathcal{I}, \mathcal{E}, \mathcal{D}, \mathcal{H}, \mathcal{T}$  is a normal subgroup of  $\mathcal{S}$ .

**Corollary 9.3.** For  $\alpha \in \mathcal{S}$ , a point  $C$  and a hyperplane  $\mathbb{H}$  in  $\mathbb{R}^n$ , we have

$$\alpha\sigma_{\mathbb{H}}\alpha^{-1} = \sigma_{\alpha(\mathbb{H})}, \quad \alpha\rho_C\alpha^{-1} = \rho_{\alpha(C)}, \quad \alpha\delta_{C,r}\alpha^{-1} = \delta_{\alpha(C),r}.$$

In particular, in  $\mathbb{R}^2$ ,  $\alpha\rho_{C,\theta}\alpha^{-1} = \rho_{\alpha(C),\pm\theta}$ .

**Proposition 9.4.** 1. If  $H \leq G$ , then  $G$  is a disjoint union of **cosets**  $gH, g \in G$ .

2. If  $K \trianglelefteq G$ , then  $G/K := \{gk \mid g \in G\}$  is a group with the subset multiplication. ( $G/K$  is called the **quotient group** of  $G$  by  $K$ ).

## 1.10 Collineations

**Theorem 10.1.** A transformation is a collineation in  $\mathbb{R}^n$  if and only if the images of collinear points are themselves collinear.

**Lemma 10.2.** If  $\alpha$  is a collineation in  $\mathbb{R}^n$ , and  $l, m$  are parallel lines, then  $\alpha(l)$  and  $\alpha(m)$  are parallel.

**Theorem 10.3.** A collineation takes the midpoint of points  $A, B$  to the midpoints of points  $\alpha(A), \alpha(B)$ .

**Corollary 10.4.** For a collineation  $\alpha$ , if  $n+1$  points  $P_0, P_1, \dots, P_n$  divide the segment  $\overline{P_0P_n}$  into  $n$  congruent segments  $\overline{P_{i-1}P_i}$ , and  $P'_i = \alpha(P_i)$ , then the  $n+1$  points  $P'_0, \dots, P'_n$  divide the segment  $\overline{P'_0P'_n}$  into  $n$  congruent segments  $\overline{P'_{i-1}P'_i}$ .

In particular, if a point  $P$  is between  $A$  and  $B$ , and  $\frac{AP}{PB} = r$  is **rational**, then  $P' = \alpha(P)$  is between  $\alpha(A)$  and  $\alpha(B)$  and  $\frac{A'P'}{P'B'} = r$ .

## 1.11 Darboux's Theorem

**Lemma 11.1.** Let  $t > 0, t \neq 1$ , and  $P, Q$  be points on  $\ell(A, B)$  such that  $\frac{AP}{PB} = t, \frac{AQ}{QB} = -t$ . Then  $C$  is the midpoint of  $P, Q$  if and only if  $\frac{AC}{CB} = -t^2$ .

**Theorem 11.2.** If  $\alpha$  is a collineation, and point  $P$  is between points  $A, B$  then  $\alpha(P)$  is between  $\alpha(A), \alpha(B)$ .

**Corollary 11.3.** A collineation on  $\mathbb{R}^n$  fixing two points on a line fixes the line pointwise.

## 1.12 Affine Transformations

**Theorem 12.1.** *A collineation in  $\mathbb{R}^n$  fixing  $n + 1$  points in generic position is the identity.*

**Definition 12.2.** An **affine transformation**  $\alpha : \mathbb{R}^n \rightarrow \mathbb{R}^n$  is one that has an equation of the form  $\alpha(\mathbf{x}) = A\mathbf{x} + \mathbf{b}$  for all  $\mathbf{x} \in \mathbb{R}^n$ , where  $A \in GL_n(\mathbb{R})$ ,  $\mathbf{b} \in \mathbb{R}^n$ . (In other words,  $\alpha = T_{A,\mathbf{b}}$ .)

**Lemma 12.3.** *The set  $\mathcal{A}$  of all affine transformations in  $\mathbb{R}^n$  forms a group. Moreover, it contains the similarity group  $\mathcal{S}$  as a subgroup of  $\mathcal{A}$ .*

**Theorem 12.4.** *Let  $\tau$  be a transformation. Then the following are equivalent:*

1.  $\tau$  is an affine transformation;
2.  $\tau$  is a collineation.

**Proposition 12.5.** *A (non-degenerate) conic section*

$$aX^2 + bXY + cY^2 + dX + eY + f = 0$$

*is affine equivalent to one of the following **affine standard form**:*

$$Y = X^2, \quad X^2 + Y^2 = 1, \quad XY = 1.$$

**Definition 12.6.** An affine transformation  $\alpha$  with equation  $\alpha(\mathbf{x}) = A\mathbf{x} + \mathbf{b}$  is called an **equi-affine transformation** if  $\det(\alpha) := \det(A) = \pm 1$ . An equi-affine transformation in  $\mathbb{R}^2$  is called an **equiareal transformation**.

**Proposition 12.7** (The group of equi-affine transformations). *The set  $\mathcal{Q}$  of all equi-affine transformations forms a subgroup of  $\mathcal{A}$  that has  $\mathcal{Q}^+ = \{\alpha \in \mathcal{Q} \mid \det(\alpha) = 1\}$  as a normal subgroup.*

**Theorem 12.8.** (1) *Let  $\alpha$  be an affine transformation in  $\mathbb{R}^2$  with equation  $\alpha(\mathbf{x}) = A\mathbf{x} + \mathbf{b}$  and let  $\alpha(P) = P'$ , etc., then  $\text{area}(\triangle P'Q'R') = |\det A| \text{area}(\triangle PQR)$ .*

(2) *If  $\Omega$  is the parallelepiped spanned by the vectors  $\mathbf{a}, \mathbf{b}, \mathbf{c}$  in  $\mathbb{R}^3$  and  $\alpha$  is an affine transformation in  $\mathbb{R}^3$ , then  $\text{vol}(\alpha\Omega) = |\det(A)| \text{vol}(\Omega)$ .*

### 1.13 The Real Projective Line $\mathbb{R}P^1$ , Plane $\mathbb{R}P^2$ and Space $\mathbb{R}P^n$

**Definition 13.1.** (1) The real projective plane  $\mathbb{R}P^2$  is defined as the extended Euclidean plane

$$\mathbb{R}P^2 := \mathbb{R}^2 \sqcup \mathbb{R}P^1$$

The points in  $b\mathbb{R}^2$  (resp.,  $\mathbb{R}P^1$ ) are called **ordinary** (resp., **ideal**) points and  $\ell_\infty := \mathbb{R}P^1$  is called the **ideal (projective) line**.

(2) In general, for  $n \geq 3$ , define the  $n$ -dimensional real projective space

$$\mathbb{R}P^n = \underbrace{\mathbb{R}^n}_{\text{ordinary points}} \sqcup \underbrace{\mathbb{R}P^{n-1}}_{\text{ideal points}}$$

as a disjoint union of the **ordinary** part  $\mathbb{R}^n$  and the **ideal** part  $\mathbb{R}P^{n-1}$

**Proposition 13.2.** *Two distinct **projective lines** have **exactly one** point of intersection.*

### 1.14 The Principle of Duality in $\mathbb{R}P^2$

**Definition 14.1.** • A projective point in  $\mathbb{R}P^n$  is a 1-dimensional subspace of  $\mathbb{R}^{n+1}$ . For  $P[x_0, x_1, \dots] \in \mathbb{R}P^n$ , we also write  $P = \langle \mathbf{x} \rangle$ , the dimensional subspace spanned by  $\mathbf{x}$  which is the column vector  $(x_0, x_1, \dots, x_n)^T$ .

- A projective **line** in  $b\mathbb{R}P^n$  is a 2-dimensional subspace of  $\mathbb{R}^{n+1}$ . If  $P = \langle \mathbf{p} \rangle, Q = \langle \mathbf{q} \rangle$  are distinct projective points then  $p\ell(P, Q) = \langle \mathbf{p}, \mathbf{q} \rangle$ , the subspace spanned by  $\mathbf{p}, \mathbf{q}$ .
- A projective **plane** in  $\mathbb{R}P^n$  is a 3-dimensional subspace of  $\mathbb{R}^{n+1}$ .
- A projective **hyperplane** in  $b\mathbb{R}P^n$  is a  $n$ -dimensional subspace of  $b\mathbb{R}^{n+1}$ .
- A projective point  $P = \langle \mathbf{x} \rangle$  lies on a projective line  $h = \langle \mathbf{p}, \mathbf{q} \rangle$  if the one dimensional subspace  $\langle \mathbf{x} \rangle$  is a **subspace** of the two dimensional subspace  $\langle \mathbf{p}, \mathbf{q} \rangle$ .
- The **Real Projective Plane**  $\mathbb{R}P^2$  is the set of all projective points  $\langle \mathbf{x} \rangle, \mathbf{x} \in \mathbb{R}^3 - \{\mathbf{0}\}$ , and lines  $\langle \mathbf{p}, \mathbf{q} \rangle$  with  $\langle \mathbf{p} \rangle \neq \langle \mathbf{q} \rangle$ , together with the above incidence structure.

**Proposition 14.2.** *In  $b\mathbb{R}P^2$ , any two projective points lie on exactly one projective line, and any two projective lines intersect in exactly one projective point.*

**Lemma 14.3.** *For subspaces  $U, V$  of  $\mathbb{R}^n$ , we have*

$$(U + V)^\perp = U^\perp \cap V^\perp \quad \text{and} \quad (U \cap V)^\perp = U^\perp + V^\perp.$$

**Principle of Duality** In  $\mathbb{R}P^2$ , any true statement involving points and straight lines remains true if the words “points” and “lines” are interchanged (i.e.,  $\langle \mathbf{x} \rangle \leftrightarrow \langle \mathbf{x} \rangle^\perp$ ). E.g.,

- Any two projective points **lie on** exactly one projective line.
- Any two projective lines **intersect in** exactly one projective point.

**Lemma 14.4.** *Projective points  $\langle \mathbf{p} \rangle, \langle \mathbf{q} \rangle, \langle \mathbf{r} \rangle$  in  $\mathbb{R}P^2$  are **collinear** if and only if projective lines  $\langle \mathbf{p} \rangle^\perp, \langle \mathbf{q} \rangle^\perp, \langle \mathbf{r} \rangle^\perp$  are **concurrent**.*

## 1.15 Desargues' Theorem and Pappus' Theorem

**Proposition 15.1.** (1) Three distinct projective points  $P = \langle \mathbf{p} \rangle, Q = \langle \mathbf{q} \rangle$ , and  $R = \langle \mathbf{r} \rangle$  in  $\mathbb{RP}^n$ , are collinear if and only if the vectors  $\mathbf{p}, \mathbf{q}, \mathbf{r}$  are linearly dependent. Moreover, we may choose  $\mathbf{p}, \mathbf{q}, \mathbf{r}$  to satisfy  $\mathbf{p} = \mathbf{q} + \mathbf{r}$ .

(2) Four distinct projective points  $P = \langle \mathbf{p} \rangle, Q = \langle \mathbf{q} \rangle, R = \langle \mathbf{r} \rangle$  and  $S = \langle \mathbf{s} \rangle$  in  $\mathbb{RP}^n$ , no three of which are collinear, are coplanar if and only if the vectors  $\mathbf{p}, \mathbf{q}, \mathbf{r}, \mathbf{s}$  are linearly dependent. Moreover, we may choose  $\mathbf{p}, \mathbf{q}, \mathbf{r}, \mathbf{s}$  to satisfy  $\mathbf{p} = \mathbf{q} + \mathbf{r} + \mathbf{s}$ .

**Theorem 15.2** (Desargues' Theorem). Let  $A, B, C, A', B', C'$  be distinct points in  $\mathbb{RP}^2$ , such that the projective lines  $pl(A, A'), pl(B, B'), pl(C, C')$  are **distinct** and **concurrent**. Then the projective points of intersections  $C'' = pl(A, B) \cap pl(A', B'), A'' = pl(B, C) \cap pl(B', C'), B'' = pl(A, C) \cap pl(A', C')$  are **collinear**.

**Dual Desargues' Theorem** Let  $l, m, n, l', m', n'$  be distinct lines in  $\mathbb{RP}^2$  such that their intersections  $l \cap l', m \cap m', n \cap n'$  are distinct projective points, and collinear. Then the projective lines joining  $l \cap m, l' \cap m'$ , and  $m \cap n, m' \cap n'$ , and  $n \cap l, n' \cap l'$  are concurrent.

**Theorem 15.3** (Pappus' Theorem). Let  $A, B, C$  and  $A', B', C'$  be two pairs of collinear triples of distinct points in a projective plane. Then the three points  $A'' = pl(B, C') \cap pl(B', C), B'' = pl(C, A') \cap pl(C', A)$  and  $C'' = pl(A, B') \cap pl(A', B)$  are collinear.

**Dual Pappus' Theorem** Let  $l, m, n, l', m', n'$  be two pairs of concurrent projective lines in  $\mathbb{RP}^2$ . Then the projective lines  $pl(m \cap n', m' \cap n), pl(n' \cap l, n \cap l'), pl(l \cap m', l' \cap m)$  are concurrent.

## 1.16 Projective Transformations in $\mathbb{RP}^n$

**Definition 16.1.** A map  $\pi : \mathbb{RP}^n \rightarrow \mathbb{RP}^n$  is called a *projective transformation* if there exists an **invertible** matrix  $A \in GL_{n+1}(\mathbb{R})$  such that  $\pi \langle \mathbf{x} \rangle = \langle A\mathbf{x} \rangle$ .

**Proposition 16.2.** (1) A **linear isomorphism**  $T_A : \mathbb{R}^{n+1} \rightarrow \mathbb{R}^{n+1}$  induces a projective transformation  $\pi_A : \mathbb{RP}^n \rightarrow \mathbb{RP}^n, \langle x \rangle \mapsto \langle A\mathbf{x} \rangle$ .

(2) For  $A, A' \in GL_{n+1}(\mathbb{R}), \pi_A = \pi_{A'} \iff A = \lambda A', \text{ for some } \lambda \in \mathbb{R}^\times$ .

**Theorem 16.3.** Let  $\mathcal{P} = \mathcal{P}(\mathbb{RP}^n)$  be the set of all projective transformations on  $\mathbb{RP}^n$ . Then  $\mathcal{P}$  is a group, called the **group of projective transformations**.

**Theorem 16.4.** (1) The set  $PGL_{n+1}(\mathbb{R})$  with coset multiplication forms a group, the **projective linear group**. This is the **quotient group**  $GL_{n+1}(\mathbb{R})/\mathcal{K}_{n+1}$  with  $\mathcal{K}_{n+1} := \mathbb{R}^\times I_{n+1} = \{\lambda I_{n+1} \mid \lambda \in \mathbb{R}^\times\}$ .

(2) The map  $\phi : PGL_{n+1}(\mathbb{R}) \rightarrow \mathcal{P}, [A] \mapsto \pi_A$  is a **bijection**, satisfying:  $\phi([A][B]) = \phi([A])\phi([B])$ . That is, the map  $\phi$  is a group isomorphism.

**Theorem 16.5.** Every affine transformation  $T_{A, \mathbf{b}}$  on  $\mathbb{R}^n$  can be **uniquely** extended to a projective transformation  $\pi \left( \begin{smallmatrix} 1 & 0 \\ \mathbf{b} & A \end{smallmatrix} \right)$  on  $\mathbb{RP}^n$  which stabilises the ideal part and the ordinary part and preserves multiplication and inverses. In group theory, terminology,  $\mathcal{A}$  is (isomorphic to) a subgroup of  $\mathcal{P}$ . That is,  $\mathcal{A} \equiv \mathcal{A}' \leq \mathcal{P}$ .

## 1.17 Projective Plane Transformations

**Theorem 17.1.** *Let  $f = \{P, Q, R, S\}$  and  $P', Q', R', S'$  be two sets of four points, no three of which are collinear in  $\mathbb{R}P^2$ . Then there is a unique  $\pi \in \mathcal{P}$  such that  $\pi(P) = P', \pi(Q) = Q', \pi(S) = S'$ .*

**Proposition 17.2.** *For two figures  $f, g \subseteq \mathbb{R}^n$ , if they are affine equivalent, then the images  $f, g$  in  $\mathbb{R}P^n$  are projective equivalent.*

**Theorem 17.3.** *All non-degenerate conic sections are projective equivalent.*

**Definition 17.4.** A bijective map  $\tau : \mathbb{R}P^2 \rightarrow \mathbb{R}P^2$  is called a **(projective) collineation** if  $\tau$  takes collinear points to collinear points. (Equivalently,  $\tau$  sends any projective line to a projective line.)

**Lemma 17.5.** *If  $\tau$  is a collineation of  $\mathbb{R}P^2$  and  $\tau$  fixes points*

$$P_1 = [1, 0, 0], P_2 = [0, 1, 0], P_3 = [0, 0, 1], Q = [1, 1, 1],$$

*then  $\tau$  is the **identity** map.*

**Theorem 17.6.** *A bijective map  $\tau$  on  $\mathbb{R}P^2$  is a projective collineation if and only if  $\tau$  is a projective transformation.*

## 2 Analysis

### 2.1 Asymptotics

**Definition 1.1** (Big-Oh). Let  $f, g$  be functions defined on an interval of the form  $(a, \infty)$ . We shall say that

$$f(x) = O(g(x)), \quad (\text{as } x \rightarrow \infty)$$

if there exists  $M > 0$  and  $x_0 > a$  such that for all  $x > x_0$ ,

$$|f(x)| \leq M|g(x)|.$$

**Definition 1.2** (Big-Oh at  $a$ ). Let  $f, g$  be functions defined on an open interval containing  $a$ . We shall say that

$$f(x) = O(g(x)), \quad (\text{as } x \rightarrow a)$$

if there exists  $M > 0$  and  $\delta > 0$  such that if  $|x - a| < \delta$ ,

$$|f(x)| \leq M|g(x)|.$$

**Definition 1.3.** We shall say that  $f(x) = o(g(x))$  as  $x \rightarrow \infty$  if for all  $\epsilon > 0$ , there exists  $x_0 = x_0(\epsilon)$  such that if  $x > x_0$ , then  $|f(x)| < \epsilon|g(x)|$ . We say  $f(x)$  is *little-oh* of  $g(x)$ .

**Definition 1.4.** We shall write that  $f(x) = \theta(g(x))$  (as  $x \rightarrow \infty$ ) if  $f(x) = O(g(x))$  and  $g(x) = O(f(x))$  (as  $x \rightarrow \infty$ ). That is, there are non-zero constants  $M_1, M_2$  and  $x_0$  such that for all  $x > x_0$

$$M_1|g(x)| \leq |f(x)| \leq M_2|g(x)|.$$

**Definition 1.5.** We shall say that  $f(x) \sim g(x)$  as  $x \rightarrow \infty$  if  $\frac{f(x)}{g(x)} \rightarrow 1$  as  $x \rightarrow \infty$ .

## 2.2 Inequalities

### 2.2.1 Basic Inequalities

1. Triangle inequality:  $|x + y| \leq |x| + |y|$ .
2. The sum inequality:  $\left| \sum_{k=1}^n x_k y_k \right| \leq \max\{|x_k|\} \sum_{k=1}^n |y_k|$ .
3. The integral inequality:  $\left| \int_a^b f(x)g(x) \, dx \right| \leq \max_{a \leq x \leq b} \{|f(x)|\} \int_a^b |g(x)| \, dx$ .
4. The AM-GM inequality: if  $x, y > 0$  then  $(xy)^{1/2} \leq \frac{x+y}{2}$ .
5. The Cauchy-Schwarz inequality:  $\left| \sum_{k=1}^n x_k y_k \right| \leq \left( \sum_{k=1}^n x_k^2 \right)^{1/2} \left( \sum_{k=1}^n y_k^2 \right)^{1/2}$ .

**Theorem 2.1** (Generalized AM-GM inequality). *Suppose that  $x_1, x_2, \dots, x_n$  are positive. Then*

$$(x_1 x_2 \dots x_n)^{1/n} \leq \frac{1}{n} \sum_{k=1}^n x_k$$

(with equality if and only if all the  $x_k$  are equal).

### 2.2.2 Role of Convexity

**Definition 2.2.** A function  $f : \mathbb{R} \rightarrow \mathbb{R}$  is **convex** if for any  $x_1, x_2 \in \mathbb{R}$  and any  $t \in [0, 1]$

$$f(tx_1 + (1-t)x_2) \leq tf(x_1) + (1-t)f(x_2).$$

**Theorem 2.3** (Jensen's Inequality). *Suppose that  $f : \mathbb{R} \rightarrow \mathbb{R}$  is convex, that  $x_1, \dots, x_n \in \mathbb{R}$  and  $a_1, \dots, a_n > 0$ . Then*

$$f\left(\frac{\sum a_i x_i}{\sum a_j}\right) \leq \frac{\sum a_i f(x_i)}{\sum a_j}.$$

### 2.2.3 The Cauchy-Schwarz and Hölder Inequalities

**Theorem 2.4** (Hölder Inequality). *Suppose that  $1 < p, q < \infty$  with  $\frac{1}{p} + \frac{1}{q} = 1$ . Then for any numbers  $x_1, \dots, x_n, y_1, \dots, y_n$ ,*

$$\left| \sum_{k=1}^n x_k y_k \right| \leq \left( \sum_{k=1}^n |x_k|^p \right)^{1/p} \left( \sum_{k=1}^n |y_k|^q \right)^{1/q}.$$

**Theorem 2.5** (Hölder's inequality for integrals). *Suppose that  $f, g : [a, b] \rightarrow \mathbb{R}$  (or to  $\mathbb{C}$ ) are continuous, and that  $1 < p, q < \infty$  with  $\frac{1}{p} + \frac{1}{q} = 1$ . Then*

$$\left| \int_a^b f(t)g(t) \, dt \right| \leq \int_a^b |f(t)g(t)| \, dt \leq \left( \int_a^b |f(t)|^p \, dt \right)^{1/p} \left( \int_a^b |g(t)|^q \, dt \right)^{1/q}.$$

## 2.3 Norms and Convex Bodies

### 2.3.1 $p$ -norms

**Definition 3.1.** Let  $V$  be a vector space. A norm on  $V$  is a function  $\mathbf{x} \mapsto \|\mathbf{x}\|$  from  $V$  to  $\mathbb{R}$  which satisfies

1.  $\|\mathbf{x}\| \geq 0$  for all  $\mathbf{x} \in V$  and  $\|\mathbf{x}\| = 0$  if and only if  $\mathbf{x} = 0$ .
2.  $\|\lambda\mathbf{x}\| = |\lambda|\|\mathbf{x}\|$  for all  $\mathbf{x} \in V$  and scalar  $\lambda$ .
3. (Triangle Inequality):  $\|\mathbf{x} + \mathbf{y}\| \leq \|\mathbf{x}\| + \|\mathbf{y}\|$  for all  $\mathbf{x}, \mathbf{y} \in V$ .

**Definition 3.2.** Let  $1 \leq p < \infty$ . For  $\mathbf{x} = (x_1, \dots, x_n) \in \mathbb{R}^n$  define

$$\|\mathbf{x}\|_p = \left( \sum_{k=1}^n |x_k|^p \right)^{1/p}.$$

**Theorem 3.3** (Minkowski's Inequality). *If  $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$ , then*

$$\|\mathbf{x} + \mathbf{y}\|_p \leq \|\mathbf{x}\|_p + \|\mathbf{y}\|_p.$$

### 2.3.2 Convex Bodies

**Definition 3.4.** A (nonempty) subset  $K$  of a vector space  $V$  is **convex** if for all  $\mathbf{x}, \mathbf{y} \in K$  and all  $\lambda \in [0, 1]$ ,

$$\lambda\mathbf{x} + (1 - \lambda)\mathbf{y} \in K.$$

That is,  $K$  contains all the line segments joining points in  $K$ .

**Proposition 3.5.** *Let  $(V, \|\cdot\|)$  be a normed vector space. Then the set*

$$K = \{\mathbf{x} \in V : \|\mathbf{x}\| \leq 1\}$$

*is convex.*

**Definition 3.6.** Suppose that  $\emptyset \neq K \subseteq \mathbb{R}^n$ . Then

1.  $K$  is said to be **centrally symmetric** with respect to the origin if  $\mathbf{x} \in K \iff -\mathbf{x} \in K$ .
2.  $K$  is **closed** if its complement is open ( $\iff$  it contains its boundary  $\iff$  it contains all its limit points).
3.  $K$  is **bounded above and below** if there exist  $0 < c \leq C < \infty$  such that  $B_c \subseteq K \subseteq B_C$  where  $B_c$  and  $B_C$  are the closed Euclidean ( $\|\cdot\|_2$ ) balls of radius  $c$  and  $C$ .

**Definition 3.7.** Suppose that  $\emptyset \neq K \subseteq \mathbb{R}^n$ . We say that  $K$  is a **convex body** if it is convex, centrally symmetric, closed and bounded above and below.

**Theorem 3.8.** *There is a one-to-one correspondence between convex bodies in  $\mathbb{R}^n$  and norms on  $\mathbb{R}^n$ .*

**Lemma 3.9.** *Let  $\|\cdot\|$  be a norm on  $\mathbb{R}^n$ . Define  $f : \mathbb{R}^n \rightarrow \mathbb{R}$  by  $f(\mathbf{x}) = \|\mathbf{x}\|$ . Then  $f$  is a continuous function from  $(\mathbb{R}^n, \|\cdot\|_2)$  to  $\mathbb{R}$ . That is, if  $\|\mathbf{x}_n - \mathbf{x}\|_2 \rightarrow 0$ , then  $f(\mathbf{x}_n) \rightarrow f(\mathbf{x})$  (ie  $|f(\mathbf{x}_n) - f(\mathbf{x})| \rightarrow 0$ ).*



## 2.4 Duality

### 2.4.1 Dual Norms

**Definition 4.1.** Suppose that  $\|\cdot\|$  is a norm on  $\mathbb{R}^n$ . Its **dual norm** is defined by

$$\|\mathbf{x}\|^* = \sup_{\mathbf{y} \in \mathbb{R}^n} \frac{|\mathbf{x} \cdot \mathbf{y}|}{\|\mathbf{y}\|} = \sup_{\|\mathbf{y}\|=1} |\mathbf{x} \cdot \mathbf{y}|.$$

**Theorem 4.2.** *The dual norm is a norm.*

### 2.4.2 Polar Bodies

**Definition 4.3.** Let  $K$  be a convex body in  $\mathbb{R}^n$ . The polar of  $K$  is the convex body associated to the dual norm to  $\|\cdot\|_K$ .

**Theorem 4.4** (Polar Duality Theorem). *Let  $K$  be a convex body. Then  $K^{\circ\circ} = K$ .*

### 2.4.3 Separating Hyperplanes

**Definition 4.5.** A hyperplane  $H_{\mathbf{u}} = \{\mathbf{y} \in \mathbb{R}^n : \mathbf{y} \cdot \mathbf{u} = 1\}$  is a separating hyperplane for  $K$  and  $\mathbf{p}$  if

1.  $\mathbf{x} \cdot \mathbf{u} \leq 1$  for all  $\mathbf{x} \in K$  (ie all of  $K$  is on the ‘low side’ of  $H_{\mathbf{u}}$ ), and
2.  $\mathbf{p} \cdot \mathbf{u} \geq 1$ . (ie  $\mathbf{p}$  is on the high side of  $H_{\mathbf{u}}$ )

We say that  $H_{\mathbf{u}}$  is a strongly separating if  $\mathbf{p} \cdot \mathbf{u} > 1$ .

**Theorem 4.6** (Separating Hyperplane Theorem). *If  $K$  is a convex body and  $\mathbf{p}$  is a point not in  $K$ , then there exists a hyperplane that strongly separates them.*

### 2.4.4 Mahler Volume

**Definition 4.7.** The Mahler volume of a convex body  $K$  is defined as

$$M(K) = \text{vol}(K)\text{vol}(K^\circ).$$

**Lemma 4.8.** *Suppose that  $A$  is an invertible  $n \times n$  matrix and that  $K$  is a convex body. Then  $AK$  is a convex body with polar  $(A^T)^{-1}K^\circ$ .*

**Theorem 4.9.** *Let  $K \subseteq \mathbb{R}^n$  be a convex body and let  $A \in M_n$  be invertible. Then*

- $M(K) = M(K^\circ)$ .
- $M(AK) = M(K)$ .

## 2.5 Prime Numbers

### 2.5.1 Infinitude of Primes

**Theorem 5.1** (Fundamental Theorem of Arithmeitic). *Every natural number  $n$  can be written uniquely, up to re-ordering of the factors, as a product of primes.*

**Theorem 5.2** (Euclid). *There are  $\infty$ -ly many primes. As  $n$  tends to infinity, we have*

$$\sum_{p \leq n_{p \in \mathbb{P}}} \frac{1}{p} \rightarrow \infty.$$

### 2.5.2 Elementary Estimates for the Growth of $\pi(x)$

**Theorem 5.3** (Gauss). *For  $x \geq 2$ , we have  $\pi(x) \geq \log \log x$ .*

### 2.5.3 Statement of the Prime Number Theorem

**Theorem 5.4.** *There exists a constant  $c > 0$ , effectively computable such that for  $x \geq 2$*

$$\pi(x) = \text{Li}(x) + O \left[ x \exp \left( -c \sqrt{\log x} \right) \right],$$

*where the implied constant is absolute.*