PURE MATHEMATICS 319 LECTURE NOTE
CHAPTER 0

Definitions: Set theory notation: $\exists, \forall, \in, \mathbb{Z}, \mathbb{R}, \subset$. Let $G = \{\alpha, \beta, \gamma, ...\}$ be a non-empty set. A binary operation $\star$ on G is a map (function) $\star : G \times G \to G$. We put $\star(\alpha, \beta) = \alpha \star \beta$ for all $\alpha, \beta \in G$. We say that $\star$ is associative if $\forall \alpha, \beta, \gamma \in G, \alpha \star (\beta \star \gamma) = (\alpha \star \beta) \star \gamma$. We say that $\star$ is commutative if $\forall \alpha, \beta \in G, \alpha \star \beta = \beta \star \alpha$.

We say that $(G, \star)$ is a group if (a) $\star$ associative binary operation on G, (b) there is a unique element $i \in G$ so that $i \star \alpha = \alpha \star i$ for all $\alpha \in G$ (i is called the *identity* element of G), and (c) $\forall \alpha \in G, \exists \beta \in G$ so that $\alpha \star \beta = i$ (β is called the *inverse* of α, and we write $\beta = \alpha^{-1}$).

If $(G, \star)$ is a group and $\star$ is commutative, we say that $(G, \star)$ is an *abelian* group. For example, $(\mathbb{Z}, +)$ and $(R \setminus \{0\}, .)$ are abelian groups.

Let $(G, \star)$ be a group. A non-empty subset $H \subset G$ is a subgroup of $(G, \star)$ if $(H, \star)$ is a group itself.

Proposition: *$(H, \star)$ is a subgroup of $(G, \star) \Longleftrightarrow \forall \alpha, \beta \in H, \alpha \star \beta^{-1} \in H$.*

Proof:

$(\Longrightarrow)$ It is clear that if $(H, \star)$ is a subgroup of $(G, \star)$ then $\alpha \star \beta^{-1} \in H$ for all $\alpha, \beta \in H$.

$(\Longleftarrow)$ Suppose that $\alpha \star \beta^{-1} \in H$ for all $\alpha, \beta \in H$. Since $H \neq \emptyset$, there is $\gamma \in H$ and so $i = \gamma \star \gamma^{-1} \in H$, and so for any $\alpha \in H$, $\alpha^{-1} = i \star \alpha^{-1} \in H$. Furthermore, for any $\alpha, \beta \in H$, $\alpha \star \beta = \alpha \star (\beta^{-1})^{-1} \in H$. In addition, $\star$ is an associative binary operation on H and so $(H, \star)$ is a group.□

Proposition: *For all $\alpha, \beta, \gamma \in G$ where $(G, \star)$ is a group,*

$\alpha \star \beta = \alpha \star \gamma \Longrightarrow \beta = \gamma$ *(left-cancellation), and*

$\beta \star \alpha = \gamma \star \alpha \Longrightarrow \beta = \gamma$ *(right-cancellation), and*

$(\alpha \star \beta)^{-1} = \beta^{-1} \star \alpha^{-1}$.

Proof: $\alpha \star \beta = \alpha \star \gamma \Longrightarrow \alpha^{-1} \star (\alpha \star \beta) = \alpha^{-1} \star (\alpha \star \gamma) \Longrightarrow (\alpha^{-1} \star \alpha) \star \beta = (\alpha^{-1} \star \alpha) \star \gamma \Longrightarrow i \star \beta = i \star \gamma \Longrightarrow \beta = \gamma$. Similarly, we can prove the right-cancellation property of $\star$.

Next, for any $\alpha, \beta \in G$, we put $\delta = (\alpha \star \beta)^{-1}$. Then $\delta \star (\alpha \star \beta) = i$. Also, $(\beta^{-1} \star \alpha^{-1}) \star (\alpha \star \beta) = (\beta^{-1} \star (\alpha^{-1} \star \alpha)) \star \beta = (\beta^{-1} \star i) \star \beta = \beta^{-1} \star \beta = i$. Thus, $\delta \star (\alpha \star \beta) = (\beta^{-1} \star \alpha^{-1}) \star (\alpha \star \beta)$, and so by right-cancellation property of $\star$, we get that $\delta = \beta^{-1} \star \alpha^{-1}$, that is, $(\alpha \star \beta)^{-1} = \beta^{-1} \star \alpha^{-1}$.□

Definitions: For any $\alpha \in G$, we put $\alpha^0 = i$, and for positive integers n, we put $\alpha^n = \alpha \star \alpha^{n-1}$, and $\alpha^{-n} = (\alpha^{-1})^n$.

If G has exactly n elements, we say that G is *finite*. Otherwise, we say that G is *infinite*. Let $\alpha \in G$. If there is a smallest positive integer n so that $\alpha^n = i$, we say that α is an element of *order* n. Otherwise, we say that α is an element of *infinite order*.

Let H be a subgroup of G. If there is an element $\alpha \in H$ so that $H = \{\alpha^n \mid n \in \mathbb{Z}\}$, then we write $H = \langle \alpha \rangle$ and we call $\langle \alpha \rangle$ the *cyclic group generated by* α. It is clear that cyclic groups are abelian.

In general, the group generated by the elements $\alpha_1, \alpha_2, \alpha_3, ..., \alpha_k$ is $\langle \alpha_1, \alpha_2, \alpha_3, ..., \alpha_k \rangle$ $= \{\beta_1^{m_1} \star \beta_2^{m_2} \star \beta_3^{m_3} \star ... \star \beta_n^{m_n} \mid m_1, m_2, m_3, ..., m_n \in \mathbb{Z}$ and $\beta_1, \beta_2, \beta_3, ..., \beta_n \in \{\alpha_1, \alpha_2, \alpha_3, ..., \alpha_k\}\}$.

We note that if α is an element of order n then $\langle\alpha\rangle = \{\alpha, \alpha^2, \alpha^3, ..., \alpha^n\}$ is a group of n elements, and if α is an element of infinite order then $\langle\alpha\rangle = \{..., \alpha^{-3}, \alpha^{-2}, \alpha^{-1}, i, \alpha^2, \alpha^3, ...\}$ an infinite group.

Example: The cyclic group $C_4 = \langle\alpha\rangle$ and the group $V_4 = \langle\alpha, \beta\rangle$ can be understood by the following tables:

C_4	i	α	α^2	α^3
i	i	α	α^2	α^3
α	α	α^2	α^3	i
α^2	α^2	α^3	i	α
α^3	α^3	i	α	α^2

V_4	i	α	β	$\alpha\beta$
i	i	α	β	$\alpha\beta$
α	α	i	$\alpha\beta$	β
β	β	$\alpha\beta$	i	α
$\alpha\beta$	$\alpha\beta$	β	α	i

These tables are called Cayley tables.

Definitions: Let $\alpha, \beta \in G$. Then $\alpha \star \beta \star \alpha^{-1}$ is called the *conjugate* of β by α. Fix $\alpha \in G$. Then $(\alpha G \alpha^{-1}, \star)$ is a subgroup of $(G, \star)$ where $\alpha G \alpha^{-1} = \{\alpha \star \beta \star \alpha^{-1} \mid \beta \in G\}$. If H is a subgroup of G then $\alpha H \alpha^{-1}$ is called the conjugate of H by α. If $H = \alpha H \alpha^{-1}$for all $\alpha \in G$ then H is called a *normal* subgroup of G.

CHAPTER 1

Definitions: The sets $\mathbb{R}^2 = \{(x, y) \mid x, y \in \mathbb{R}\}$ and $\mathbb{R}^3 = \{(x, y, z) \mid x, y, z \in \mathbb{R}\}$ are called the *Euclidean plane* and *Euclidean space*, respectively. The elements of $\mathbb{R}^2$ and $\mathbb{R}^3$ are called points. A *line* in $\mathbb{R}^2$ is a set of the form $\{(x, y) \mid ax + by + c = 0\}$ where a, b and c are some fixed real numbers so that not both a and b are zero. Similarly, a *plane* in $\mathbb{R}^2$ is a set of the form $\{(x, y, z) \mid ax + by + cz + d = 0\}$ where a, b, c and d are some fixed real numbers so that not all a, b and c are zero.

Let $n = 1$ or 2, a *map* (*function*) α from $\mathbb{R}^n$ to $\mathbb{R}^n$ is a rule so that for each point $P \in \mathbb{R}^n$, there is exactly one point $Q \in \mathbb{R}^n$ associated to P. The point Q is called the image of P under the map α, and we write $Q = \alpha(P)$. We write $\alpha : \mathbb{R}^n \to \mathbb{R}^n$ if α is a map from $\mathbb{R}^n$ to $\mathbb{R}^n$, and for any subset A of $\mathbb{R}^n$, the image of A under α is the set $\alpha(A) = \{\alpha(P) \mid P \in A\}$.

Let $\alpha : \mathbb{R}^n \to \mathbb{R}^n$ be a map where $n = 1$ or 2. We say that α is an *injection* (*one-to-one* map) if $\alpha(P) = \alpha(Q) \implies P = Q$. We say that α is a *surjection* (*onto* map) if for any $Q \in \mathbb{R}^n$, there is $P \in \mathbb{R}^n$ so that $\alpha(P) = Q$. We say that α is an *bijection* (*transformation*) if α is one-to-one and onto. Lastly, α is called a *collineation* if it is a transformation and the image of every line under α is a line.

For example, the map $\gamma : \mathbb{R}^2 \to \mathbb{R}^2$ defined by $\gamma(x, y) = (x^3 - x, y)$ is not a transformation (because it is not one-to-one), but the map $\tau : \mathbb{R}^2 \to \mathbb{R}^2$ defined by $\tau(x, y) = (x + 2, y - 3)$ is a transformation. In fact, τ is a collineation.

Definitions:

· Two lines in a plane are *parallel* if and only if they are the same or they are disjoint (as sets of points).

· Two planes in $\mathbb{R}^3$ are *parallel* if and only if they are the same or they are disjoint.

· A *line* in $\mathbb{R}^3$ is the intersection of twp non-parallel planes.

· Two lines in $\mathbb{R}^3$ are *parallel* if and only if they are coplanar and are parallel in the plane containing them.

· Two lines in $\mathbb{R}^3$ are *skew* if and only if they are not coplanar but are disjoint.

· The distance between the points (x_1, y_1) and (x_2, y_2) is $\sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2}$.

· The distance between the points (x_1, y_1, z_1) and (x_2, y_2, z_2) is $\sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2 + (z_1 - z_2)^2}$.

Notations:

Consider the points P and Q. Then PQ is the distance between P and Q, and if $P \neq Q$, $\overleftrightarrow{PQ}$ is the line through P and Q, $\overline{PQ}$ is the line segment from P to Q, and $\overrightarrow{PQ}$ is the ray with initial point P and containing Q.

Definitions: Let P, Q, R be points.

· P, Q, R are *collinear* if and only if they lie on a line.

· $\angle PQR = \overrightarrow{QP} \cup \overrightarrow{QR}$ is the angle determined by the rays $\overrightarrow{QP}$ and $\overrightarrow{QR}$, and

· $m(\angle PQR)$ is the measurement of $\angle PQR$ in degrees and is a number between 0 and 180.

· If P, Q, R are non-collinear then $\triangle PQR = \overline{PQ} \cup \overline{QR} \cup \overline{RP}$ is the triangle with vertices P, Q, R and edges $\overline{PQ}, \overline{QR}$ and $\overline{RP}$.

· $\cong$ denotes a congruence between geometric figures. We have $\overline{AB} \cong \overline{PQ} \iff AB = PQ$, and $\angle ABC \cong \angle PQR \iff m(\angle ABC) = m(\angle PQR)$.

· $\triangle ABC \cong \triangle PQR \iff AB = PQ, BC = QR, CA = RP, \angle ABC \cong \angle PQR, \angle BCA \cong \angle QRP$ and $\angle CAB \cong \angle RPQ$.

Congruence Theorem for $\triangle ABC$ and $\triangle PQR$.

(SAS) If $AB = PQ$, $\angle A \cong \angle P$ and $BC = QR$ then $\triangle ABC \cong \triangle PQR$.

(ASA) If $\angle A \cong \angle P$, $AB = PQ$ and $\angle B \cong \angle Q$ then $\triangle ABC \cong \triangle PQR$.

(SSS) If $AB = PQ$, $BC = QR$ and $RP = CA$ then $\triangle ABC \cong \triangle PQR$.

(SAA) If $AB = PQ$, $\angle B \cong \angle Q$ and $\angle C \cong \angle R$ then $\triangle ABC \cong \triangle PQR$.

Exterior Angle Theorem:

If C is a point on the line segment $\overline{BD}$ where $B \neq C \neq D$, then $m(\angle ABC) + m(\angle BAC) = m(ACD)$.

Definitions: We say that $\triangle ABC$ and $\triangle PQR$ are similar, and we write $\triangle ABC \sim \triangle PQR$ if and only if $\angle A \cong \angle P$, $\angle B \cong \angle Q$ and $\angle C \cong \angle R$. We note that $\triangle ABC \sim \triangle PQR \iff \frac{AB}{PQ} = \frac{BC}{QR} = \frac{AC}{PR}$. Other notions we amy use are “directed angle”, “half-plane” and “perpendiculer bisector”.

CHAPTER 2: Transformations.

Definition: Recall that a transformation of $\mathbb{R}^2$ is a one-to-one and onto map from $\mathbb{R}^2$ to $\mathbb{R}^2$. Let $\mathcal{G}$ be the set of all transformations of $\mathbb{R}^2$. Define a binary operation $\circ$ on $\mathcal{G}$ as follow. For $\alpha, \beta \in \mathcal{G}$, $\beta \circ \alpha(P) = \beta((P))$. We call $\beta \circ \alpha$ the composite transformations of α and β.

We show that $(\mathcal{G}, \circ)$ is a group. First, we show that $\circ$ is closed on $\mathcal{G}$, that is, if $\alpha, \beta \in \mathcal{G}$ then $\beta \circ \alpha \in \mathcal{G}$. Let $\alpha, \beta \in G$. Then

$$\begin{aligned} \beta \circ \alpha(P) = \beta \circ \alpha(Q) &\implies \beta(\alpha(P)) = \beta(\alpha(Q)) && \text{by definition of } \beta \circ \alpha \\ &\implies \alpha(P) = \alpha(Q) && \text{because } \beta \text{ is one-to-one} \\ &\implies P = Q && \text{because } \beta \text{ is one-to-one} \end{aligned}$$

Thus, $\beta \circ \alpha$ is one-to-one. In addition, let $R \in \mathbb{R}^2$. Since β is onto, there is $Q \in \mathbb{R}^2$ so that $\beta(Q) = R$. Since α is onto, there is $P \in \mathbb{R}^2$ so that $\alpha(P) = Q$. Thus, $\beta \circ \alpha(P) = \beta(\alpha(P)) = (Q) = R$. Hence, $\beta \circ \alpha$ is also onto, and so $\beta \circ \alpha \in \mathcal{G}$.

It is clear that $\circ$ is associative on $\mathcal{G}$. Also, $(\mathcal{G}, \circ)$ has an identity element, namely, the *identity* transformation $i : \mathbb{R}^2 \to \mathbb{R}^2$ defined by $i(P) = P$ for all points $P \in \mathbb{R}^2$.

For each $\alpha \in \mathcal{G}$, we define $\alpha^{-1} : \mathbb{R}^2 \to \mathbb{R}^2$ by $\alpha^{-1}(Q) = P \iff (P) = Q$. This implies $\alpha(\alpha^{-1}(P)) = P$ and $\alpha^{-1}(\alpha(P)) = P$, that means $\alpha \circ \alpha^{-1} = \alpha^{-1} \circ \alpha = i$. We still have to show $\alpha^{-1} \in \mathcal{G}$. Let $P, Q \in \mathbb{R}^2$ and suppose that $\alpha^{-1}(P) = \alpha^{-1}(Q)$. Then $P = \alpha(\alpha^{-1}(P)) = \alpha(\alpha^{-1}(Q)) = Q$. Thus, α^{-1} is one-to-one. Now, α^{-1} is onto because for any $P \in \mathbb{R}^2$, $\alpha^{-1}(\alpha(P)) = P$. Since α^{-1} is one-to-one and onto, $\alpha^{-1} \in \mathcal{G}$.

Notation: In $(\mathcal{G}, \circ)$, we write $\alpha\beta$ instead of $\alpha \circ \beta$. We put $\mathcal{C}$ to be the set of all collineations from $\mathbb{R}^2$ to $\mathbb{R}^2$.

Proposition: $(\mathcal{C}, \circ)$ *is a group.*

*Proof***:** We only have to show that $(\mathcal{C}, \circ)$ is a subgroup of $(\mathcal{G}, \circ)$, that is, we show that for all $\alpha, \beta \in \mathcal{C}$, $\alpha \circ \beta^{-1} \in \mathcal{C}$. Let $\alpha, \beta \in \mathcal{C}$. We show that $\alpha \circ \beta^{-1}$ is a collineation. Let l be a line and let P and Q be two different points on l. Since β is a bijection, there are two different points A and B, so that $\beta(A) = P$ and $\beta(B) = Q$ Let m be the line through A and B. Since β is a collineation, $\beta(m)$ is a line. Since $P, Q \in \beta(m)$, we see that $\beta(m) = l$ and so $\beta^{-1}(l) = m$ and $\alpha \circ \beta^{-1}(l) = \alpha(m)$ is a line because α is a collineation. Thus, $\alpha \circ \beta^{-1}$ is a collineation.□

We note that $(\mathcal{G}, \circ)$ and $(\mathcal{C}, \circ)$ are not abelian.

Definition: An *involution* is a transformation α with the property that $\alpha \neq i$ and $\alpha^2 = i$.

Chapter 3: Translations

Definition: A map $\tau : \mathbb{R}^2 \to \mathbb{R}^2$ ia a translation if there are real numbers r ans s so that for all $(x, y) \in \mathbb{R}^2$, $\tau(x, y) = (x + r, y + s)$. Let $P = (a, b)$ and $= (c, d)$. Then there is a unique translation that maps P to Q, which we will denote by τ_{PQ}. In fact, $\tau_{PQ}(x, y) = (x + c - a, y + d - b)$ and so $\tau_{PQ}(P) = Q$. It is clear that $\tau_{PP} = i$.

Proposition 3.1: *Let A, B, C be non-collinear points. If $\tau_{AB} = \tau_{CD}$ for some point D then $\square ABDC$ is a parallelogram.*

Proof: Let $A=(a_1,a_2), B=(b_1,b_2), C=(c_1,c_2)$ and $D=(d_1,d_2)$, and suppose that $\tau_{AB}=\tau_{CD}$. We note that $\tau_{AB}(x,y)=(x+b_1-a_1, y+b_2-a_2)$ and $\tau_{CD}(x,y)=(x+d_1-c_1, y+d_2-c_2)$. Now,

$$\begin{aligned}
& (b_1,b_2)=B=\tau_{AB}(A)=\tau_{CD}(A)=(a_1+d_1-c_1, a_2+d_2-c_2)\\
\Longrightarrow\ & b_1=a_1+d_1-c_1 \text{ and } b_2=a_2+d_2-c_2\\
\Longrightarrow\ & \begin{cases} a_1-b_1=c_1-d_1 \text{ and } a_2-b_2=c_2-d_2\\ a_1-c_1=b_1-d_1 \text{ and } a_2-c_2=b_2-d_2\end{cases}\\
\Longrightarrow\ & \begin{cases} AB^2=(a_1-b_1)^2+(a_2-b_2)^2=(c_1-d_1)^2+(c_2-d_2)^2=CD^2, \text{ and}\\ AC^2=(a_1-c_1)^2+(a_2-c_2)^2=(b_1-d_1)^2+(b_2-d_2)^2=BD^2\end{cases}\\
\Longrightarrow\ & AB=CD \text{ and } AC=BD
\end{aligned}$$

Thus, $\square ABDC$ is a parallelogram.□

The converse is also true, that is, if $\square ABDC$ is a parallelogram then $\tau_{AB}=\tau_{CD}$.

Proposition 3.2: *τ_{AB} is a collineation.*

Proof: We leave to the reader to prove that τ_{AB} is a transformation (that is, τ_{AB} is a bijection). Thus, we only have to prove that τ_{AB} maps lines to lines. Let $A=(a_1,a_2), B=(b_1,b_2)$ and let l be the line with equation $rx+sy+t=0$. Let m be the line with equation $rx+sy+(t+r(a_1-b_1)+s(a_2-b_2))=0$. Then, it is easy to see that $\tau_{AB}(l)=m$. Thus, τ_{AB} maps lines to lines.□

Note that in the above proof, $l\parallel m$. Thus, translations map a line to a parallel line.

Definition: A *dilatation* is a collineation which maps a line to a parallel line. Thus, a translation is a dilatation.

Proposition 3.3: *If $l\parallel \overleftrightarrow{AB}$ then $\tau_{AB}(l)=l$.*

Proof: Suppose that $l\parallel \overleftrightarrow{AB}$. Let $P\in l$ and $Q=\tau_{AB}(P)$. Then by Prop. 3.1, $\tau_{AB}=\tau_{PQ}$ and $\overleftrightarrow{AB}\parallel\overleftrightarrow{PQ}$. Since $l\parallel\overleftrightarrow{AB}$ and $\overleftrightarrow{AB}\parallel\overleftrightarrow{PQ}$, we see that $l\parallel\overleftrightarrow{PQ}$ and so $l=\overleftrightarrow{PQ}$ because $P\in l$. Thus, $\tau_{AB}(P)=Q\in l$, that is, $\tau_{AB}(l)=l$.□

Proposition 3.4: *If $A\neq B$ and $\tau_{AB}(m)=m$ then $m\parallel\overleftrightarrow{AB}$.*

Proof: Let $A\neq B$ and $\tau_{AB}(m)=m$ for some line m. Let $P\in m$. Since $\tau_{AB}(m)=m$, $Q=\tau_{AB}(P)\in m$. Since $A\neq B$, $Q=\tau_{AB}(P)\neq P$ and so $m=\overleftrightarrow{PQ}$. Now, since $\tau_{AB}(P)=Q$, from Prop. 3.1 we have $\overleftrightarrow{AB}\parallel\overleftrightarrow{PQ}$, that is, $m\parallel\overleftrightarrow{AB}$.□

Thus,

Proposition 3.5: *τ_{AB} fixes exactly those lines that are parallel to $\overleftrightarrow{AB}$.*

Definition: We denote by $\mathcal{D}$ the set of all dilatations and by $\mathcal{T}$ the set of all translations. We note that $\mathcal{T}\subset\mathcal{D}\subset\mathcal{C}\subset\mathcal{G}$, where $\mathcal{C}$ and $\mathcal{G}$ are known to be groups.

Proposition 3.6: *Collineations map parallel lines to parallel lines.*

Proof: Let $\alpha\in\mathcal{C}$ and $l\parallel m$. Then $\alpha(l)$ and $\alpha(m)$ are lines. Since $l\parallel m$, either $l=m$ or $l\cap m=\emptyset$. If $l=m$ then $\alpha(l)=\alpha(m)$ and so $\alpha(l)\parallel\alpha(m)$. If $l\cap m=\emptyset$, then $\alpha(l)\cap\alpha(m)=\emptyset$ because α is one-to-one, and so $\alpha(l)\parallel\alpha(m)$.□

Proposition 3.7: *$\mathcal{D}$ is a subgroup of $\mathcal{C}$.*

Proof: We only need to show that if $\alpha,\beta\in\mathcal{D}$ then $\alpha\beta^{-1}\in\mathcal{D}$. Let $\alpha,\beta\in\mathcal{D}$ and l be a line. Since $\beta\in\mathcal{D}$, $\beta(\beta^{-1}(l))\parallel\beta^{-1}(l)$, that is, $l\parallel\beta^{-1}(l)$. Since $l\parallel\beta^{-1}(l)$ and α is a collineation, by Prop 3.6, we have $\alpha(l)\parallel\alpha\beta^{-1}(l)$. Since $\alpha\in\mathcal{D}$, $\alpha(l)\parallel l$. From $\alpha(l)\parallel l$

and $\alpha(l) \parallel \alpha\beta^{-1}(l)$, we get $\alpha\beta^{-1}(l) \parallel l$. Thus, $\alpha\beta^{-1} \in \mathcal{D}$, and $\mathcal{D}$ is a subgroup of $\mathcal{C}$.□

Proposition 3.8: *$\mathcal{T}$ is an abelian subgroup of $\mathcal{D}$.*

Proof: We need to show that if $\tau_1, \tau_2 \in \mathcal{T}$ then $\tau_1\tau_2{}^{-1} \in \mathcal{T}$. Let $\tau_1, \tau_2 \in \mathcal{T}$. Then there are real numbers a, b, c, d so that $\tau_1(x, y) = (x + a, y + b)$ and $\tau_2(x, y) = (x + c, y + d)$ for all $(x, y) \in \mathbb{R}^2$. Then $\tau_2^{-1}(x, y) = (x - c, y - d)$ and so $\tau_1\tau_2{}^{-1} = (x + a - c, y + b - d)$ for all $(x, y) \in \mathbb{R}^2$. Thus, $\tau_1\tau_2{}^{-1} \in \mathcal{T}$ and so $\mathcal{T}$ is a subgroup of $\mathcal{D}$. It is easy to see that $\tau_1\tau_2(x, y) = \tau_2\tau_1(x, y) = (x + a + c, y + b + d)$, so $\mathcal{T}$ is abelian.□

Definition: Let $P = (a, b) \in \mathbb{R}^2$. A *halfturn σ_P about P* is the transformation $\sigma_P : \mathbb{R}^2 \to \mathbb{R}^2$ defined by $\sigma_P(x, y) = (-x + 2a, -y + 2b)$. We note that if $Q = (c, d)$ and $Q' = \sigma_P(Q) = (-c + 2a, -d + 2b)$ and so $\frac{1}{2}(Q + \sigma_P(Q)) = P$. This means that P, Q and $\sigma_P(Q)$ are collinear and that P is the midpoint of $\overline{QQ'}$.

In general, $P, (x, y)$ and $\sigma_P(x, y)$ are collinear and that P is the midpoint of the line segment determined by (x, y) and $\sigma_P(x, y)$.

Proposition 3.9: *σ_P is a transformation.*

Proof: We need to prove that σ_P is one-to-one and onto. It is easy to see that σ_P is one-to-one. We prove that σ_P is onto. Let $Q = (c, d) \in \mathbb{R}^2$. Put $R = \sigma_P(Q) = (-c + 2a, -d + 2b)$. Then $\sigma_P(R) = (-(-c + 2a) + 2a, -(-d + 2b) + 2b) = (c, d) = Q$. Thus, σ_P is onto. In fact, we have shown that $\sigma_P^2 = i$.□

Proposition 3.10: *σ_P is a dilatation.*

Proof: We need to prove that for any line l, $\sigma_P(l) \parallel l$. Let l be the line with equation $cx + dy + e = 0$. It is easy to verify that $\sigma_P(l) = m$ where m is the line with equation $cx + dy - (e + 2ac + 2bd) = 0$, and so $m \parallel l$, that is $\sigma_P(l) \parallel l$.□

It is clear that for any point A, if $\sigma_P(A) = A$ then $A = P$, and for any line l, if $\sigma_P(l) = l$ then $P \in l$.

Proposition 3.11: *For any points P and Q, $\sigma_P\sigma_Q = \tau_{QR} = \sigma_Q\sigma_R$ where R is the point so that P is the midpoint of $\overline{QR}$.*

Proof: Let $P = (a, b)$ and $Q = (c, d)$. Let $R = (2a - c, 2b - d)$. Then P is the midpoint of $\overline{QR}$. Now, for any $(x, y) \in \mathbb{R}^2$,

$$\begin{aligned}
\sigma_P\sigma_Q(x, y). &= \sigma_P(-x + 2c, -y + 2d) \\
&= (-(-x + 2c) + 2a, -(-y + 2d) + 2b) \\
&= (x + 2a - 2c, y + 2b - 2d) \\
&= (x + (2a - c) - c, y + (2b - d) - d) \\
&= \tau_{PQ}(x, y)
\end{aligned}.$$

Therefore, $\sigma_P\sigma_Q = \tau_{QR}$. Similarly, we see that $\tau_{QR} = \sigma_Q\sigma_R$.□

Thus, the product of two halfturns is a translation. The converse is also true.

Proposition 3.12: *Each translation is a product of two halfturns.*

Proof: Let $\tau \in \mathcal{T}$ and let $R = \tau(O)$ where $O = (0, 0)$. Then $\tau = \tau_{OR}$. Let P be the midpoint of $\overline{OR}$. Then, by the proof of Proposition 3.11, $\tau = \tau_{OR} = \sigma_P\sigma_O = \sigma_R\sigma_P$.□

It is immediate from the defination of halfturns that the product of three halfturns is a halfturn. In fact,

Proposition 3.13: *If P, Q, R are non-collinear points then $\sigma_R\sigma_Q\sigma_P = \sigma_S$ where $\square PQRS$ is a parallelogram, and so $\sigma_S\sigma_R\sigma_Q\sigma_P = \sigma_S^2 = i$.*

Proof: Let $P = (a, b), Q = (c, d)$ and $R = (e, f)$. Let $S = (a - c = e, b - d+, f)$. then it is easy to verify that $\sigma_R\sigma_Q\sigma_P = \sigma_S$ and $\square PQRS$ is a parallelogram.$\square$

Thus, **the product of halfturns is a translation or a halfturn**.

EXERCISES:

1. Suppose that we know three of the points A, B, C and D. Prove that the condition $\tau_{AB} = \sigma_D\sigma_C$ uniquely determine the fourth point.
2. For any points A, B, C, $\sigma_A\sigma_B\sigma_C = (\sigma_A\sigma_B\sigma_C)^{-1} = \sigma_C^{-1}\sigma_B^{-1}\sigma_A^{-1} = \sigma_C\sigma_B\sigma_A$. Thus, $\sigma_R\sigma_Q\sigma_P = \sigma_P\sigma_Q\sigma_R = \sigma_S$ where $\square PQRS$ is a parallelogram
3. Let $\mathcal{H}$ be the group generated by halfturns. We know that $\mathcal{H} \subset \mathcal{D}$ and $\mathcal{H} = \{\delta \in \mathcal{D} \mid \delta \text{ is a halfturn or } \delta \text{ is a translation}\}$. Prove that $\mathcal{H}$ is a subgroup of $\mathcal{D}$.

Chapter 4: REFLECTIONS

Definition: Let m be a line. The *reflection in the line* m is the map $\sigma_m : \mathbb{R}^2 \to \mathbb{R}^2$ defined by:

$$\sigma_m(P) = \begin{cases} P & \text{if } P \in m, \text{ and} \\ Q & \text{if } P \notin m \text{ and } m \text{ is the bisector of } \overline{PQ}. \end{cases}$$

Exercises:

1. σ_m is an involution.
2. σ_m fixes m pointwise, that is, $\sigma_m(P) = P \Longleftrightarrow P \in m$.
3. For any line l, $\sigma_m(l) = l \Longleftrightarrow l = m$ or $l \perp m$.b
4. If m is the line with equation $ax+by+c = 0$ then $\sigma_m(x, y) = \left(x - \frac{2a(ax+by+c)}{a^2+b^2}, y - \frac{2a(ax+by+c)}{a^2+b^2}\right)$.

Definition: An *isometry* is a transformation α that preserve distance; that is, $\alpha(P)\alpha(Q) = PQ$ for all points P and Q.

It can be shown that isometries preserve: collinearity, betweeness, mid-points, segments, rays, triangles, angles, angle measure, perpendicularity.

The set $\mathcal{I}$ of all isometries is a group, and reflections are isometries (an easy proof is on page 27 of the text).

Definition: Let S be a set of points of $\mathbb{R}^2$ (we can think of S as a figure). Let P be a point in $\mathbb{R}^2$ and m is a line in $\mathbb{R}^2$. We say that P is a *point of symmetry* of S, and S is *symmetrical about the point* P if $\sigma_P(S) = S$. We say that m is a *line of symmetry* of S, and S is *symmetrical about the line* m if $\sigma_m(S) = S$.

Definition: Let S be a set of points of $\mathbb{R}^2$. A *symmetry* for S is an isometry α so that $\alpha(S) = S$. The set $\mathcal{I}_S$ of all symmetries for S is a group, called the *symmetry group* for S.

Chapter 5: ISOMETRIES

⋆**Theorem 1**: *Let $\alpha \neq i$ be an isometry.*
(a) *If α fixes two different points of a line then α fixes that line pointwise.*
(b) *α fixes at most two of any three non-collinear points. In fact, if α fixes any three non-collinear points then .$\alpha = i$*
(c) *α is uniquely determined by any three non-collinear points and their images.*
(d) *If α fixes two distinct points then α is a reflection (in the line through these points).*
(e) *If α fixes exactly one point then α is a product of two reflections.*

Proof:

(a) Suppose that $\alpha(P) = P$ and $\alpha(Q) = Q$ for some points $P \neq Q$, and $l = \overleftrightarrow{PQ}$. Let $R \in l$ and $R' = \alpha(R)$. Since α is an isometry, $R'P = RP$ and $R'Q = RQ$ which imply that $R' = R$ and so $\alpha(R) = R$.
(b) We prove (b) by a contradiction proof. Suppose that α fixes three non-collinear points A, B, C. Then by (a), α fixes each points of the lines $\overleftrightarrow{AB}$, $\overleftrightarrow{BC}$, $\overleftrightarrow{AC}$. Let P be any point and we can choose a line l containing P such that l intersects the lines $\overleftrightarrow{AB}$, $\overleftrightarrow{BC}$, $\overleftrightarrow{AC}$ at at least two points. Since α fixes these two points, by (a), α fixes l pointwise and so α fixes P, that is, $\alpha(P) = P$. Thus, $\alpha = i$ which contradicts the assumption that $\alpha \neq i$. Thus, α fixes at most two of any three non-collinear points.
(c) Let A, B, C be three non-collinear points and suppose that α and β are isometries so that $\alpha(A) = \beta(A)$, $\alpha(B) = \beta(B)$ and $\alpha(C) = \beta(C)$. We show that $\alpha = \beta$. Since $\alpha, \beta \in \mathcal{I}$ and $\mathcal{I}$ is a group, we have $\alpha\beta^{-1} \in \mathcal{I}$. Thus, $\alpha\beta^{-1}$ is an isometry that fixes three non-collinear points A, B, C, and so by (b), $\alpha\beta^{-1} = i$ and so $\alpha = \beta$.
(d) Let $\alpha(P) = P$ and $\alpha(Q) = Q$ for some points $P \neq Q$. By (a), $\alpha(R) = R$ for all points $R \in \overleftrightarrow{PQ} = m$. Let $A \notin m$. Then P, Q, A are non-collinear and so by (b), $\alpha(A) \neq A$. Let $l = \overleftrightarrow{A\alpha(A)}$. Since α is an isometry, $AQ = \alpha(A)Q$ and $AP = \alpha(A)P$, which imply that m is the perpendicular bisector of $\overline{A\alpha(A)}$ and so $\alpha = \sigma_m$.
(e) Suppose that $\alpha(P) = P$ and $\alpha(A) \neq A$ for all points $A \neq P$. Let $Q \neq P$ and let m be the perpendicular bisector of $\overline{Q\alpha(Q)}$. Since $PQ = \alpha(P)\alpha(Q) = P\alpha(Q)$, we see that $P \in m$. It is clear that $\sigma_m\alpha(P) = P$ and $\sigma_m\alpha(Q) = Q$. Since $\sigma_m\alpha \in \mathcal{I}$ and $\sigma_m\alpha$ fixes two points P and Q, it follows by (d) that $\sigma_m\alpha = \sigma_n$ for some line n. This means $\alpha = \sigma_m^{-1}\sigma_n = \sigma_m\sigma_n$.□

⋆**Theorem 2**:
(a) *A product of reflections is an isometry.*
(b) *Each $\alpha \in \mathcal{I}$ is a product of at most three reflections.*

Proof:
(a) Since each reflection is an isometry and $\mathcal{I}$ is a group, the statement (a) is obvious.
(b) Let $\alpha \in \mathcal{I}$. If $\alpha = i$ then $\alpha = \sigma_m^2$ for any line m, and so α is a product of two reflections. Suppose that $\alpha \neq i$. If α fixes some point(s) then by Theorem 1, α is a product of at most two reflections. Suppose that α has no fixed points. Let $P \in \mathbb{R}^2$ and

let m be the perpendicular bisector of $\overline{P\alpha(P)}$. Then $\sigma_m\alpha(P) = P$, that is, $\sigma_m\alpha$ fixes point P and so by Theorem 1, $\sigma_m\alpha$ is the product of at most two reflections. Hence, α is the product of at most three reflections.$\square$

Definition: Two sets S and T are *congruent* if there is an isometry α so that $\alpha(S) = \alpha(T)$.

Definition (Rotations): We denote by $\rho_{C,\theta}$ the rotation centred at C through an angle of θ. Let O be the origin. Then $\rho_{O,\theta}(x,y) = (x\cos\theta - y\sin\theta, x\sin\theta + y\sin\theta)$ and if $C = (a,b)$ then

$\rho_{C,\theta}(x,y) = (x\cos\theta - y\sin\theta + (b\sin\theta - a\cos\theta + a), x\sin\theta + y\sin\theta + (b - a\sin\theta - b\cos\theta))$.

It is easy to show that:

· A rotation is an isometry.

· $\rho_{C,180} = \sigma_C$ (the halfturn about C).

· When $\theta \neq 360k$ where k is an integer, $\rho_{C,\theta}$ fixes exactly one point, namely C.

· $\rho_{C,\theta}^{-1} = \rho_{C,-\theta}$.

· $\rho_{C,\theta}\rho_{C,\varphi} = \rho_{C,\theta+\varphi} = \rho_{C,\varphi}\rho_{C,\theta}$.

· $\rho_{C,\theta} = \rho_{C,\theta+360k}$ for any integers k.

· Fix a point C. The set $\{\rho_{C,\theta} \mid \theta \in \mathbb{R}\}$ is a group.