PMAT 319 Winter 2016.
Chapter 0.

Definition: Let G be a non-empty set. A binary operation on G is a function $* : G\times G \to G$. We put $*(\alpha,\beta) = \alpha*\beta$. We say that $*$ is associative if and only if $(\alpha*\beta)*\gamma = \alpha*(\beta*\gamma)$ for all $\alpha,\ \beta,\ \gamma \in G$. We say $*$ is commutative iff $\alpha*\beta = \beta*\alpha$ for all $\alpha,\ \beta \in G$.

We say that $(G,*)$ is a *group* if:

(1) $*$ is an associative binary operation on G,

(2) There is a element $i \in G$ so that $\alpha * i = i * \alpha = \alpha$ for all $\alpha \in G$, (i is called the identity element of G), and

(3) For every $\alpha \in G$, there is a unique $\beta \in G$ so that $\alpha*\beta = \beta*\alpha = i$, ($\beta$ is called the inverse of α, and we write $\beta = \alpha^{-1}$).

If $(G,*)$ is a group and $*$ is commutative then we say that $(G,*)$ is an *abelian* group.

Exercise: Prove that (i) the identity element if exists must be unique and (ii) if β and γ are inverses of α then $\beta=\gamma$.

Example: $(\mathbb{Z},+)$ and $(\mathbb{R}\setminus\{0\},\cdot)$ are abelian groups.

Definition: Let $(G,*)$ be a group. A non-empty subset H of G is a subgroup of G iff $(H,*)$ is a group itself.

Theorem 0.1: $(H,*)$ is a subgroup of $(G,*)$ if and only if $\alpha*\beta^{-1} \in H$ for all $\alpha,\ \beta \in H$.
Proof:

Theorem 0.2: Let Let $(G,*)$ be a group. For any $\alpha,\ \beta \in G$,
if $\beta*\alpha = \beta*\gamma$ then $\alpha=\gamma$, (left-cancellation)
if $\alpha*\beta = \gamma*\beta$ then $\alpha=\gamma$, (right-cancellation)
and $(\alpha*\beta)^{-1} = \beta^{-1}*\alpha^{-1}$.
Proof:

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

If G has exactly n element for some positive integer n, we say that G is finite. Otherwise, we say that G is infinite.

Let $\alpha \in G$. We say that α is an element of *order* n if n is the smallest positive integer (if exists) so that $\alpha^n = i$. Otherwise, we say that α is an element of *infinite order* (in this case, $\alpha^n \neq i$ for all positive integers n.

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 $H = \langle\alpha\rangle$ which is called the *cyclic group* generated by α. It is clear that cyclic groups are abelian.

In general, the group generated by the elements $\alpha_1,\ \alpha_2,\ ...,\ \alpha_m$ is
$\langle\alpha_1,\ \alpha_2,\ ...,\ \alpha_m\rangle = \{\alpha_1^{s_1} * \alpha_2^{s_2} * ... * \alpha_m^{s_m} \mid s_1,\ s_2,\ ...,\ s_m \in \mathbb{Z}\}$.

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

Examples: $C_4 = \langle\alpha\rangle$ and $V_4 = \langle\alpha, \beta\rangle$ and below are their Cayley 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

Let $\alpha, \beta \in G$. Then $\alpha * \beta * \alpha^{-1}$ is called the *conjugate* of β by α, and the set $\alpha G\alpha^{-1} = \{\alpha * \beta * \alpha^{-1} \mid \beta \in G\}$ is a subgroup of G.

If H is a sugroup of G then $\alpha H\alpha^{-1}$ is called the *conjugate* of H by α. If $H = \alpha H\alpha^{-1}$ for all $\alpha \in G$ the H is called a *normal* subgroup of G.

PMAT 319 Winter 2015.
Chapter 1.

The coordinate plane $\mathbb{R}^2 = \{(x, y) \mid x, y \in \mathbb{R}\}$ and the real three space $\mathbb{R}^3 = \{(x, y, z) \mid x, y, z \in \mathbb{R}\}$ are also called the *Euclidean* plane and space.

Let $\alpha : \mathbb{R}^n \to \mathbb{R}^n$ be a map (function) where $n = 2$ or 3.

We say that α is an *injection* (*one-to-one*, 1-1) if and only if $\forall P, Q \in \mathbb{R}^n$, if $\alpha(P) = \alpha(Q)$ then $P = Q$.

We say that α is a *surjection* (*onto*) if and only if $\forall P \in \mathbb{R}^n$, $\exists Q \in \mathbb{R}^n$ so that $\alpha(Q) = P$.

We say that α is a *bijection* (*transformation*) if and only if α is one-to-one and onto.

Example: Let $\gamma : \mathbb{R}^n \to \mathbb{R}^n$ and $\tau : \mathbb{R}^n \to \mathbb{R}^n$ be function defined by $\gamma(x, y) = (x^3 - x, y)$ and $\tau(x, y) = (x - 2, y + 3)$ for every (x, y). Then γ is onto but not one-to-one and τ is a transformation.

A *line* in $\mathbb{R}^2$ is a subset of $\mathbb{R}^2$ which has the form $\{(x, y) \mid ax + by + c = 0\}$ for some fixed real numbers $a,\ b$ and c where not both a and b are zeros.

A *plane* in $\mathbb{R}^3$ is a subset of $\mathbb{R}^3$ which has the form $\{(x, y, z) \mid ax + by + cz + d = 0\}$ for some fixed real numbers $a,\ b,\ c$ and d where not all $a,\ b$ and c are zeros.

Two lines l and m in the plane $\mathbb{R}^2$ are *parallel* if and only if $l = m$ or $l \cap m = \emptyset$.

Two planes Γ and Λ in $\mathbb{R}^3$ are *parallel* if and only if $\Gamma = \Lambda$ or $\Gamma \cap \Lambda = \emptyset$.

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

Two lines l and m in $\mathbb{R}^2$ are *parallel* if and only if they are coplanar, and $l = m$ or $l \cap m = \emptyset$.

$\alpha : \mathbb{R}^n \to \mathbb{R}^n$ is a *collineation* if it is a transformation and the image of every line is a line.

Two lines l and m in $\mathbb{R}^2$ are *skew* if and only if they are not coplanar and $l \cap m = \emptyset$.

The distance between two points (a, b) and (c, d) is $\sqrt{(a - c)^2 + (b - d)^2}$.

The distance between two points (a, b, c) and (x, y, x) is $\sqrt{(a - x)^2 + (b - y)^2 + (c - z)^2}$.

Let P, Q, R be points (elements) of $\mathbb{R}^2$ or $\mathbb{R}^3$.

PQ is the distance between P and Q.

Now, if $P \neq Q$,

$\overleftrightarrow{PQ}$ is the line through P and Q.

$\overline{PQ}$ is the line segment from P to Q.

$\overrightarrow{PQ}$ is the ray with initial point P and containing Q.

$P,\ Q$ and R are *collinear* if and only if they lie on one line.

The angle $\angle PQR$ is the union $\overrightarrow{QP} \cup \overrightarrow{QR}$.

$m(\angle PQR)$ is the measurement of the angle $\angle PQR$ and is a number between 0 and 180, that is $0 \leq m(\angle PQR) \leq 180$.

Let P, Q, R be non collinear points.

$\triangle PQR = \overline{PQ} \cup \overline{QR} \cup \overline{RP}$ is called the triangle with vertices $P,\ Q,\ R$ and edges $\overline{PQ}$, $\overline{QR}$ and $\overline{RP}$.

$\cong$ denotes a congruence between geometric figures (subsets of $\mathbb{R}^2$ or $\mathbb{R}^3$). It is clear that

$\overline{AB} \cong \overline{PQ}$ if and only if $AB = PQ$.

$\angle ABC \cong \angle PQR$ if and only if $m(\angle ABC) = m(\angle PQR)$.

$\triangle ABC \cong \triangle PQR$ if and only if $AB = PQ,\ BC = QR,\ CA = RP,\ m(\angle CAB) = m(\angle RPQ),\ m(\angle ABC) = m(\angle PQR)$ and $m(\angle BCA) = m(\angle QRP)$.

Congruence Theorems:

(SAS) If $AB = PQ$, $\angle A \cong \angle P$ and $AC = PR$ 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 $CA = RP$ 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:

Consider $\triangle ABC$. Let D be a point on $\overrightarrow{BC}$ but $D \notin \overline{BC}$. Then
$m(\angle ACD) = m(\angle A) + m(\angle B)$.