Now $A_3 = \{f_0, f_1, f_2\}$ is the alternating group of degree.

It is a commutative group of order 3.

3. The symmetries of a square form a group with respect to composition of symmetries (as given in Fig 3 in Page-2) form a group. It is called the dihedral group D_4. It has $4 \times 2 = 8$ elements.

Similarly the symmetries of a regular n-gon form a group with respect to composition of symmetries form a group, called the dihedral group D_n. It contains $2n$ elements.

4. Let H be the set of complex matrices given by

$$H = \{I, J, K, L, -I, -J, -K, -L\} \text{ where}$$

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad -I = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \quad J = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad -J = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}$$

$$K = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad -K = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad L = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \quad -L = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}$$

Consider the binary operation matrix multiplication. Multiplication table for H is

$\cdot$	I	$-I$	J	$-J$	K	$-K$	L	$-L$
I	I	$-I$	J	$-J$	K	$-K$	L	$-L$
$-I$	$-I$	I	$-J$	J	$-K$	K	$-L$	L
J	J	$-J$	$-I$	I	L	$-L$	$-K$	K
$-J$	$-J$	J	I	$-I$	$-L$	L	K	$-K$
K	K	$-K$	$-L$	L	$-I$	I	J	$-J$
$-K$	$-K$	K	L	$-L$	I	$-I$	$-J$	J
L	L	$-L$	K	$-K$	$-J$	J	$-I$	I
$-L$	$-L$	L	$-K$	K	J	$-J$	I	$-I$

Here $J^2 = K^2 = L^2 = -I$,
$JK = L$, $KJ = -L$
$KL = J$, $LK = -J$
$LJ = K$, $JL = -K$

$(H, \cdot)$ is a group, called the group of unit quaternions, and is denoted by Q_8

5. Let $S = \{e, a, b, c\}$ and let $\circ$ be the binary operation defined on S given by the following table:

$\circ$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

$(S, \circ)$ is called Klein's 4-group.

$(S, \circ)$ is an abelian group of order 4

(A group $(G, \circ)$ is said to be a finite group if G contains a finite number of elements. The order of a finite group $(G, \circ)$ is the number of elements of G. The order of the group G is denoted by $o(G)$ or $|G|$)

6. The set $\mathbb{Z}_n$, the classes of residues of integers modulo n, forms an abelian group with respect to $+$, addition (modulo n) defined by

$$\bar{a} + \bar{b} = \overline{a+b} \quad \text{if } a+b < n$$
$$= \overline{a+b-n} \quad \text{if } a+b \geq n$$

The composition table for '$+$' in $\mathbb{Z}_3$ is

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

Elementary properties of groups:

Theorem 1.3 Let $(G, *)$ be a group.

(i) $(a^{-1})^{-1} = a \quad \forall a \in G$

(ii) $(a*b)^{-1} = b^{-1} * a^{-1}$

(iii) (Cancellation Law) $a*b = a*c \Rightarrow b = c$ (right cancellation Law)

$b*a = c*a \Rightarrow b = c$ (left cancellation Law)

$\forall a, b, c \in G$

(iv) For each $a, b \in G$, the equations $a*x = b$ and $y*a = b$ have unique solutions for x and y.

Proof: Let $a \in G$. Then $a^{-1} * a = a * a^{-1} = e$ (e is the identity element in G)

$\therefore a^{-1}$ has an inverse a. As the inverse is unique, $(a^{-1})^{-1} = a$ as $(a^{-1})^{-1}$ is the inverse of a^{-1}.

(ii) Let $a, b \in G$. Then

$$(a*b)*(b^{-1}*a^{-1}) = ((a*b)*b^{-1})*a^{-1} = (a*(b*b^{-1}))*a^{-1} = (a*e)*a^{-1}$$
$$= a*a^{-1} = e$$

Similarly $(b^{-1}*a^{-1})*(a*b) = e$. Hence $b^{-1}*a^{-1}$ is an inverse of $a*b$

Since the inverse of an element is unique in a group since $(a*b)^{-1}$ denotes the inverse of $a*b$, it follows that $(a*b)^{-1} = b^{-1}*a^{-1}$

(iii) $a*b = a*c \Rightarrow a^{-1}*(a*b) = a^{-1}*(a*c) \Rightarrow (a^{-1}*a)*b = (a^{-1}*a)*c$

$\Rightarrow e*b = e*c \Rightarrow b = c$

Similarly $b*a = c*a \Rightarrow b = c$

(iv) Substituting $a^{-1}*b$ for x, we have

$$a*(a^{-1}*b) = (a*a^{-1})*b$$
$$= e*b$$
$$= b$$

Thus $a^{-1}*b$ is a solution of the equation $a*x = b$

Let x_1, x_2 be two solutions of $a*x = b$. Then $a*x_1 = b$, $a*x_2 = b$

$\Rightarrow a*x_1 = a*x_2 \Rightarrow x_1 = x_2$ (left cancellation law)

$\therefore$ $a*x = b$ has a unique solution and it is $a^{-1}*b$

Similarly, $y*a = b$ has a unique solution and it is $b*a^{-1}$

Corollary 1.3.1 Let $(G, *)$ be a group and $a \in G$. If $a*a = a$, then $a = e$

Proof: Since $a = a*a \Rightarrow a*a = a*e \Rightarrow a = e$ (left cancellation law)

corollary 1.3.2 In a composition table for a group $(G, *)$, each element appears exactly once in each row and exactly once in each column.

Proof: Let $b \in G$ be such that b occurs twice in a row marked by $a \in G$. Then $\exists\ u, v \in G$ with $u \neq v$ such that $a*u = b$ and $a*v = b$. Thus, the equation $a*x = b$ has two distinct solutions, u and v. This is a contradiction to Theorem 1.3(iv) Since the equation $a*x = b$ has a unique solution for x. A similar argument for columns can be used.

Theorem 1.4 A semigroup $(S, *)$ is a group if and only if

(i) $\exists\, e \in S$ such that $e * a = a \;\forall a \in S$ and

(ii) for each $a \in S$ $\exists\, b \in S$ such that $b * a = e$.

Proof: Suppose $(S, *)$ is a semigroup that satisfies (i) and (ii). Let a be any element of S. Then $\exists\, b \in S$ such that $b * a = e$ by (ii). For $b \in S$, $\exists\, c \in S$ such that $c * b = e$ by (ii). Now

$$a = e * a = (c * b) * a = c * (b * a) = c * e$$

and $$a * b = (c * e) * b = c * (e * b) = c * b = e$$

Hence $a * b = b * a = e$. Also,

$$a * e = a * (b * a) = (a * b) * a = e * a = a$$

Thus $a * e = e * a = a \;\forall a \in S$. This shows that e is the identity element of S. Now since $a * b = e = b * a$, we have $b = a^{-1}$. Therefore $(S, *)$ is a group. The converse follows from the definition of a group.

Theorem 1.5 Let $(S, *)$ be a semigroup and for any two elements $a, b \in S$, each of the equation $a * x = b$ and $y * a = b$ has a solution in S for x and y. Then $(S, *)$ is a group.

Proof: Let $a \in S$. Consider the equation $y * a = a$. By our assumption, $y * a = a$ has a solution $u \in S$, say. Then $u * a = a$. Let b be any element of S. Consider the equation $a * x = b$. Again, by our assumption, $a * x = b$ has a solution in S. Let $c \in S$ be a solution of $a * x = b$. Then $a * c = b$. Now

$$\begin{aligned} u * b &= u * (a * c) && \text{(since } b = a * c\text{)} \\ &= (u * a) * c && \text{(since } * \text{ is associative)} \\ &= a * c && \text{(since } u * a = a\text{)} \\ &= b \end{aligned}$$

Since b was an arbitrary element of S, we find $u * b = b, \forall b \in S$. Thus $(S, *)$ satisfies (i) of Theorem 1.4. Consider the

equation $y*a = u$. Let $d \in S$ be a solution of $y*a = u$.
Then $d*a = u$. This shows that $(S, *)$ satisfies (ii) of Theorem 1.4
Hence $(S, *)$ is a group by Theorem 1.4.

Theorem 1.5 Let $(S, *)$ be a semigroup containing a finite number of elements in which both the cancellation laws hold. Then $(S, *)$ is a group.

Proof: Let $(S, *)$ be a finite semigroup satisfying the cancellation laws. Let $a, b \in S$. Consider the equation $a*x = b$. We show that this equation has a solution in S. Let us write $S = \{a_1, a_2, \ldots, a_n\}$ where a_i's are all distinct elements of S. Since S is a semigroup $a*a_i \in S$ for all $i = 1, 2, \ldots, n$. Thus, $\{a*a_1, a*a_2, \ldots, a*a_n\} \subseteq S$. Suppose $x*a_i = a*a_j$ for some $i \neq j$. Then by the left cancellation law, $a_i = a_j$, a contradiction. Hence all elements of $\{a*a_1, a*a_2, \ldots, a*a_n\}$ are distinct. So, $S = \{a*a_1, a*a_2, \ldots, a*a_n\}$. Let $b \in S$
Then $a*a_k = b$ for some $a_k \in S$. So, the equation $a*x = b$ has a solution in G. Similarly, we can show that the equation $y*a = b$ has a solution in S. Hence by theorem 1.5, $(S, *)$ is a group.

Let $(G, *)$ be a group. Due to associativity of $*$, $a*a$, $a*a*a$, $a*a*a*a$ can be calculated unambiguously. So, for a group $(G, *)$, and for $a \in G$, we define the integral power of a as follows:

$$a^0 = e \quad (\text{the identity element in } G)$$
$$a^n = a*a^{n-1} \quad \text{if } n > 0 \text{ and } n \in \mathbb{Z}$$
$$= (a^{-1})^{-n} \quad \text{if } n < 0 \text{ and } n \in \mathbb{Z}$$

2. Subgroups Let $(G, *)$ be a group and H be a non-empty subset of G. Then H is said to be closed under the binary operation $*$ if $a * b \in H, \forall a, b \in H$.

Suppose H is closed under the binary operation $*$. Then the restriction $*$ to $H \times H$ is a mapping from $H \times H$ into H. Thus, the binary operation $*$ defined on G induces a binary operation on H. We denote this induced binary operation in H by $*$ also. Thus $(H, *)$ is a mathematical system. It also follows that $*$ is associative as a binary operation on H, i.e., $a * (b * c) = (a * b) * c \quad \forall a, b, c \in H$. If $(H, *)$ is a group, then we call H a subgroup of G. More formally, we have the following definition:

Definition 2.1 Let $(G, *)$ be a group and H be a non-empty subset of G. Then $(H, *)$ is called a subgroup of $(G, *)$ if $(H, *)$ is a group.

Let $(H, *)$ be a subgroup of a group $(G, *)$. Let e_H be the identity of H and e denote the identity of G. Now $e_H * e_H = e_H = e_H * e$, Hence by the left cancellation Law, $e_H = e$. Thus, the identity elements of G and H are the same. Now let $h \in H$. Let h' denotes the inverse of h in H and h^{-1} denotes the inverse of h in G. Then $h' = h' * e = h' * (h * h^{-1}) = (h' * h) * h^{-1} = e * h^{-1} = h^{-1}$. Thus the inverse of h in H and in G are the same. $(\{e\}, *)$ and $(G, *)$ are two subgroups of $(G, *)$. These subgroups are called trivial subgroups.

Examples of subgroups :

1. $(\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ and $(\mathbb{C}, +)$ and $(\mathbb{R}\setminus\{0\}, \cdot)$ is a subgroup of $(\mathbb{C}\setminus\{0\}, \cdot)$

Proof:

2. Let $m\mathbb{Z} = \{mk : k \in \mathbb{Z}\}$ where m is a fixed natural number, Here $(m\mathbb{Z}, +)$ is a subgroup of the group $(\mathbb{Z}, +)$

Note: In the remainder of the note, we shall generally use the notation G instead $(G, *)$ for a group and we write ab for $a * b$. We shall refer to ab as the product of a and b. This notation is usually called multiplicative notation.

Theorem 2.1 Let G be a group and H be a nonempty subset of G. Then H is a subgroup of G if and only if $ab^{-1} \in H$, $\forall a, b \in H$.

Proof: Suppose H is a subgroup of G. Let $a, b \in H$. Since H is a subgroup, it is a group and so $b^{-1} \in H$. Thus $ab^{-1} \in H$ since H is closed under the binary operation.

Conversely, suppose H is a nonempty subset of G such that $a, b \in H \Rightarrow ab^{-1} \in H$. Since $H \neq \phi$, $\exists\ a \in H$. So, $e = aa^{-1} \in H$ i.e H contains the identity. Now for each $b \in H$, $b^{-1} = eb^{-1} \in H$, i.e., every element of H has an inverse in H.

Thus, $\forall a, b \in H$, $a, b^{-1} \in H$ and so $ab = a(b^{-1})^{-1} \in H$, i.e., H is closed under the binary operation. As $H \subseteq G$, so, associativity holds for H as it holds for G.

Hence H is a group and so, H is a subgroup of G.

We use Theorem 2.1 to see whether a certain non-empty subset of a given group is a subgroup or not.

Theorem 2.1 Let G be a group and H be a finite nonempty subset of G. Then H is a subgroup of G if and only if $ab \in H$, $\forall a, b \in H$.

Proof: If H is a subgroup, then $ab \in H$, $\forall a, b \in H$. Conversely, suppose that $ab \in H$, $\forall a, b \in H$. Let $h \in H$. Then $h, h^2, \ldots h^n, \ldots \in H$ and so $\{h, h^2, \ldots, h^n, \ldots\} \subseteq H$. Since H is finite, all elements of $\{h, h^2, \ldots, h^n, \ldots\}$ can not be distinct. Thus, $\exists$ integers r and s such that $0 \leq r < s$ and $h^r = h^s$. Hence, $e = h^{s-r} \in H$ Now $s - r \geq 1$. Thus $e = h h^{s-r-1} \Rightarrow h^{-1} = h^{s-r-1} \in H$. Let $a, b \in H$. Then $a, b^{-1} \in H$ and so $ab^{-1} \in H$ by the hypothesis. Thus by Theorem 2.1, H is a subgroup.

Theorem 2.2 Let G be a group and $Z(G) = \{b \in G : ab = ba, \forall a \in G\}$. Then $Z(G)$ is a commutative subgroup of G. $Z(G)$ is called the center of G.

Proof: Since $ae = a = ea$ $\forall a \in G$, $e \in Z(G)$ and so $Z(G) \neq \phi$. Let $a, b \in Z(G)$. Then $bc = cb$ $\forall c \in G$. From this, it follows that $cb^{-1} = b^{-1}c$ $\forall c \in G$. and so $b^{-1} \in Z(G)$. Now $(ab^{-1})c = a(b^{-1}c) = a(cb^{-1})$ $= (ac)b^{-1} = (ca)b^{-1} = c(ab^{-1})$ $\forall c \in G$ and so $ab^{-1} \in Z(G)$. Hence by Theorem 2.1 $Z(G)$ is a subgroup. That $Z(G)$ is commutative follows from the definition $Z(G)$.

Theorem 2.2. Let G be a group and H be a non-empty subset of G. Then H is a subgroup G if and only if

(i) $ab \in H$, $\forall a, b \in H$

(ii) $a^{-1} \in H$ for each $a \in H$

Proof: Similar as that of Theorem 2.1