Theorem 2.3 Let G be a group and $\{H_\alpha : \alpha \in I\}$ be any non-empty collection of subgroups of G. Then $\bigcap_{\alpha \in I} H_\alpha$ is a subgroup.

Proof: Since each H_α is a subgroup, $e \in H_\alpha$ for all $\alpha \in I$. Hence $e \in \bigcap_{\alpha \in I} H_\alpha$ and $\bigcap_{\alpha \in I} H_\alpha \neq \phi$. Let $a, b \in \bigcap_{\alpha \in I} H_\alpha$. Then

$a, b \in H_\alpha$, $\forall \alpha \in I$. Thus, $ab^{-1} \in H_\alpha$, $\forall \alpha \in I$ since each H_α is a subgroup and so $ab^{-1} \in \bigcap_{\alpha \in I} H_\alpha$. Consequently $\bigcap_{\alpha \in I} H_\alpha$ is a subgroup

Note: Union of two subgroups of a group may not be a subgroup. $(3\mathbb{Z}, +)$ and $(4\mathbb{Z}, +)$ are two subgroups of $(\mathbb{Z}, +)$ but $3 \in 3\mathbb{Z}$ and $4 \in 4\mathbb{Z}$ but $3+4 = 7 \notin 3\mathbb{Z} \cup 4\mathbb{Z}$

So, $3\mathbb{Z} \cup 4\mathbb{Z}$ is not a subgroup of $(\mathbb{Z}, +)$.

Let G be a group and $a \in G$. Let $\langle a \rangle = \{a^n : n \in \mathbb{Z}\}$ Then $\langle a \rangle$ is a subgroup of G. $\langle a \rangle$ is called subgroup generated by a.

In additive notation, we have $\langle a \rangle = \{na : n \in \mathbb{Z}\}$

Let $(\mathbb{Z}, +)$ be the group. Then $\langle 2 \rangle = 2\mathbb{Z}$

Let G be a group and $a \in G$. Let $C(a) = \{b \in G : ba = ab\}$
Let e be the identity in G. Then $ea = ae = a$, so, $e \in C(a)$
$\therefore C(a) \neq \phi$. Let $b, c \in C(a)$. Then $ba = ab$ and $ca = ac$

As $ca = ac$, so, $c^{-1}a = ac^{-1}$.

Now $(bc^{-1})a = b(c^{-1}a) = b(ac^{-1}) = (ba)c^{-1} = (ab)c^{-1} = a(bc^{-1})$

$\therefore bc^{-1} \in C(a)$ $\therefore$ $C(a)$ is a subgroup G. $C(a)$ is called the centralizer of a in G. It is also called normalizer of a in G.

Let H and K be two subgroups of a group G.
Let $HK = \{hk : h \in H, k \in K\}$. HK may not be a subgroup.

For example, let $G = S_3$ $H = \{\rho_0, \rho_3\}$ and $K = \{\rho_0, \rho_4\}$ are two subgroups of G

Here $HK = \{\rho_0, \rho_1, \rho_3, \rho_4\}$ and $KH = \{\rho_0, \rho_2, \rho_3, \rho_4\}$

HK and KH are both not subgroups of S_3

Theorem 2.4 Let H and K be two subgroups of G. Then HK is a subgroup of G if and only if $HK = KH$

Proof: Let HK be a subgroup of G. Let $x \in HK$. Since HK is a subgroup, $x^{-1} \in HK$. Let $x^{-1} = h_1 k_1$, $h_1 \in H$, $k_1 \in K$

Then $x = k_1^{-1} h_1^{-1} \in KH$ $\therefore$ $HK \subset KH$

Let $y = k_2 h_2 \in KH$, $k_2 \in K$, $h_2 \in H$. Now $h_2^{-1} k_2^{-1} \in HK$ as $h_2^{-1} \in H$ and $k_2^{-1} \in K$

Since HK is a subgroup $(h_2^{-1} k_2^{-1})^{-1} = k_2 h_2 = y \in HK$.

$\therefore$ $KH \subset HK$. So $HK = KH$

Conversely, let $KH = HK$. Let $p, q \in HK$ and $p = h_3 k_3$, $q = h_4 k_4$ where $h_3, h_4 \in H$ and $k_3, k_4 \in K$

Then $pq = (h_3 k_3)(h_4 k_4) = h_3 (k_3 h_4) k_4 = h_3 (h_5 k_5) k_4$, since $KH = HK$

$= (h_3 h_5)(k_5 k_4) \in HK$. So, $p, q \in HK \Rightarrow pq \in HK$

Let $r \in HK$ and $r = hk$, $h \in H, k \in K$. $r^{-1} = (hk)^{-1} = k^{-1} h^{-1} \in KH = HK$

So, $r \in HK \Rightarrow r^{-1} \in HK$. So, HK is a subgroup of G.

We state a theorem without proof

Theorem 2.5 Let H, K are two finite subgroups of a group G such that HK is a subgroup of G. Then $o(HK) = \dfrac{o(H) \cdot o(K)}{o(H \cap K)}$

We state another theorem without proof

Theorem 2.6 Let a be an element of a group G. Then for integers m and n, (i) $a^m a^n = a^{m+n}$ (ii) $(a^m)^n = a^{mn}$ (iii) $(a^n)^{-1} = a^{-n}$

Order of an element : Let G be a group and $a \in G$. a is said to be of finite order if $\exists$ a positive integer such that $a^n = e$, e is the identity in G. The order of a, denoted by $o(a)$ is the least positive integer n such that $a^n = e$ and is denoted by $o(a)$.
a is said to be of infinite order if the order of a is not finite.

Examples : 1. In the group $(\mathbb{Z}_6, +)$, $o(\bar{1}) = 6$, $o(\bar{2}) = 3$, $o(\bar{3}) = 2$, $o(\bar{4}) = 3$, $o(\bar{5}) = 6$

2. In the group S_3, $o(\rho_1) = 3$, $o(\rho_2) = 3$, $o(\rho_3) = o(\rho_4) = o(\rho_5) = 2$

3. In the Klein's 4-group, $o(a) = o(b) = o(c) = 2$

4. In the group $(\mathbb{Z}, +)$, the order of each non-zero element is infinite

Note : The only element in a group which has order 1 is the identity element.

Another Theorem without proof is

Theorem 2.7 Let a be an element of a group G. Then

(i) $o(a) = o(a^{-1})$

(ii) if $o(a) = n$ and $a^m = e$, then n is a divisor of m (e is the identity element in G)

(iii) if $o(a) = n$ then $a, a^2, \ldots, a^n (= e)$ are distinct elements of G.

(iv) if $o(a) = n$, then for a positive integer m $o(a^m) = \frac{n}{\gcd(m, n)}$

(v) if $o(a) = n$, then $o(a^p) = n$ if and only if p is prime to n

(vi) if $o(a)$ is infinite and p is a positive integer, then $o(a^p)$ is infinite

Theorem 2.8 Every element of a finite group is of finite order.

Proof Let a be an element of a finite group G. Then $a, a^2, \cdots$ are all elements of G. Since G is finite, these elements are not all distinct. So, $a^m = a^n$ must hold for some positive integers m, n $(m > n)$

$\therefore \quad a^m(a^n)^{-1} = e \Rightarrow a^{m-n} = e$ (e is the identity in G)

This proves that a is ~~of~~ of finite order.

Worked out exercises: 1. In a group G, a is an element of order 30. Find the order of a^{18}

Ans: $o(a^{18}) = \cancel{\frac{o(a)}{\gcd}} = \frac{30}{\gcd(18,30)} = \frac{30}{6} = 5$

2. Find all elements of order 8 in the group $(\mathbb{Z}_{24}, +)$

Ans: The elements of the group are $\bar{0}, \bar{1}, \cdots, \overline{23}$, $o(\bar{0}) = 1$ and $o(\bar{1}) = 24$

Let $o(\bar{m}) = 8$, where $0 < m < 24$

$o(\bar{1}) = 24$. $o(\bar{m}) = o(m\bar{1}) = \frac{24}{\gcd(24, m)}$. As $o(\bar{m}) = 8$

$\therefore \gcd(24, m) = 3$. So $\frac{m}{3}$ and $\frac{24}{3}$ are prime to each other

So $\frac{m}{3}$ is less than 8 and prime to 8

i.e., $\frac{m}{3} = 1, 3, 5, 7$

Hence the elements of order 8 are $\bar{3}, \bar{9}, \overline{15}, \overline{21}$

Exercise 1. Show that $SL(2, \mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{R} \text{ and } \det\begin{pmatrix} a & b \\ c & d \end{pmatrix} = 1 \right\}$ is a subgroup of $GL(2, \mathbb{R})$ where $GL(2, \mathbb{R})$ is the group of all real non-singular matrices of order 2 with respect to matrix multiplication.

Note: $GL(2, \mathbb{R})$ is called the General linear group of degree 2 over $\mathbb{R}$ and $SL(2, \mathbb{R})$ is called the Special linear group of degree 2 over $\mathbb{R}$

2. In a group G, a is the only element of order n and $a \neq e$ (e is the identity element in G. Show that $n=2$ and $a \in Z(G)$)

~~Ans~~ Proof: Here $o(a) = n$ Now we know that

$o(a) = o(a^{-1})$, So $a = a^{-1} \Rightarrow a^2 = e$ As $a \neq e$, $n=2$

Also we know that $o(a) = o(xax^{-1})$ for any $x \in G$.

$\therefore$ $a = xax^{-1}$ or $xa = ax$ for any $x \in G$

$\therefore$ $a \in Z(G)$

3. Let G be a group in $(ab)^3 = a^3b^3$ $\forall a, b \in G$. Show that $H = \{x^2 : x \in G\}$ is a subgroup of G.

Proof: Let e be the identity in G. Then $e = e^2 \in H$ as $e \in G$

$\therefore$ $H \neq \phi$. Let ~~$a, b \in H$~~

Now ~~$(ab)^3 = a^3b^3$ $\forall a, b$~~ $(ab)^3 = a^3b^3$, $\forall a, b \in G$.

or. $(ab)(ab)(ab) = a^3b^3$ or $b(ab)a = a^2b^2$

or, $(ba)^2 = a^2b^2$, $\forall a, b \in G$. ... (1)

Let $a, b \in H$ then ~~(ab^{-1})~~ $a = x^2$, $b = y^2$, $x, y \in G$

So, $ab^{-1} = x^2(y^2)^{-1} = x^2(y^{-1})^2 = (y^{-1}x)^2$ from (1)

$\therefore$ $ab^{-1} = (y^{-1}x)^2$, $y^{-1}x \in G$.

$\therefore$ $ab^{-1} \in H$ $\therefore$ H is a subgroup of G.

We state another theorem without proof.

Theorem 2.9. Let G be a group and H, K are subgroups of G. Then $H \cup K$ forms a subgroup of G if and only if ~~$H \subset K$~~ $H \subset K$ or $K \subset H$

3. Cyclic group : A group G is said to be a cyclic group if $\exists$ an element $a \in G$ such that $G = \{a^n : n \in \mathbb{Z}\}$, i.e., $G = \langle a \rangle$. a is said to be a generator of the cyclic group.
In additive notatation, $G = \{na : n \in \mathbb{Z}\} = \langle a \rangle$

Examples: 1. $(\mathbb{Z}, +)$ is a cyclic group generated by 1. -1 is also a generator.
2. $(\mathbb{Z}_4, +)$ is a cyclic group generated by $\bar{1}$. $\bar{3}$ is also a generator.
3. Klein's 4-group is not a cyclic group as there is no generator.

Theorem 3.1 Let G be a cyclic group generated by a. Then a^{-1} is also a generator.
Proof Since a is a generator, $G = \{a^n : n \in \mathbb{Z}\}$
Let $H = \{(a^{-1})^n : n \in \mathbb{Z}\}$. Let $p \in G$ $\therefore p = a^r, r \in \mathbb{Z}$
Now $p = (a^{-1})^{-r}$, $-r \in \mathbb{Z}$ $\therefore p \in H$, So, $G \subset H$
$\therefore$ $H = G$ $\therefore$ a^{-1} is a generator of G.

Theorem 3.2 Every cyclic group is abelian
Proof: Let G be a cyclic group generated by a
Let $p, q \in G$. So, $p = a^r, q = a^s$, $r, s \in \mathbb{Z}$
So, $pq = a^r a^s = a^{r+s} = a^{s+r}$ as $r+s = s+r$
$= a^s a^r = qp$
$\therefore$ G is abelian

Note: An abelian group may not be cyclic. Example, Klein's 4-group is abelian but not cyclic.