Theorem 1: Let G be a non-empty set and o be a binary operation on G such that (1) o is associative

(2) $\exists$ an element e in G such that $e o a = a, \forall a \in G$ (e is called a left identity)

(3) For each $a \in G$, $\exists\ a' \in G$ such that $a' o a = a$ (a' is called a left inverse)

Then (G, o) is a group.

Proof: Let $a \in G$. So, $\exists\ a' \in G$ such that $a' o a = e$

we show that $a o a' = e$. As $a' \in G$, $\exists\ a'' \in G$ such that $a'' o a' = e$ ...(i)

Now $a o a' = e o (a o a')$ by (2)

$= (a'' o a') o (a o a')$ by (i)

$= a'' o (a' o a) o a'$ by (1)

$= a'' o (e o a')$ as $a' o a = e$

$= a'' o a'$ by (2)

$= e$ by (i)

Also $a o e = a o (a' o a)$

$= (a o a') o a$

$= e o a$

$= a$

So, $a o e = e o a = a$, for all $a \in G$

and for each $a \in G$, $\exists\ a'$ such $a o a' = a' o a = e$

So, G is a group.

Theorem 2 (Similar to Theorem 1) Let G be a non-empty set and o be a binary operation on G such that

(1) o is associative

(2) $\exists$ an element e in G such that $a o e = a, \forall a \in G$ (e is called a right identity)

(3) For each $a \in G$, $\exists\ a' \in G$ such that $a o a' = e$ (a' is called a right inverse)

Then (G, o) is a group

Proof: Exercise.

Note: A semigroup (G, o) in which there is a left identity e and every element a in G has right inverse, may not be a group.

Example: Consider the groupoid $(\mathbb{Z}, *)$ where $*$ is defined by $a * b = b$, $a, b \in \mathbb{Z}$. $*$ is associative as $a*(b*c) = b*c$ and $(a*b)*c = b*c$, so, $a*(b*c) = (a*b)*c$

Now $0 \in \mathbb{Z}$ and $0 * a = a$, $\forall a \in \mathbb{Z}$. So 0 is a left identity. Also, $a * 0 = 0$, $\forall a \in \mathbb{Z}$

So, 0 is a right inverse of each element $a \in \mathbb{Z}$

but $(\mathbb{Z}, *)$ is not a group as there is no identity element..

Problem 1: Let (G, o) be a group and $c \in G$. Define a binary operation $*$ on G by $a * b = a o c o b$, $\forall a, b \in G$. Show that $(G, *)$ is a group with c^{-1} as the identity element

Solution: As o is associative in G, so, $*$ is associative in G.

Let $a \in G$. Then $a * c^{-1} = a o c o c^{-1} = a o e = a$, e is the identity in (G, o)

and $c^{-1} * a = c^{-1} o c o a = e o a = a$

So, $a * c^{-1} = c^{-1} * a = a$, $\forall a \in G$. So, c^{-1} is the identity element in G.

Let $a \in G$. Then $a * (c^{-1} o a^{-1} o c^{-1}) = (c^{-1} o a^{-1} o c^{-1}) * a = c^{-1}$

So, $(G, *)$ is a group with c^{-1} as the identity element.

Problem 2: Let (G, o) be a finite abelian group with elements $a_1, a_2, \ldots, a_n$ and $x = a_1 o a_2 o \ldots o a_n$. Show that $x o x = e$, e is the identity element in (G, o).

Proof: $x^{-1} = a_n^{-1} o a_{n-1}^{-1} o \cdots o a_1^{-1} = a_1^{-1} o a_2^{-1} \cdots o a_n^{-1}$ (as (G, o) is abelian)

Now $a_i^{-1} = a_j^{-1} \Rightarrow a_i = a_j$. So, $a_1^{-1}, a_2^{-1}, \ldots a_n^{-1}$ are distinct elements in G. So, they are $a_1, \ldots a_n$ in some order.

So, $x^{-1} = a_1 o a_2 o \cdots o a_n = x$ (as G is abelian). So, $x o x = x o x^{-1} = e$

Theorem 3 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

(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.

Proof: (i) **Case 1** Let $o(a) = n$. Then $a^n = e$ and n is the least positive integer such that $a^n = e$. Now, $(a^{-1})^n = a^{-n} = (a^n)^{-1} = e^{-1} = e$.

If possible, let there be another positive integer $m < n$ such that $(a^{-1})^m = e$

Then $a^{-m} = e \Rightarrow (a^m)^{-1} = e \Rightarrow a^m = e$, a contradiction that n is the least positive integer such that $a^n = e$. So, n is the least positive integer such that $(a^{-1})^n = e$. So, $o(a^{-1}) = n$

So, $o(a) = o(a^{-1})$

Case 2 Let $o(a)$ be infinite. We assert that $o(a^{-1})$ is infinite.

If not, let $o(a^{-1}) = m$. Then $(a^{-1})^m = e$ or, $(a^m)^{-1} = e$

$\Rightarrow a^m = e$, a contradiction to the fact that $o(a)$ is infinite.

So, $o(a^{-1})$ is infinite also.

(ii) ~~$o(a) = n$~~ Here $o(a) = n$. By division algorithm,

$\exists$ integers q and r such that $m = qn + r$, $0 \le r < n$

Now $e = a^m = a^{nq+r} = a^{nq} \cdot a^r = (a^n)^q \cdot a^r = e^q \cdot a^r = a^r$

As, $o(a) = n$ and $0 \le r < n$, So, we must have

$r = 0$. So, $m = nq$. So n is a divisor of m.

(iii) If possible, let $a^r = a^s$ for some positive integers r and s such that $r < s \le n$ Then $a^s \cdot a^{-r} = e$ or $a^{s-r} = e$

Since $0 < s - r < n$, this contradicts the fact that $o(a) = n$

So, $a, a^2, \ldots a^n (= e)$ are all distinct.

(iv) $(a^m)^n = a^{mn} = (a^n)^m = e^m = e$ as $o(a) = n$. So $o(a^m)$ is finite.

Let $o(a^m) = k \Rightarrow (a^m)^k = e \Rightarrow a^{mk} = e \Rightarrow n$ divides mk (by (ii))

Let $\gcd(m,n) = d$ Then $m = du$, $n = dv$ and $\gcd(u,v) = 1$

n divides $mk \Rightarrow dv$ divides $duk \Rightarrow v$ divides uk

$\Rightarrow v$ divides k (as $\gcd(u,v) = 1$) ... (i)

Again, $(a^m)^v = (a^{du})^v = a^{duv} = (a^n)^u = e$ (as $o(a) = n$)

Now as $o(a^m) = k$ and $(a^m)^v = e$, k divides v ... (ii)

So, from (i) and (ii), $k = v = \frac{n}{d} = \frac{n}{\gcd(m,n)}$

So, $o(a^m) = \frac{n}{\gcd(m,n)}$

(v) Let p be prime to n. Then $\gcd(p,n) = 1$

Since $o(a) = n$, so, $o(a^p) = \frac{n}{\gcd(n,p)} = n$

conversely, let $o(a^p) = n$. But we have $o(a^p) = \frac{n}{\gcd(p,n)}$

So, $\gcd(p,n) = 1$. So p is prime to n.

(vi) If possible, let $o(a^p)$ be finite, say, m.

So, $o(a^p) = m \Rightarrow (a^p)^m = e \Rightarrow a^{pm} = e$

$\Rightarrow o(a)$ is finite, a contradiction

So, $o(a^p)$ is infinite.

Problem 3 Let G be a group and $a \in G$. An element b is said to conjugate to a if $\exists\ x \in G$ such that $b = xax^{-1}$

Prove that any conjugate of a has the same order as that of a.

Deduce that $o(ab) = o(ba)$, for $a, b \in G$.

Ans: Case I Let $o(a) = m$. Then $a^m = e$

Now $(xax^{-1})^m = xa^m x^{-1}$ (by mathematical induction)

$= xex^{-1} = xx^{-1} = e$.

Let $(xax^{-1})^k = e$ for some positive integer $k < m$. Then

$x a^k x^{-1} = e \Rightarrow a^k = e$, a contradiction that $o(a) = m$.

Hence $o(xax^{-1}) = m$, as m is the least positive integer such that $(xax^{-1})^m = e$

Case 2 Let $o(a)$ be infinite. Let $o(xax^{-1})$ be finite and $o(xax^{-1}) = k$ then $(xax^{-1})^k = e \Rightarrow x a^k x^{-1} = e$

$\Rightarrow a^k = e$, a contradiction, that $o(a)$ is infinite.

Hence $o(xax^{-1})$ is infinite

Now $ab = a(ba)a^{-1}$ So, $o(ab) = o(ba)$.

Theorem 4 Let H and K be finite subgroups of a group G such that HK is a subgroup of G. Then $o(HK) = \frac{o(H) \cdot o(K)}{o(H \cap K)}$

Proof: Let $o(H) = m$ and $o(K) = n$ and $o(H \cap K) = p$

Let $H = \{h_1, h_2, \ldots, h_m\}$ $K = \{k_1, k_2, \ldots, k_n\}$

$HK = \{h_i k_j : i, j \text{ are integers}, 1 \le i \le m, 1 \le j \le n\}$

The elements $h_i k_j$ in the list may not all be distinct. Let us find how many times an element, say, $h_p k_q$ $(1 \le p \le m, 1 \le q \le n)$ appears in the list.

Let $h_p k_q = h_r k_s$ for some integers r, s, $1 \le r \le m$, $1 \le s \le n$

Then $h_p^{-1} h_r = k_q k_s^{-1} = t$ (say) Then $h_p^{-1} h_r \in H$, $k_q k_s^{-1} \in K$

So, $t \in H \cap K$

$h_r = h_p t$ $k_s = t^{-1} k_q$. Thus $h_r k_s$ which equals $h_p k_q$ is of the form $(h_p t)(t^{-1} k_q)$ for some $t \in H \cap K$

Conversely, let $t \in H \cap K$, the element $(h_p t)(t^{-1} k_q) = h_p t_q$

Thus $h_p k_q$ appears in the list p times. As $h_p k_q$ may be any $h_i k_j$, i, j are integers, $1 \le i \le m$, $1 \le j \le n$, so,

$$o(HK) = \frac{mn}{p} = \frac{o(H)\,o(K)}{o(H \cap K)}$$