Chapter-I

Preliminaries and Prerequisites of Groups.

Introduction:- In this chapter, we discuss some basic definitions, results and certain technical terminologies of group theory which will be used throughout the rest of the chapters.

§(1.1) Groups :-

Definition (1.1) Let G be a nonempty set and $*$ be a binary operation defined on G. Then $(G,*)$ is said to be a group if the following conditions hold:

(i) $(a*b)*c = a*(b*c)$ for all $a,b,c \in G$.

(ii) There exists an element $e \in G$ such that $a*e = e*a = a$ for all $a \in G$.

(iii) For any $a \in G$, there exists $b \in G$ such that $a*b = b*a = e$.

In the above definition, e is unique and e is called the identity of the group G. Also b is unique and b is called the inverse of a and is denoted by a^{-1}.

Note that in an associative algebraic system with identity if an element has an inverse then that inverse is unique.

A group $(G,*)$ is said to be commutative (or abelian) if $a*b = b*a$ for all $a,b \in G$.

A group G is said to be non commutative if G is not commutative.

A group G is said to be finite if G has finite number of elements.

A group G is said to be infinite if G has infinite number of elements.

Examples (1.2) (i) $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{C},+)$ are all infinite commutative groups.

(ii) Note that neither $(\mathbb{Z},\cdot)$ nor $(\mathbb{Z}^*,\cdot)$ is a group, where $\mathbb{Z}^* = \mathbb{Z} - \{0\}$. On the other hand $(\mathbb{Q},\cdot)$, $(\mathbb{R},\cdot)$, $(\mathbb{C},\cdot)$ are not groups but $(\mathbb{Q}^*,\cdot)$, $(\mathbb{R}^*,\cdot)$, $(\mathbb{C}^*,\cdot)$ are all infinite commutative groups, where $\mathbb{Q}^* = \mathbb{Q} - \{0\}$, $\mathbb{R}^* = \mathbb{R} - \{0\}$ & $\mathbb{C}^* = \mathbb{C} - \{0\}$.

Let $\mathbb{Z}_n = \{[0], [1], \cdots, [n-1]\}$. We define a binary operation $+_n$ on $\mathbb{Z}_n$ by $[a] +_n [b] = [a+b]$ for all $[a], [b] \in \mathbb{Z}_n$. Then $(\mathbb{Z}_n, +_n)$ is a finite commutative group.

Note that $(\mathbb{Z}_n, \cdot_n)$ is not a group where the binary operation $\cdot_n$ is defined on $\mathbb{Z}_n$ by $[a] \cdot_n [b] = [ab]$ for all $[a], [b] \in \mathbb{Z}_n$.

Let $\mathbb{Z}_n^* = \mathbb{Z}_n - \{[0]\}$. Then $(\mathbb{Z}_n^*, \cdot_n)$ is a group if and only if n is a prime. Note that for a prime p, $\mathbb{Z}_p^*$ is a finite commutative group w.r.t. the multiplication defined above.

(iii) Let $M_n(\mathbb{R})$ denote the collection of all square matrices of order n over $\mathbb{R}$. Then $M_n(\mathbb{R})$ forms an infinite commutative group w.r.t. matrix addition, but it is important to note that $M_n(\mathbb{R})$ does not form a group w.r.t. matrix multiplication.

If we consider the collection of all invertible $n \times n$ matrices over $\mathbb{R}$ then it forms a non-commutative group under matrix multiplication. This group is called the general linear group of degree n and is denoted by $GL(n, \mathbb{R})$ or $GL_n(\mathbb{R})$.

(iv) Let X be a non-empty set and $A(X) = \{f : X \to X \mid f \text{ is a bijection}\}$. Then $A(X)$ forms a group under composition of mappings.

If X is an infinite set, then $A(X)$ forms an infinite non-commutative group.

If X is a non-empty set then a bijection $f : X \to X$ is called a permutation on X. The permutations on the set $X = \{1, 2, \cdots, n\}$ forms a group under composition of mappings. This group is called the symmetric group on n symbols and is denoted by S_n. Since there are $n!$ permutations on a set of n elements, S_n has $n!$ elements. Note that S_n is a finite non-commutative group.

Result (1.3) Let $(G, *)$ be a group. Then the following results hold:

(i) For all $a \in G$, $(a^{-1})^{-1} = a$

(ii) For all $a, b \in G$, $(a*b)^{-1} = b^{-1} * a^{-1}$.

(iii) For all $a, b, c \in G$, if either $a*c = b*c$ or $c*a = c*b$ then $a = b$. i.e. in a group, both left cancellation and right cancellation property hold.

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

(v) If $a*a = a$ then $a = e_G$ i.e. in a group, the identity element is the only idempotent element in G.

Definition (1.4) Let $(G, *)$ be a group and $a \in G$. If there exists a positive integer m such that $a^m = e_G$, then a is said to be of finite order. The smallest positive integer n such that $a^n = e_G$ is called the order of a. If no such positive integer exists then a is said to be of infinite order. The order of a will be denoted by $o(a)$.

By the order of a finite group G we shall mean the number of elements in G. The order of G will be denoted by $|G|$.

Result (1.5) Let $(G, *)$ be a group and $a \in G$ be such that $o(a) = n$.

(i) If $a^m = e_G$ for some positive integer m, then n divides m.

(ii) For every positive integer t, $o(a^t) = \frac{n}{\gcd(t, n)}$.

§1.2 Subgroup.

Definition 1.2.1 (i) Let $(G,*)$ be a group and H a nonempty subset of G. H is said to be stable under the binary operation '$*$' defined on G if $h_1 * h_2 \in H$ for all $h_1, h_2 \in H$.

The stability of H under '$*$' induces a binary operation on H which we call the induced binary operation on H and which is denoted by the same symbol '$*$'.

Definition 1.2.1 (ii) Let $(G,*)$ be a group and H a nonempty subset of G. Then H is called a subgroup of G if H is stable under the binary operation '$*$' defined on G and is group w.r.t. the binary operation induced by the stability of H under '$*$'. This subgroup is denoted by $(H,*)$.

Alternative definition of subgroup:—

Definition 1.2.1 (iii) Let $(G,*)$ and $(H,*')$ be two groups. Then $(H,*')$ is called a subgroup of G if H is a subset of G and the binary operation '$*'$' defined on H is the restriction of the binary operation '$*$' defined on G i.e. $h_1 *' h_2 = h_1 * h_2$ for all $h_1, h_2 \in H$.

A subgroup $(H,*)$ of a group $(G,*)$ is said to be proper if $H \neq G$.

Examples 2.2 (i) Let $G=(\mathbb{Z},+)$. Then $H=n\mathbb{Z}$, where n is a non-negative integer, is a subgroup of $\mathbb{Z}$. Note that all subgroups of $\mathbb{Z}$ are of the form $n\mathbb{Z}$, where n is a non-negative integer.

(ii) Let $G=(S_n,\circ)$. Consider the subset A_n of all even permutations of S_n. Then A_n is a subgroup of S_n, called the alternating group on n symbols.

(iii) Let $G=GL(n,\mathbb{R})$ and $SL(n,\mathbb{R})=\{A\in GL(n,\mathbb{R}): \det A=1\}$. Then $SL(n,\mathbb{R})$ is a subgroup of $GL(n,\mathbb{R})$; it is called the special linear group of degree n.

(iv) Let G be a group w.r.t. multiplication and $Z(G)=\{a\in G: ab=ba \text{ for all } b\in G\}$. Then $Z(G)$ is a subgroup of G. It is called the centre of G. Note that G is a commutative group if and only if $G=Z(G)$.

(v) Let G be a group w.r.t. multiplication and $C(a)=\{g\in G: ga=ag\}$. Then $C(a)$ is a subgroup of G and it is called the centralizer of a in G.

(vi) Let $O(n)=\{A\in GL(n,\mathbb{R}): AA^T=A^TA=I_n\}$ and
$SO(n)=\{A\in O(n): \det A=1\}$.
Then $SO(n)$ is a subgroup of $O(n)$.

Result: (i) Let G be a group with identity e_G and H be a subgroup of G with identity e_H. Then $e_G = e_H$.

(ii) Let G be a group and H be a nonempty subset of G. Then H is a subgroup of G if and only if for all $a, b \in H$, $ab^{-1} \in H$.

(iii) Let G be a group and H be a nonempty finite subset of G. Then H is a subgroup of G if and only if for all $a, b \in H$, $ab \in H$.
Note that the finiteness condition of the nonempty subset H in the above result is necessary. For this consider $G = (\mathbb{Z}, +)$ and $H = (\mathbb{N}, +)$. Then $\mathbb{N}$ is not a subgroup of $\mathbb{Z}$ although $\mathbb{N}$ is closed under addition.

(iv) The intersection of any collection of subgroups of a group G is a subgroup of G. But union of two subgroups of G may not be a subgroup of G.

(v) Let H and K be two subgroups of a group G. Then $HK = \{hk : h \in H \text{ and } k \in K\}$ is a subgroup of G if and only if $HK = KH$.

(vi) Let H and K be two finite subgroups of a group G. Then
$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

(vii) Let H be a subgroup of a group G. Then for every $g \in G$, the set $gHg^{-1} = \{ghg^{-1} : h \in H\}$ is a subgroup of G and $|gHg^{-1}| = |H|$.

§3 Cyclic Groups

Let G be a group and S be a subset of G. Now consider the collection $\mathcal{H}$ of all subgroups of G that contain S. This collection is not empty since it clearly includes the whole group G itself. Also the intersection of all subgroups of G that contain S, is also a subgroup of G containing S. It is the smallest subgroup of G that contains S. We denote it by $\langle S \rangle$ and call it the subgroup generated by S. Clearly if $S = \emptyset$ then $\langle S \rangle = \{e\}$. If S is a non-empty subset of G, say $S = \{x_1, x_2, \ldots, x_n\}$ then

$$\langle S \rangle = \{x_1 x_2 \cdots x_n : x_i \in S \text{ or } x_i^{-1} \in S \text{ for each } i = 1, 2, \ldots, n\}.$$

In this case if $\langle S \rangle = G$, then G is called a finitely generated group. If there does not exist a finite set S such that $\langle S \rangle = G$ then we say that the group G is not finitely generated. An important particular case of the above is obtained by taking the set S to be a singleton, say $S = \{g\}$ for some $g \in G$. In this case we write $\langle S \rangle = \langle g \rangle$ and

$$\langle g \rangle = \{\cdots g^{-2}, g^{-1}, g^0, g^1, g^2 \cdots\} = \{g^n : n \in \mathbb{Z}\}.$$

Definition 3.1 A group G is said to be a cyclic group if $G = \langle g \rangle$ for some $g \in G$. Thus if G is a cyclic group then $G = \langle g \rangle = \{g^n : n \in \mathbb{Z}\}$. In this case g is called a generator of G.

Examples 3.2 (i) $(\mathbb{Z}_n, +_n)$ is a finite cyclic group.
(ii) $(\mathbb{Z}, +)$ is an infinite cyclic group.

Results 3.3 (i) Every cyclic group is a commutative group; but a commutative group may not be a cyclic group. For this consider $G = K_4$ (the Klein's 4-group). Then K_4 is a commutative group but not a cyclic group. It is important to note that every proper subgroup of K_4 is cyclic.

(i) Let G be a cyclic group generated by a. Then a^{-1} is also a generator of G. If G is an infinite cyclic group generated by a then a and a^{-1} are the only generators of G. If G is a finite cyclic group of order n then G has $\phi(n)$ number of generators where $\phi(n) = \{m \in \mathbb{N} : m < n \text{ and } \gcd(m,n) = 1\}$. Note that if G is a finite cyclic group then G has unique generator if and only if $|G| = 1$ or $|G| = 2$.

(ii) A finite group G is a cyclic group if and only if there exists an element $a \in G$ such that $o(a) = |G|$.

(iii) Let $G = \langle a \rangle$ be a cyclic group of order n. Then for any integer m, where $1 \leq m < n$, a^m is a generator of G if and only if $\gcd(m,n) = 1$.

(iv) Every subgroup of a cyclic group is cyclic.

(v) A cyclic group G of finite order n has one and only one subgroup of order d for every positive divisor d of n i.e. there exists a one-to-one correspondence between the set of all positive divisors of n and the set of all subgroups of G.

(vi) The group G_n of the n^{th} roots of unity is a cyclic group of order n.

** Note that if G is a finite commutative group of order n then corresponding to each positive divisor d of n there may exist more than one subgroup of G of order d. For example K_4 is a finite commutative group of order 4 and corresponding to the divisor 2 of 4, K_4 has more than one subgroup of order 2.

(vii) ~~Every finite cyclic group of ord~~

1.4 Cosets and Lagrange's Theorem :—

Definitions 1.4.1 Let G be a group and H be a subgroup of G. Then the subset aH of G is called a left coset of H in G and a is called a representative element of the left coset aH in G. Similarly we can define a right coset of H in G and a representative element of aH in G.

Results 1.4.2 (i) Let G be a group and H be a subgroup of G. Then H itself is a left coset of H in G since $eH = He = H$ for all $h \in H$.

The order of the set of all distinct left cosets of H in G is equal to the order of the set of all distinct right cosets of H in G. This order is called the index of H in G and is denoted by $[G : H]$.

Results 1.4.2. Let H be a subgroup of a group G and $a, b \in G$. Then

(i) H is a left coset as well as a right coset of itself in G since $eH = He = H = hH = Hh$ for all $h \in H$.

(ii) $aH = H$ iff $a \in H$ and $Ha = H$ iff $a \in H$.

(iii) $aH = bH$ iff $a^{-1}b \in H$ and $Ha = Hb$ iff $ab^{-1} \in H$.

(iv) either $aH \cap bH = \phi$ or $aH = bH$. Similarly either $Ha \cap Hb = \phi$ or $Ha = Hb$.

(v) G is the union of all distinct left cosets as well as of all distinct right cosets of H in G.

(vi) $|aH| = |H| = |Ha|$.

(vii) The relation ρ defined on G by $a \rho b$ iff $a^{-1}b \in H$. Then ρ is an equivalence relation

Theorem 4.4 (Lagrange's Theorem): 11

Let H be a subgroup of a finite group G. Then $|H|$ divides $|G|$. and precisely, $|G| = [G:H]\,|H|$.

Note that the converse of Lagrange's Theorem does not always hold.

Corollary 4.5 (i) In a finite group the order of every element divides the order of the group i.e. $o(a) \mid |G|$ for all $a \in G$.

(ii) If G is a group of order n then $g^n = e_G$ for all $g \in G$.

(iii) All groups of prime order are cyclic. From this result we can conclude that all groups of prime order are commutative, since every cyclic group is a commutative group.

(iv) Let G be a group and H, K be two subgroups of G such that $|H| = m$ and $|K| = n$. If $\gcd(m,n) = 1$, then $|H \cap K| = 1$ i.e. $H \cap K = \{e_G\}$.

§(5) Normal Subgroups and Quotient Groups:

In the previous §(4), we have seen that each subgroup H of a group G partitions G into left cosets and also partitions G into right cosets. In general, these partitions are not the same, i.e. the left cosets and the right cosets may not coincide for an arbitrary subgroup. But certainly there exists certain class of subgroups for which the left and right cosets coincide. This special class of subgroups are commonly known as the normal subgroups in group theory.

Definition (5.1) Let G be a group and H be a subgroup of G. Then H is said to be a normal subgroup of G if $gH = Hg$ for all $g \in G$.

Note that $gH = Hg$ implies that $gh = h'g$ for some $h, h' \in H$ but $gH = Hg$ does not always mean that $gh = hg$ for all $h \in H$ and for all $g \in G$.

Clearly every group G has atleast two normal subgroups, namely $\{e\}$ and G itself. If G is a commutative group then every subgroup of G is a normal subgroup of G.

Examples (5.2) (i) $n\mathbb{Z}$, where n is a non-negative integer is a normal subgroup of $\mathbb{Z}$.

(ii) A_n is a normal subgroup of S_n

(iii) $SL(n, \mathbb{R})$ is a normal subgroup of $GL(n, \mathbb{R})$

(iv) $SO(n)$ is a normal subgroup of $O(n)$.

(v) Let G be a group and $Z(G)$ be the centre of G. Then $Z(G)$ is a normal subgroup of G.

Let's (5.3) (i) Let G be a group and H be a subgroup of G. Then H is normal subgroup of G if and only if $gHg^{-1} \subseteq H$ for all $g \in G$ i.e., $ghg^{-1} \in H$ for all $g \in G$ and for all $h \in H$.

(ii) If H and K are two normal subgroups of a group G then $HK = KH$ is a normal subgroup of G. Also $H \cap K$ is a normal subgroup of G.

(iii) Let H be a subgroup of a group G such that $[G:H] = 2$. Then H is a normal subgroup of G.

(iv) The transitive property of the relation 'being a normal subgroup' does not hold for normal subgroups of a group i.e. if H is a normal subgroup of K and K is a normal subgroup of G then H need not be the normal subgroup of G. For this consider the following example: consider the group $G = A_4$ and $H = \{e, (12)(34)\}$, $K = \{e, (12)(34), (13)(24), (14)(23)\}$. Then H is a normal subgroup of K and K is a normal subgroup of G, but H is not a normal subgroup of G.

(v) If H is the unique subgroup of order n in a group G then H is a normal subgroup of G.

Definition (5.4) Let G be a group and H be a normal subgroup of G. Consider $G/H = \{aH : a \in G\}$. We define a binary operation $*$ on G/H by $(aH) * (bH) = (ab)H$ for all $aH, bH \in G/H$. Then $(G/H, *)$ forms a group. This group is called the quotient group or factor group of G by H.

Note that the identity of G/H is $eH = H$, since $e \in H$.

Results (i) If G is a finite group and H is a normal subgroup of G then $|G/H| = \frac{|G|}{|H|} = [G:H]$, by using Lagrange's Theorem.

(ii) If G is a finite cyclic group of order n then G has a unique normal subgroup of order d for every positive divisor of n. Consequently, the number of quotient groups of a finite cyclic group of order n is equal to the number of positive divisors of n.

(iii) If H is a subgroup of a commutative group G, then the quotient group G/H is a commutative group but not conversely. Note that S_3/A_3 is a commutative group but S_3 is not a commutative group.

(iv) If H is a subgroup of a cyclic group then the quotient group G/H is cyclic but not conversely. Note that S_3/A_3 is cyclic but S_3 is not cyclic.

~~(vi) Let H be a subgroup of a group G. If G/H is commutative. Then H is a normal subgroups of G and G/H is commutative.~~

(v) Let H and K be two normal subgroups of a group G such that $H \subseteq K$. Then K/H is a normal subgroup of G/H. Also every normal subgroup of G/H is of the form K/H, where K is a normal subgroup of G such that $H \subseteq K$.

Worked Out Exercises

Exercise (1.1) Let $G = \left\{ \begin{pmatrix} a & a \\ a & a \end{pmatrix} : a (\neq 0) \in \mathbb{R} \right\}$. Does G forms a group w.r.t. matrix multiplication? Justify your answer.

Solution: Obviously G is closed w.r.t. the matrix multiplication property. Matrix multiplication is associative, G has the identity element $E = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}$ as $\begin{pmatrix} a & a \\ a & a \end{pmatrix}\begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}\begin{pmatrix} a & a \\ a & a \end{pmatrix} = \begin{pmatrix} a & a \\ a & a \end{pmatrix}$.

Also every element $\begin{pmatrix} a & a \\ a & a \end{pmatrix}$ of G has the inverse $\begin{pmatrix} \frac{1}{4a} & \frac{1}{4a} \\ \frac{1}{4a} & \frac{1}{4a} \end{pmatrix}$, since $\begin{pmatrix} a & a \\ a & a \end{pmatrix}\begin{pmatrix} \frac{1}{4a} & \frac{1}{4a} \\ \frac{1}{4a} & \frac{1}{4a} \end{pmatrix} = \begin{pmatrix} \frac{1}{4a} & \frac{1}{4a} \\ \frac{1}{4a} & \frac{1}{4a} \end{pmatrix}\begin{pmatrix} a & a \\ a & a \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}$.

Hence G forms a group w.r.t. matrix multiplication.

Exercise (1.2) Show that A_4 has no subgroup of order 6.

Solution: If possible, let H be a subgroup of A_4 of order 6.

Note that A_4 has eight 3-cycles namely, $(1\,2\,3), (1\,3\,2), (1\,2\,4), (1\,4\,2), (2\,3\,4), (2\,4\,3), (1\,3\,4), (1\,4\,3)$. Since $|H| = 6$, there exists a 3-cycle, say α such that $\alpha \in H$. Since α is a 3-cycle, $\alpha^3 = e$. This implies that $\alpha^2 = \alpha^{-1} \in H$. Let $X = \{e, \alpha, \alpha^2\}$. Then X is a subgroup of A_4 such that $|X| = 3$ and $H \cap X = \{e\}$. Thus $|HX| = \frac{|H||X|}{|H \cap X|} = 18$ ~~=~~ $|A_4| = 12$, which is a contradiction.

Hence A_4 has no subgroup of order 6.

Note: From above Exercise (1.2), we can conclude that the converse of Lagrange's Theorem does not always hold.

Exercise (1.3) (i) Let G be a group and $Z(G)$ be the centre of G. If $G/Z(G)$ is cyclic then show that G is a commutative group.

(ii) Let G be a finite non-commutative group. Show that $|Z(G)| \leq \frac{1}{4}|G|$.

Solution: Let $Z(G) = H$ and $G/Z(G) = G/H$ be cyclic. Then $G/H = \langle gH \rangle$ for some $g \in G$. Let $a, b \in G$. Then $aH, bH \in G/H = \langle gH \rangle$. So we have $aH = g^m H$ and $bH = g^n H$ for some $m, n \in \mathbb{Z}$. Since $a = ag \in aH = g^m H$ and $b = bg \in bH = g^n H$, it follows that $a = g^m c$ and $b = g^n d$ for some $c, d \in H = Z(G)$. Now $ab = (g^m c)(g^n d) = g^m g^n cd = g^{m+n} cd = g^{n+m} dc = g^n g^m dc = (g^n d)(g^m c) = ba$. This shows that G is a commutative group.

(ii) To show that $|Z(G)| \leq \frac{1}{4}|G|$, we have to show that $\frac{|G|}{|Z(G)|} = |G/Z(G)| \geq 4$. If possible, let $|G/Z(G)| < 4$. Then $|G/Z(G)|$ is either 1 or 2 or 3. If $|G/Z(G)| = 1$ then $G = Z(G)$ i.e. G is a commutative group, which is a contradiction. If $|G/Z(G)| = 2$ or 3 then $G/Z(G)$ is cyclic and hence G is commutative, by previous result, which is again a contradiction. Hence $|G/Z(G)| \geq 4$ i.e. $\frac{|G|}{|Z(G)|} \geq 4$ i.e. $|Z(G)| \leq \frac{1}{4}|G|$.

Exercise (1.4) Let H be a normal subgroup of a group G such that $|H| = 2$. Show that $H \subseteq Z(G)$.

Solution: Let $H = \{e, h\}$. Then for every $g \in G$, we have $ghg^{-1} \in H = \{e, h\}$. Since H is normal in G. So $ghg^{-1} = e$ or $ghg^{-1} = h$. If $ghg^{-1} = e$ then $h = e$, a contradiction to our assumption that $|H| = 2$. So $ghg^{-1} = h$ i.e. $gh = hg$ for all $g \in G$. This shows that $h \in Z(G)$ and hence $H \subseteq Z(G)$.

✓

Exercise (1.5). Let H and K be two normal subgroups of a group G. If $H \cap K = \{e\}$, then show that $ab = ba$ for all $a \in H$ and $b \in K$.

Solution: Let $a \in H$ and $b \in K$. Then $aba^{-1}b^{-1} = a(ba^{-1}b^{-1}) \in H$, since H is normal in G and $a \in H$. Again $aba^{-1}b^{-1} = (aba^{-1})b^{-1} \in K$, since K is normal in G and $b \in K$. So we find that $aba^{-1}b^{-1} \in H \cap K = \{e\}$ i.e. $aba^{-1}b^{-1} = e$ i.e. $ab = ba$ for all $a \in H$ and $b \in K$.

Exercise (1.6) Let G be a finite group and N be a normal subgroup of G such that $[G:N]$ and $|N|$ are relatively prime. Show that an element $x \in G$ satisfying $x^{|N|} = e$ must be in N.

Solution: We first note that $x^{[G:N]} \in N$, since $|G/N| = [G:N]$, so we have $(xN)^{[G:N]} = N$ i.e. $x^{[G:N]}N = N$ i.e. $x^{[G:N]} \in N$.
Again, since $[G:N]$ and $|N|$ are relatively prime, there exist $m, n \in \mathbb{Z}$ such that $m[G:N] + n|N| = 1$. Let $x \in G$ be such that $x^{|N|} = e$.
Then $x = x^{m[G:N]+n|N|} = (x^{[G:N]})^m (x^{|N|})^n = (x^{[G:N]})^m \in N$, since $x^{|N|} = e$ and $x^{[G:N]} \in N$.

Exercise (1.7) Show that every group of order less than 6 is commutative.

Solution: Let G be a group such that $|G| < 6$.
Case (I) If $|G| = 1$, then $G = \{e\} = \langle e \rangle$ and hence G is trivially commutative.
Case (II) If $|G| = 2$ or 3 or 5 then G is cyclic and hence G is commutative.
Case (III) If $|G| = 4$ then G is also commutative. We now show this.
If G is a cyclic group of order 4 then G is a commutative group.
Now suppose that G is a non cyclic group of order 4. Then G has no element of order 4. By corollary (4.5) (2), each non-identity element of G is of order 2 i.e. $O(a) = 2$ for all $a (\neq e) \in G$. Thus $a^2 = e$ implies that $a = a^{-1}$ for all $a \in G$. Now for any $a, b \in G$, we have $ab = (ab)^{-1} = b^{-1}a^{-1} = ba$. This shows that G is a commutative group.

Exercises 18

(1) Let θ be a fixed real number and let $A = \begin{pmatrix} 0 & 1 & -\sin\theta \\ -1 & 0 & \cos\theta \\ -\sin\theta & \cos\theta & 0 \end{pmatrix}$. Given $x \in \mathbb{R}$, define the 3×3 matrix A_x by $A_x = I_3 + xA + \frac{1}{2}x^2A^2$, where I_3 is the 3×3 identity matrix. Prove that $G = \{A_x : x \in \mathbb{R}\}$ is a commutative group w.r.t. matrix multiplication.

(2) (i) Give an example of an infinite group whose every element is of finite order.

(ii) Give an example of a group G in which there exist two elements a and b of finite order whereas ab is of infinite order.

(3) (i) Let G be a finite group of even order. Show that G contains an odd number of elements of order 2.

(ii) Let G be a commutative group of order $2n$, where n is a positive integer. Show that G has unique element of order 2. Is the condition of commutativity of G essential? Justify your answer.

(4) (i) Let G be a group and a be the only element of order 2 in G. Show that $a \in Z(G)$, where $Z(G)$ is the centre of G.

(ii) Let G be a group of order 8 and g be an element of order 4. Show that $g^2 \in Z(G)$.

(5) (i) Let G be a non commutative group of order 6. Show that $Z(G) = \{e\}$.

(ii) Show that $Z(S_3) = \{e\}$.

(iii) Let $G = GL(2,\mathbb{R})$. Show that $Z(G) = \left\{\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} : a \in \mathbb{R}\right\}$.

(6) Show that a group cannot be written as the union of its two proper subgroups.

(7) If a cyclic subgroup H of a group G is normal in G then show that every subgroup of H is also normal in G.

(8) (i) Give an example of a non cyclic commutative group all of whose proper subgroups are cyclic.

(ii) Give an example of a non cyclic non commutative group all of whose proper subgroups are cyclic.

(9) Let $G = \left\{ \begin{pmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ b & c & 1 \end{pmatrix} : a, b, c \in \mathbb{Z}_3 \right\}$. Show that $|G| = 27$ and each non-identity element of G has order 3.

(10) Let G be a group which has a subgroup H such that $|G| < 45$ and $|H| > 10$. If $[G:H] > 3$, then find $|H|$, $|G|$ and $[G:H]$.

(11) Let G be a group such that G has subgroups of order 15 and 75. If $|G| < 400$ then find $|G|$.

Let H be a subgroup of a group G such that $g^2 \in H$ $\forall$ all $g \in G$. Show that H is a normal subgroup of G and G/H is commutative.

(12) Show that $(\mathbb{R}, +)$ is not a cyclic group. Hence show that $(\mathbb{R}, +)$ is not a cyclic group.