(2.11) Theorem. Let G be any group and let $a \in G$ have order n. Then, for any integer k, $a^k = e$ if and only if $k = nq$, where q is an integer.

Proof. Suppose that n is the order of a and, for some integer k, $a^k = e$. By the division algorithm[1], there are unique integers q and r such that

$$k = nq + r, \quad 0 \le r < n$$

so that

$$e = a^k = (a)^{nq+r} = (a^n)^q \cdot a^r = e \cdot a^r = a^r \quad (\text{as } a^n = e)$$

Since a has order n, therefore, n is the smallest integer for which $a^n = e$ and so $r = 0$.

Thus $k = nq$.

Conversely, suppose that $k = nq$. Then

$$a^k = e^{nq} = (a^n)^q = e^q = e.$$

Example 11. Show that the set

$$S = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$$

is a group under multiplication modulo 8. Find the order of each element of S.

Solution. The Cayley's table for S under multiplication modulo 8 is as given below:

$\cdot$	$\bar{1}$	$\bar{3}$	$\bar{5}$	$\bar{7}$
$\bar{1}$	$\bar{1}$	$\bar{3}$	$\bar{5}$	$\bar{7}$
$\bar{3}$	$\bar{3}$	$\bar{1}$	$\bar{7}$	$\bar{5}$
$\bar{5}$	$\bar{5}$	$\bar{7}$	$\bar{1}$	$\bar{3}$
$\bar{7}$	$\bar{7}$	$\bar{5}$	$\bar{3}$	$\bar{1}$

For example, here $5 \times 3 = 15$ which gives 7 as remainder after division by 8.

So $\quad \bar{5} \times \bar{3} = \bar{7}$

Similarly, $\quad \bar{3} \times \bar{7} = \bar{5}$

One may observe from the multiplication table that $\bar{1}$ is the identity element in S. The closure law and the existence of inverse of each element can easily be verified from the table.

1. The division algorithm states that, for any two integers a and b with $a > 0$, there are integers q and r such that

$$b = aq + r, \quad 0 \le r < a.$$

For the orders of elements, we see that the order of $\overline{1}$ is 1.

The order of $\overline{3}$ is 2 because $\overline{3} \times \overline{3} = \overline{1}$.

Similarly, the order of each of $\overline{5}$ and $\overline{7}$ is 2.

Example 12. Let G be a group and $a, b \in G$. Show that

(i) The orders of a and a^{-1} are equal.

(ii) The orders of a and $b^{-1}ab$ are equal.

(iii) The orders of ab and ba are equal.

Solution. (i) Let $a \in G$. Suppose the order of a is m so that $a^m = e$.

Now, $a^m = e \quad \Leftrightarrow \quad a^{-m} . a^m = a^{-m} . e$

$\Leftrightarrow \quad e = (a^{-1})^m$.

So the order of a^{-1} is a divisor k of m.

But $(a^{-1})^k = e$ implies $a^{-k} . a^k = e . a^k = a^k$

Thus $e = a^k$.

But then m divides k. Thus $k = m$. So the order of a^{-1} is also m.

(ii) Let $a, b \in G$. Suppose, the order of a is m then $a^m = e$. Therefore,

$$a^m = e \quad \Leftrightarrow \quad b^{-1} a^m b = b^{-1} eb$$

$$\Leftrightarrow \quad (b^{-1} ab)^m = e$$

Hence the orders of a and $b^{-1} ab$ are equal.

[Here we have used the fact that $(b^{-1} ab)^m = b^{-1} a^m b$ which is proved induction on m as follows.

The result is true for $m = 1$. Suppose it is true for $m = k$, i.e., $(b^{-1} ab)^k = b^{-1} a^k b$

Now $(b^{-1} ab)^{k+1} = (b^{-1} ab)^k (b^{-1} ab) = (b^{-1} a^k b)(b^{-1} ab) = b^{-1} a^k e ab = b^{-1} a^{k+1}$

Hence $(b^{-1} ab)^m = b^{-1} a^m b$ for all $m \in N$].

(iii) Suppose $|ab| = m$.

Now, $ab = b^{-1} bab = b^{-1}(ba)b$, **(Associative Law)**

$$\text{or} \quad (ab)^m = e = [b^{-1}(ba)b]^m$$

$$= b^{-1}(ba)^m b, \quad \text{as in (ii)}$$

$$\text{or} \quad beb^{-1} = bb^{-1}(ba)^m bb^{-1}$$

$$\text{or} \quad e = (ba)^m$$

$$\text{Thus} \quad |ba| = m.$$

Example 13 Let G be a group of even order. Prove that there is at least one element of order 2 in G.

Solution. Let G be a group of even order. Then the non-identity elements in G will be odd in number. Also the inverse of each element of G belongs to G and that $e^{-1} = e$.

There occur pairs each consisting of some non-identity element x and x^{-1} in G such that $x \neq x^{-1}$. As there are odd number of non-identity elements in G, after pairing off such non-identity elements for which $x \neq x^{-1}$, we must have at least one element $a\ (\neq e) \in G$ such that

$$a = a^{-1}$$

But then $\quad aa = aa^{-1}$

or $\quad a^2 = e$

Hence $\quad |a| = 2.$

Example 14. Let G be a group and x be an element of odd order in G. Then there exists an element y in G such that $y^2 = x$.

Solution. For some nonnegative integer m and $x \in G$, let $\quad |x| = 2m + 1$,

so that we have $\quad x^{2m+1} = e \qquad (1)$

Clearly $\quad x, x^2, \cdots, x^m, x^{m+1}, \cdots, x^{2m} \in G$

Let $\quad y = x^{m+1}$. Then

$$y^2 = x^{2m+2} = x^{2m+1}x = ex = x, \text{ by (1)}.$$

EXERCISE 2.1

1. Answer true or false. Justify your answer.
   (i) A group can have more that one identity element.
   (ii) The null set can be considered to be a group.
   (iii) There may be groups in which the cancellation law fails.
   (iv) Every set of numbers which is group under addition is also a group under multiplication and vice versa.
   (v) The set R of all real numbers is a group with respect to subtraction.
   (vi) The set of all nonzero integers is a group with respect to division.
   (vii) To each element of a group, there does not correspond an inverse element.
   (viii) To each element of a group, there corresponds only one inverse element.
   (ix) To each element of a group, there correspond more that one inverse elements.

2. Show that in a group G

(i) the identity element is unique

(ii) the inverse of each element is unique.

3. Which of the following sets are groups and why?

(i) The set of all positive rational numbers under multiplication.

(ii) The set of all complex numbers z such that $|z| = 1$, under multiplication defined for complex numbers.

(iii) The set Z of all integers under binary operation o defined by

$$a \, o \, b = a - b \qquad \text{for all } a, b \in Z.$$

(iv) The set Q' of all irrational numbers under multiplication.

(v) $R^+ = \{ x \in R : x > 0 \}$ under multiplication

(vi) $R^- = \{ x \in R : x < 0 \}$ under multiplication

(vii) $E = \{ e^x : x \in R \}$ under multiplication

4. Show that the set $\{\overline{1}, \overline{2}, \overline{4}, \overline{5}, \overline{7}, \overline{8}\}$ under multiplication modulo 9 is a group.

5. Is (Z, o) a group? where o is defined by $a \, o \, b = 0$ for all $a, b \in Z$.

6. Show that the matrices:

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, A = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, B = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, C = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$$

form a group under matrix multiplication.

7. Prove that the set of complex-valued functions I, f, g and h defined on $C \setminus \{0\}$ of nonzero complex numbers by:

$$I(z) = z, \ f(z) = -z, \ g(z) = 1/z, \ h(z) = -1/z, \ z \in C \setminus \{0\}$$

forms a group under composition of functions $(g o f)(z) = g(f(z))$.

8. Show that the set

$$G = \{ 2^k : k = 0, \pm 1, \pm 2, \cdots \}$$

is a group under multiplication.

9. Show that if a group G is such that $x \cdot x = e$, for all $x \in G$, where e is the element of G, then G is an abelian group.

10. If a group G has three elements, show that it is abelian.

11. If every element of a group G is its own inverse, show that G is abelian.

12. Prove that if every non-identity element of a group G is of order 2, then G is abelian.

13. In a group G, let a, b and ab all have order 2. Show that $ab = ba$.

14. Show that a group G is abelian if and only if $(ab)^2 = a^2b^2$ for all $a, b \in G$.

15. Suppose that a group G has only one element a of order 2. Show that, for all $x \in G$, $ax = xa$.

16. Let G be a group such that $(ab)^n = a^n b^n$ for three consecutive natural numbers n and all a, b in G. Show that G is abelian.

17. If G is an abelian group, show that

$$(ab)^n = a^n b^n \qquad \text{for all } a, b \in G.$$

18. Show that the set $GL_2(R)$ of all 2×2 nonsingular matrices over R is a group under the usual multiplication of matrices.

(This group is called the **general linear group of degree 2**).

SUBGROUPS

(2.12) Definition. Let $(G, .)$ be a group and H be a nonempty subset of G. If H is itself a group with the binary operation of G restricted to H, then H is called a **subgroup** of G.

Example 15. $(Z, +)$ is a subgroup of $(Q, +)$ and $(Q, +)$ is a subgroup of $(R, +)$.

Example 16. The set of cube roots of unity forms a subgroup of $C \setminus \{ 0 \}$, where $C \setminus \{ 0 \}$ is the group of nonzero complex numbers under multiplication of complex numbers.

Example 17. Every group G has at least two subgroups namely G itself and the identity group $\{ e \}$. These are called **trivial** subgroups. Any other subgroup of G is called a **nontrivial** subgroup of G.

The following theorem establishes an easy criterion for determining whether or not a subset H of a group G is a subgroup of G.

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

Proof. Suppose that H is a subgroup of G. Then for all $a, b \in H$, $a, b^{-1} \in H$. Hence $ab^{-1} \in H$ by the closure law in H.

Conversely, suppose that for all $a, b \in H$, $ab^{-1} \in H$.