Algebra

Group—A non empty set elements, G is said to form a group if in G, there is defined a binary operator called product such that

(a) $a, b \in G \Rightarrow a * b \in G$ (closed)

(b) $a, b, c \in G \Rightarrow a * (b * c) = (a * b) * c$ (Associative)

(c) There exist $e \in G : a * e = e * a = a$, for all $a \in G$. (Existence of identity)

(d) For every $a \in G$, there exist $a^{-1} \in G$.

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

(Existence of inverse)

Abelian Group—A group G is Abelian (commutative) if for every $a, b \in G, a * b = b * a$.

If G is a non empty set and * is any binary operation defined on G, then $(G, *)$ is—

(a) Quasi-group—$a, b \in G \Rightarrow a * b \in G$.

(b) Semi-group—$a, b \in G \Rightarrow a * b \in$ and $(a * b) * c = a * (b * c), a, b, c \in G$.

(c) Monoid—$a, b \in G \Rightarrow a \cdot b \in G, (a * b) * c = a * (b * c), a, b, c \in G$ and there exist $e \in G$ identity : $a * e = e * a = a$.

i.e., semi-group is a quasi-group with associativity.

Monoid is a semi-group with identity. Group is a monoid with inverse. Abelian group is a group with commutativity.

Order of group—The number of elements in G, o (G).

Cyclic group—$a^i \in G$ and o $(G) = n$:

$$a^i = \begin{cases} a^0 = a^n = e, \; i = 0, n \\ a^i = i < n \\ a^{i-n} = i > n \end{cases}$$

Lemma—(a) The identity element of G is unique.

(b) $\forall a \in G$, its inverse a^{-1} is unique

(c) $a \in G \Rightarrow (a^{-1}) = a$

(d) $a, b \in G \Rightarrow (a * b)^{-1} = b^{-1} * a^{-1}$

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

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

Sub-group—A non empty subset H of G, is a sub-group of group G, if H is a group on the operator of G.

Right and Left Co-sets—H is a sub-group of group G, $a \in G$, then

Right co-set of H in G is $Ha = \{ha : h \in H\}$

Left co-set of H in G is $aH = \{ah : h \in H\}$

Index of Sub-group—If H is a sub-group of G, the index of H in G is the number of distinct right co-set of H in G.

Order (period) of Element—If G is a group $a \in G$, the order of a (period of a), is the least positive integer $m : a^m = e$, o $(a) = m$.

Product Sub-groups—$HK = \{x \in G : x = hk; h \in H, K \in K\}$ H, G are sub-group of G.

Lemma—A non empty subset H of a group G is a subgroup of G iff

(a) $a, b \in H \Rightarrow ab \in H$

(b) $a \in H \Rightarrow a^{-1} \in H$.

Lemma—If H is a non empty finite subset of G and H is closed, then H is a subgroup of G.

Lemma—$\forall a \in G, Ha = \{x \in G : a \equiv x \bmod H\}$

Lemma—There is one to one corresponding between two right cosets of H in G.

Normal Subgroups and Quotient Groups

Normal Subgroup—A subgroup N of G is normal subgroup is $\forall g \in G$ and $n \in N, gng^{-1} \in N$.

Quotient Group—If G is a group, N is normal subgroup of G, then group G/N is called quotient (factor) group.

Lemma—N is a normal subgroup of G iff $g N g^{-1} = N$, for $\forall g \in G$.

Lemma—N is a normal subgroup of G iff $Na = aN, \forall a \in G$.

Lemma—N is a normal subgroup of G iff $(Na)(Nb) = Nab$.

Lemma —N is a normal subgroup of G, G is finite group then $o\,(G/N) = o\,(G)/o\,(N)$.

Homomorphism

Homorphism—A mapping ϕ from group $\bar{G}$ into a group G is said to be a homomorphism if $\forall a, b \in G$, $\phi(ab) = \phi(a)\phi(b)$.

Kernel—If ϕ is a homomorphism of G into $\bar{G}$, then Kernel of ϕ, $k\phi$ is defined by $k\phi = \{x \in G : \phi(x) = \bar{e} \cdot \bar{e}$ an identity element in $\bar{G}\}$.

Isomorphism—A homomorphism ϕ from G into $\bar{G}$ is an isomorphism if ϕ is one-to-one.

Isomorphic—Two groups G and G* are isomorphic if there is an isomorphism of G into G* ($G = G^*$).

Lemma—N is a normal subgroup of G; $\phi : G \to G/N : \phi(x) = Nx, \forall x \in G$. Then ϕ is homomorphism of G on to G/N.

Lemma—If ϕ is homomorphism of G into $\bar{G}$, then

(a) $\phi(e) = \bar{e}$, the identity element of $\bar{G}$.
(b) $\phi(x^{-1}) = \phi(x)^{-1}, \forall x \in G$.

Lemma—If ϕ is homomorphism of G into $\bar{G}$ with Kernel K, then K is a normal subgroup of G.

Lemma—If ϕ is a homomorphism of G into $\bar{G}$ with Kernel k, then the set of all inverse images of $\bar{g} \in \bar{G}$ under ϕ is given by kx, where x is any particular inverse image of $\bar{g} \in \bar{G}$.

Lemma—A homomorphism ϕ of G into $\bar{G}$ with Kernel $k\phi$ is isomorphism of G into $\bar{G}$ iff $k\phi = (e)$.

Some Important Theorems

1. If ϕ is a homomorphism of G onto $\bar{G}$ with Kernel k, then $G/K = \bar{G}$.

2. **Cauchy's theorem for Abelian group**—If G is a finite Abelian group and any prime number $P/o(G)$ there exist $a \neq e \in G'$. $oP = e$.

3. **Sylow's theorem for Abelian group**—If G is a finite Abelian group and P any prime such that $P^2/o(G)$, $P^{\alpha+1}/o(G)$, the G has a subgroup of order P^α.

4. If G is Abelian group of order $o(G)$ and $P^\propto | o(G)$, $P^{\alpha+1}/o(G)$, then there is unique subgroup of G of order P^α.

5. If ϕ is homomorphism of G into $\bar{G}$, with Kernel k, and $\bar{N}$ is a normal subgroup of $\bar{G}$, $N = \{x \in G \mid \phi(x) = \bar{N}\}$

Then $G/N \approx \bar{G}|\bar{N}$ and $G|N = (G|K)(N|K)$

Automorphism—A homomorphism of a group G onto itself.

Theorems—1. If G is a group, A (G), a set of automorphism is also a group.

2. Let G be a group and ϕ an automorphism of G.

If $a \in G$ and $o(a) > 0$, then $o(\phi(a)) = o(a)$.

Sylowis theorem—1. If P is a prime number and $P^2|o(G)$, then G has a subgroup of order P^α.

2. If $P^m|o(G)$, $P^{m+1}|o(G)$, then G is a subgroup of order P^m.

3. If A and B are finite subgroup of G, then

$$o(AxB) = \frac{o(A)\,o(B)}{o(A \cap xBx^{-1})}$$

Direct Product

Internal direct product—If G is a group and $N, N_2, \ldots N_n$ are normal subgroup of G :

(a) $G = N_1, N_2, \ldots N_n$

(b) $g \in G$, $g = m_1 m_2 \ldots m_n$, $m_i \in N_i$ in a unique way, then G is internal direct product of $N_1 N_2, \ldots N_n$.

1. If G is internal direct product of $N_1, \ldots N_n$, then for $i \neq j$, $N_i \cap N_j = (e)$ and $a \in N_i$, $b \in N_j$ then $ab = ba$.

2. If G is internal direct product of $N_1, \ldots N_n$ and if $T = N_1 \times N_2 \times \ldots \times N_n$, then G and T are isomorphic.

Finite Abelian Group

Invariants of G—If G is an Abelian group of order P^n, P a prime $G = A_1 \times A_2 \times \ldots \times A_n, \forall A_j$ is cyclic of order P^{ni}, $n_i \leq n_{i+1}$, then $n_{11} \ldots n_{1\propto}$ are invariant of G.

Theorem—The number of non-isomorphic Abelian groups of order P^n are equals to the number of partitions of n.

Rings

Associative Ring—A non empty set R is said to be a ring if in R there are defined two operators + and. respectively : $a, b, c \in R$.

(a) $a + b \in R$
(b) $a + b = b + a$
(c) $(a + b) + c = a + (b + c)$
(d) $o \in R : a + o = a, \forall a \in R$
Abelian group with o on addition

(e) $-a \in R : a + (-a) = 0$ (closed under)
(f) $a \cdot b \in R$ (Associative under)
(g) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (Left distribution)
(h) $(a + b) \cdot c = a \cdot c + b \cdot c$ (Right distribution)
$c \cdot (a + b) = c \cdot a + c \cdot b$

Ring with Unity—$1 \in R : a \cdot 1 = 1 \cdot a = a\ \forall \cdot a \in R$

Commutative Ring—If $a \cdot b = b \cdot a, \forall a, b \in R$

Zero Divisor—R is commutative ring, $a \neq a \in R$, is zero divisor if there exist $b \in R, b \neq 0 : ab = 0$.

Integral Domain—A commutative ring is an integral domain if it has no zero divisor.

Division Ring (skew field)—A ring is called a division ring if its non-zero elements from a group under multiplication.

Characteristic Zero—An integral domain D is of characteristic zero if $ma = 0, a \neq 0, \in P, \Rightarrow m = 0$.

Finite Characteristic—An integral domain D is a finite characteristic if there exist a positive integer $m : ma = 0, \forall a \in D$.

Null (zero) ring—$\{0\}, + :) : 0 + 0 = 0$ and $0 \cdot 0 = 0$

Field—A field is a commutative division ring.

Homomorphism

Homomorphism—A mapping ϕ from ring R into ring R' is homomorphism if $\forall a, b \in R$.

(a) $\phi(a + b) = \phi(a) + \phi(b)$

(b) $\phi(ab) = \phi(a)\, \phi(b)$

Kernel—If ϕ is a homomorphism of R into R', then the Kernel of ϕ, I (ϕ) is the set of all $a \in R : \phi(a) = 0$, the zero element of R.

Zero Homomorphism—$\phi(a) = 0$ for all $a \in R$ and I (ϕ) = R.

Isomorphism—A homomorphism of R into R' if it is also one-to-one mapping.

Isomorphic—A and B are isomorphic, if there is a isomorphism from one onto another.

Some Important Theorems

1. If ϕ is homomorphism of R into R', then (i) $\phi(a) = 0$ (ii) $\phi(-a) = -\phi(a), \forall a \in R$.

2. If ϕ is homomorphism of R into R' with Kernel I (ϕ), then

(a) I (ϕ) is a subgroup of R under addition

(b) If $a \in I(\phi)$ and $r \in R$, then both $ar \in R$ and $ra \in R$.

3. The homomorphism ϕ of R into R' is an isomorphism iff I (ϕ) = 0.

4. If integral domain is of finite characteristic then its characteristic is a prime number.

Ideals and Quotient Rings

Ideal—A non-empty subset $\cup$ of R is ideal if

(a) U is a subgroup under addition

(b) $\forall u \in U$ and $r \in R$, $ur, ru \in U$.

Quotient Ring—If U is an ideal of ring R, then R/U is a quotient ring and is homomorphic image of R.

Maximal Ideal—An ideal $M \neq R$ in a ring R is maximal ideal of R whenever U is an ideal of $R : M \subset U \subset R$ then either R = U or M = U.

Some Important Theorems

1. If R is a commutative ring with unit element and M is an ideal of R then M is maximum ideal of R iff R/M is a field.

2. If R is a commutative ring with unit element whose only ideals are (0) and R, itself, then R is a field.

Euclidean Ring

Euclidean Ring—An integral domain R is an Euclidean ring if for every $a \neq 0 \in R$ there is defined a non-negative integer $d/(a)$.

(a) $\forall a, b \in R, a \neq 0, b \neq 0 \Rightarrow d(a) \leq d(ab)$

(b) For any $a, b \in R, a \neq 0, b \neq 0$ there exist $t, r \in R : a = tb + r$ where either $r = 0$ or $d(r) < d(b)$.

Principal Ideal—An integral domain R with unit element is a principal ideal ring if every ideal $A \in R$ is of the form $A = (a) = \{xa | x \in R\}$ for some $a \in R$.

Unit (elements)—$a \in R$ is unit element in R if there exist $b \leq R : ab = 1$.

Unit—If R is commutative ring with unit element.

Prime Element—In Euclidean ring R a non unit π is said to be prime element of R if when ever $\pi = ab$, $a, b \in R$, then one of a or b is a unit in R.

Relatively Prime—In the Euclidean ring R a, $b \in$ R are relatively prime if their greatest common divisor is a unit of R.

Some Important Theorems

1. If R is an Euclidean ring and A an ideal of R. Then there exist an element $a_0 \in$ R : A consists exactly of all $a_0 x$ as range over R.

2. A Euclidean ring possesses a unit element.

3. If R is an Euclidean ring. Then any two elements a, $b \in$ R have a greatest common divisor d. Moreover $d = \lambda a + ub$ for some λ, $u \in$ R.

4. If R is an integral domain with unit element and suppose for a, $b \in$ R, a/b and b/a are true. Then $a = ub$, where u is a unit in R.

5. If R is an Euclidean ring and a, $b \in$ R. If $b \neq 0$ is not a unit in R, then $\alpha(a) < d(ab)$

6. If R is an Euclidean ring, then every element in R is either a unit in R or can be written as the product of a finite number of prime elements of R.

7. If R is an Euclidean ring. Suppose for a, b, $c \in$ R, a/bc but $(a, b) = 1$, then a/c.

8. If π is a prime element in the Euclidean ring R and π/ab, where a, $b \in$ R, then π divides atleast one of a or b.

9. If π is a prime element in the Euclidean ring R and $\pi/a_1, a_2, \dots a_n$, then π divides atleast one $a_1, a_2, \dots a_n$.

10. **Unique factorization theorem**—If R is an Euclidean ring and $a \neq 0$ a non unit in R suppose $a = \pi, \pi_2 \dots \pi_n = \pi'_1 \pi'_2 \dots \pi'_n$ where π, and π'_1 are prime elements in R. Then $n = m$ and each π_1, $i = 1, 2, \dots n$ is an associate of same π'_j, $j = 1 \dots n$ and conversely each π'_j is associated with same π_j.

11. Every non–zero element in a Euclidean ring R can be uniquely written as a product of prime elements or is a unit in R.

12. The ideal A = (a_0) is a maximal ideal of the Euclidean ring R iff a_0 is a prime element of R.

Polynomial Rings Over Commutative Rings—F $(x_n \dots x_n)$: The field of aration functions in $x_1 \dots, x_n$ over F.

Unique factorization domain—An integral domain R, with unit element is a unique factorization domain if—

(a) Any non-zero element in R is either a unit or can be written as the product of a finite number of irreduciable elements of R.

(b) The decomposition in part (a) is unique upto the order and associates of the irreduciable elements.

Some Important Theorems

1. If R is an integral domain, then so in R $[x]$.

2. If R is an integral domain, then so is R $[x_1 \dots x_n]$

3. If R is unique factorization domain and if a, $b \in$ R, then a and b have the greatest common divisor $(a, b) \in$ R. Moreover if a, b are relatively prime $(a, b) = 1$, whenever $a|bc$ then a/c.

4. If $a \in$ R is an irreducible element and $a|bc$ then $a|b$ or $a|c$.

5. If R is a unique factorization domain, then the product of two primitive polynomials in R $[x]$ is again a primitive polynomial in R $[x]$.

6. If R is a unique factorization domain, and if $f(x)$, $g(x) \in$ R $[x]$, then $c(fg) = c(g) = c(f)\,c(g)$.

7. If $f(x) \in$ R (x) is both primitive and irreducible as an element of R $[x]$, then it is irreducible as an element of F $[x]$. Conversely, if the primitive element $f(x) \in$ R $[x]$ is irreducible as an element of F $[x]$, it is also irreducible as an element of R $[x]$.

8. If R is a unique of factorization domain and if P (x) is a primitive polynomial in R $[x]$, then it can be factored in a unique way as the product of irreducible elements in R $[x]$.

9. If R is a unique factorization domain, then so is R $[x]$.

10. If R is a unique factorization domain the n so is R $[x_1 \dots, x_n]$.

11. If F is a field then F $[x_1, \dots, x_n]$ is a unique factorization domain.

Fields

Fields (F) is a non empty set, F is a field,

(a) (F, +) is an Abelian group

(b) (F, ·) is semi-Abelian *i.e.*, (F – {0} ·) is Abelian group

(c) Multiplication is distributive over addition.

$$a(b + c) = ab + ac$$
$$(b + c)a = bc + ca$$

Extension—K, F are fields K is an extension of F if $F \subset K \Leftrightarrow F$ is a subfield of K.

Degree of Extension—The degree of extension K over F, [K', F] is the dimension of K as a vector space of F.

Algebraic Over F—K is an extension of F, $a \in K$ is algebraic over F, if there exist elements $\alpha_0, \alpha_1, \ldots \alpha_n \in F$, not all zero, such that $\alpha_0 a^n + \alpha_1 \alpha^{n-1} + \ldots + \alpha_n = 0$.

Sub-field Obtained by Adjoining *a* to F—If K is an extension of F, $a \in K$, then F (a) is the smallest subfield containing both F and a.

Algebraic of Degree *n*—The element $a \in F$ is algebraic of degree n over F if it satisfies a non-zero polynomial over F of degree n but no, non-zero polynomial of lower degree.

Algebraic Extension—The extension K of F is called an algebraic extension of F if every element in K is algebraic over F.

Algebraic Number—A complex number is algebraic number if it is algebraic over the field of rational number.

Some Important Theorems

1. If L is a finite extension of K and if K is a finite extension of F, then L is a finite extension of F and [L : F] = [L : K] [K : F].

2. If L is a finite extension of F and K is a sub-field of L which contains F, then [K : F]\ [L : F].

3. The element $a \in k$ is a algebraic over F iff F (a) is a finite extension of F.

4. If $a \in k$ is algebraic of degree over F, then [F (a)' F] = n.

5. If $a, b \in k$ are algebraic over F then $a \pm b$, ab and a/b $(b \pm a)$ are all algebraic over F *i.e.*, the element in k which are algebraic over F from a subfield of K.

6. If $a, b \in k$ are algebraic over, F of degrees m and n respectively, then $a \pm b$, ab and a/b $(b \neq 0)$ are algebraic over F of degree at most mn.

7. If L is an algebraic extension of K and if K is an algebraic extension of F, then L is an algebraic extension of F.

Some Solved Examples

Example 1. If order of a group G is a prime number P, then G does not possess proper sub-group.

Solution : P is a prime number, its divisors are only ± 1 and ± P.

Let H be a sub-group of G, by Lagrange's theorem o (H) · o (G) is adivisor of P.

$\Rightarrow$ o (H) = P or 1

$\Rightarrow$ H = G or H = $\{e\}$

$\Rightarrow$ H is not a sub-group of G in either case.

Hence G does not possess proper subgroup.

Example 2. If G = {1, –1} is a group (G;), the order of 1 and –1 is ?

Solution : G have an identity element 1.

$$(1)^1 = 1$$

$\Rightarrow$ $0\,(1) = 1$

and $(-1)^2 = 1$

$\Rightarrow$ $0\,(-1) = 2$

Thus, order 1 is 1 and (–1) is 2.

Example 3. If a, b are any two elements of a group G and H is any sub-group of G, then $a \in Hb$ iff $Ha = Hb$.

Solution : $a \in Hb$

$\Rightarrow$ $ab^{-1} \in Hbb^{-1}$

$\Rightarrow$ $ab^{-1} \in He$

$\Rightarrow$ $ab^{-1} \in H$

$\Rightarrow$ $Hab^{-1} = H$

$\Rightarrow$ $Hab^{-1}b = Hb$ (Multiplying both sides an the left by b)

$\Rightarrow$ $Hae = Hb$ $(\because b^{-1}b = e)$

$\Rightarrow$ $Ha = Hb$ $(\because ae = a)$

Conversely let $Ha = Hb$. Since $a \in Ha$.

Therefore, $a \in Hb$.

Example 4. Prove that if R is a Euclidean ring and $b \in R$ is not a unit, then $\alpha\,(a) < \alpha\,(ab)$ $\forall a \in R$.

Solution : Let $a\,(\pm 0) \in R$, consider the ideal $U = (a)$. By the definition of Euclidean ring $\alpha\,(a) \leq \alpha\,(xa)$ for any non-zero $x \in R$.

Also $ab \in U$ and if $\alpha\,(a) = \alpha\,(a\alpha)$, then $(a) = (ab) = U$

i.e., every element of U is a multiple of ab. In particular, a is also a multiple of ab, *i.e*, $a = abx$ for some x in R

Now $a = abx$

$\Rightarrow$ $a \cdot 1 = abx$

$\Rightarrow$ $1 = bx$ $(\because a \neq 0)$

$\Rightarrow$ b is a unit in R.

Thus, if b is not unit in R, then $\alpha\,(a) \neq (ab)$ and hence we conclude that $\alpha\,(a) < \alpha\,(ab)$

Example 5. A non-empty subset H of a group G is a sub-group iff $a \in H, b \in H \Rightarrow aob^{-1} \in H$ where b^{-1} is the inverse of b in G.

Solution : Suppose H is a subgroup of G and $a \in H, b \in H$.

Now each element of H must possess inverse because H itself is a group (assumption) $b \in H \Rightarrow b^{-1} \in H$.

Also H is closed under the composition (o say) in G, therefore

$$a \in H, b^{-1} \in H \Rightarrow aob^{-1} \in H$$

Let $a \in H, b \in H \Rightarrow aob^{-1} \in H$, then to show that H is a subgroup it has to satisfy group postulate.

(i) **Closure Property**—Let $a, b \in H$, then $b \in H \Rightarrow b^{-1} \in H$.

$\therefore$ By the given condition $a \in H, b^{-1} \in H \Rightarrow a_0 (b^{-1})^{-1} \in H \Rightarrow aob \in H$.

Thus H is closed with respect to the composition in G.

(ii) **Associatively**—Since the elements of H are also the elements of G the composition is associative in H.

(iii) **Existence of Identity**—Since $a \in H, a^{-1} \in H \Rightarrow aoa^{-1} \in H$.

$\Rightarrow$ $e \in H$, identity element $e \in H$.

(iv) **Existence of Inverse**—Let $a \in H$, then $e \in H, a \in H \Rightarrow eoa^{-1} \in H$.

$\Rightarrow$ $a^{-1} \in H$ each element of H possesses inverse

Hence, H itself is a group for the composition o in group G.

Example 6. If $a^2 = a$, then $a = e$, a being an element of a group G.

Solution :

$$\begin{aligned} a^2 &= a \\ \Rightarrow \quad a \cdot a &= a \\ \Rightarrow \quad (a \cdot a)\, a^{-1} &= a \cdot a^{-1} \\ \Rightarrow \quad a\,(a \cdot a^{-1}) &= e \\ \Rightarrow \quad a \cdot e &= e \\ \Rightarrow \quad a &= e \end{aligned}$$

Example 7. If G is a group of even order, then it has an element $a \neq e : a^2 = e$, e being identity element.

Solution : $a \in G \Rightarrow \exists a^{-1} \in G$ and $e = e^{-1}$, e an identity element.

Since o (G) is even, there exist at least one element $a \in G$, which is its own inverse.

$$\begin{aligned} i.e., \quad a &= a^{-1}, a \neq e \\ \Rightarrow \quad a \cdot a &= a^{-1} \cdot a = e \\ \Rightarrow \quad a^2 &= e \end{aligned}$$

Example 8. In the additive group of integers, the order of every element a ($\neq 0$) is infinite.

Solution : For additive group of integers, 0 is an identity element and

$$0\,(0) = 1 \text{ as } 0' = 0$$

There exist no positive integer n which gives $na = 0$ for ($a \neq 0$)

Hence, order of every element except 0 is infinite.

Example 9. A group (G, *) is commutative iff $(a * b)^{-1} = a^{-1} * b^{-1}, \forall a, b \in G$.

Solution : (G, *) is commutative, $a^{-1}, b^{-1} \in G$

$$\Rightarrow \quad a^{-1} * b^{-1} = b^{-1} * a^{-1} \quad \ldots(1)$$

$$\text{and} \quad (a * b)^{-1} = b^{-1} * a^{-1} \quad \ldots(2)$$

By (1) and (2)

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

Conversely let

$$(a * b)^{-1} = a^{-1} * b^{-1}, \forall a, b \in G \quad \ldots(3)$$

By (2) and (3), we have

$$a^{-1} * b^{-1} = b^{-1} * a^{-1}, \forall a, b \in G$$

$\Rightarrow$ * is commutative

$\Rightarrow$ The group (G, *) is Abelian.

Example 10. Is the set of integer z with binary operation $a \cdot b = a - b, \forall a, b \in z$ a group ?

Solution : (a) Closure : $a - b \in z$ for $\forall a, b \in z$

(b) Associatively : $a, b, c \in z$

$$(a - b) - c \neq a - (b - c)$$

$\therefore$ Set of integer z is not a group on defined operation.

Example 11. $H \subseteq K$ be two subgroup of a finite group G, then $[G : H] = [G : K]\,[K : H]$.

Solution : $H \subseteq K$ are subgroups of a group G.

$\therefore$ H is also a subgroup of K

Since H is a subgroup of finite group G

By Lagrange's theorem

$$[G : H] = \frac{o\,(G)}{o\,(H)} = \frac{o\,(G)}{o\,(H)} = \frac{o\,(G)}{o\,(K)} \cdot \frac{o\,(K)}{o\,(H)} = [G : K]\,[K : H]$$

Example 12. If H is a subgroup of group G. For $x \in G$, $xHx^{-1} = \{xhx^{-1} : h \in H\}$ is a subgroup of G.

Solution : Let xh_1x^{-1}, xh_2x^{-1} are two elements of xhx^{-1} then $h_1, h_2 \in$ H.

$$\begin{aligned}(xh_1x^{-1})(xh_2x^{-1})^{-1} &= xh_1x^{-1}x(xh_2)^{-1}\\ &= xh_1(xh_2)^{-1}\\ &= xh_1h_2^{-1}x^{-1}\\ &= x(h_1h_2^{-1})x^{-1}\end{aligned}$$

where $h_1h_2^{-1} \in$ H

$\Rightarrow x(h_1h_2)x^{-1} \in x\text{H}x^{-1}$ is a subgroup of G.

Example 13. If a, b belongs to a ring R, and $(a+b)^2 = a^2 + 2ab + b^2$, then R is a commutative ring.

Solution :
$$\begin{aligned}(a+b)^2 &= (a+b)\cdot(a+b)\\ &= a\cdot(a+b)+b.(a+b)\\ &= a\cdot a + a\cdot b + b\cdot a + b\cdot b\\ &= a^2 + ab + ba + b^2 \quad \ldots(1)\end{aligned}$$

Given $\quad (a+b)^2 = a^2 + 2ab + b^2 \quad \ldots(2)$

By (1) and (2), we conclude

$$ab + ba = 2ab$$

$$\Rightarrow \quad ba = ab$$

i.e., R is a commutative ring.

Example 14. If a non zero element x of a ring R with unity has a multiplicative inverse, then x can not be a zero divisor.

Solution : Given $x \neq 0$ and x^{-1} exists. Also let $y \neq 0$ but $xy = 0$ so

$xy = 0 \Rightarrow x^{-1}(xy) = x^{-1}(0) \Rightarrow (x^{-1}x)y = 0 \Rightarrow 1\cdot y = 0 \Rightarrow y = 0$

Thus, $x \neq 0$, $xy = 0 \Rightarrow y = 0$, which is against our assumptions that $y = 0$.

Hence x can not be a zero divisor.

Example 15. If a, b are any elements of the ring (R, +;) m, n are integers, then

$$(na)(mb) = (nm)(ab)$$

Solution :
$$\begin{aligned}a(mb) &= a(b + b + \ldots m \text{ times})\\ &= ab + ab + \ldots m \text{ times}\\ &= m(ab)\\ (na)(mb) &= (a + a + \ldots n \text{ times})(mb)\\ &= amb + amb + \ldots n \text{ times}\\ &= m(ab) + m(ab) + \ldots n \text{ times}\\ &= n\, m(ab))\\ &= (nm)(ab)\end{aligned}$$

Example 16. The set of integer is a subring of the ring of rational numbers.

Solution : z is a set of integers, Q is a set of rational numbers.

$z \subset$ Q and $a, b \in z \Rightarrow a - b \in z$ and $ab \in z$

$\therefore$ z is a subring of Q.

Example 17. $s = \{\pm ma : m = 0, , 2, \ldots$ and 'a' any fixed integer$\}$ then s is a subring of (1, + ;) the ring of integers over addition and multiplication.

Solution : Let $ra, sa \in$ S and $s, r \in$ I

$ra - sa = (r - s)a \in s$ as $(r - s) \in$ I

$(ra)(sa) = (rsa)a \in s$ as $(rs)a \in$ I

$\therefore$ s is a subring of I.

Example 18. Any group of prime order can have no proper subgroup.

Solution : Let o (G) = P, P is a prime number. Let H be a subgroup of G and let o (H) = m,

By Lagrange's theorem o (H)|o (G) $\Rightarrow m|p$

$\because$ P is a prime number.

$\therefore$ $m = 1$ or p. If $m = 1 \Rightarrow o$(H) = 1 $\Rightarrow$ H $\{e\}$, if $m = p \Rightarrow o$ (H) = o (G)

$\Rightarrow$ H = G.

$\therefore$ Either H = $\{e\}$ or H = G, *i.e.*, H is not a proper subgroup of G.

Hence, any group of prime order can have no proper subgroup.

Example 19. Two right cosets Ha and Hb are distinct iff two left cosets a^{-1} H and b^{-1} H are distinct.

Solution : Let a^{-1} H = b^{-1} H, then a^{-1} H = b^{-1} H $\Leftrightarrow (b^{-1})^{-1}a^{-1} \in$ H

$\Leftrightarrow ba^{-1} \in \text{H} \Leftrightarrow (ba^{-1})^{-1} \in \text{H} \Leftrightarrow (a^{-1})^{-1}b^{-1} \in$ H

$\Leftrightarrow ab^{-1} \in \text{H} \Leftrightarrow \text{H}a = \text{H}b$

$\because$ Ha = Hb $\Leftrightarrow ab^{-1} \in$ H, which is a contraction

Hence, H$a \neq$ H$b \Rightarrow a^{-1}\text{H} \neq b^{-1}\text{H}$

Similarly $a^{-1}\text{H} \neq b^{-1}\text{H} \Rightarrow \text{H}a \neq \text{H}b$

$\therefore$ H$a \neq$ H$b \Leftrightarrow a^{-1}\text{H} \neq b^{-1}\text{H}$

Example 20. Prove that in a field :

(a) $\dfrac{a}{b} - \dfrac{c}{d} = \dfrac{ad - bc}{bd}$

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

(c) $\dfrac{(-a)}{(-b)} = \dfrac{a}{b}$

Solution : (a) $\dfrac{a}{b} - \dfrac{c}{d} = ab^{-1} - cd^{-1}$

$= b^{-1}a - cd^{-1}$ ($\because$ commutative law holds)

$= b^{-1}\, add^{-1} - b^{-1}\, bcd^{-1} \qquad (\because b^{-1}b = 1\; dd^{-1})$

$= (b^{-1}ad - b^{-1}bc)\, d^{-1}$

($\because$ right distributive law holds)

$= b^{-1}\,(ad - bc)\, d^{-1}$

($\because$ left distributive law holds)

$= \dfrac{ad - bc}{bd}$

(b) Let $(-a)^{-1} = x$, $\Rightarrow (-a)\,x = 1$, (unit element of the field)

$\Rightarrow ax = -1, \Rightarrow x = a^{-1}\,(-1)$

(a^{-1} is the multiplicative inverse of a)

$\Rightarrow x = -(a^{-1}\cdot 1) = -(a^{-1}) \qquad \because a^{-1}\cdot 1 = a^{-1}$

$\Rightarrow (-a)^{-1} = -(a^{-1})$

(c) $\left(\dfrac{-a}{-b}\right) = (-a)\cdot(-b)^{-1} = (-a)\,[(-b)^{-1}]$

$= ab^{-1}$

$= \dfrac{a}{b}$

Example 21. If I is an additive group of integers and E the additive group of even integers with zero, then the map $f : \mathrm{I} \to \mathrm{E}$ given by $f(x) = 2x$, where $x \in \mathrm{I}$, is an isomorphism.

Solution : Let $m, n \in \mathrm{I}$, then $f(m) = f(n)$

$\Rightarrow \quad 2m = 2n$

$\Rightarrow \quad m = n$

i.e., mapping f is one-one.

Let $z = \mathrm{E}, \exists\, x \in \mathrm{I} : x = \dfrac{z}{2}$, z even

i.e., mapping f is onto

Again $f(m + n) = 2\,(m + n)$

$= 2m + 2n$

$= f(m) + f(n)$

$\therefore$ The mapping f preserves the group composition and hence the mapping f is an isomorphism.

Example 22. Again G is Abelian if $b^{-1}a^{-1}ba = e\,\forall a, b \in \mathrm{G}$.

Solution : We have

$$(ab)^{-1} = b^{-1}a^{-1}, \forall a, b \in \mathrm{G} \qquad \ldots(1)$$

If e is an identity element, then

$(ab)^{-1}\,(ab) = e$

$\Rightarrow \quad b^{-1}a^{-1}ab = e \qquad \ldots(2)$

given $\quad b^{-1}a^{-1}ba = e \qquad \ldots(3)$

By (2) and (3)

$b^{-1}a^{-1}ab = b^{-1}a^{-1}ba$

$\Rightarrow \quad ab = ba$

$\Rightarrow$ G is Abelian.

Example 23. Prove that if G is a group and for $a, b \in \mathrm{G}$

$(a\cdot b)^2 = a^2\cdot b^2$ iff G be Abelian.

Solution : Let

$(a\cdot b)^2 = a^2\cdot b^2$

$\Rightarrow \quad (a\cdot b)\cdot(a\cdot b) = (a\cdot a)\,(b\cdot b)$

$\Rightarrow \quad a\cdot(b\cdot a)\cdot b = a\,(a\cdot b)\cdot b$

(By associative law)

$\Rightarrow \quad a\cdot(b\cdot a) = a\cdot(a\cdot b)$

(By right cancellation law)

$\Rightarrow \quad b\cdot a = a\cdot b$

(By left cancellation law)

$\Rightarrow$ G is Abelian.

Conversely

G is Abelian

$\Rightarrow \quad b\cdot a = a\cdot b, \forall a, b \in \mathrm{G}$

$\Rightarrow \quad a\cdot(b\cdot a) = a\cdot(ab)$

(Multiplying both sides on the left by a)

$\Rightarrow \quad (ab)\cdot(ab) = (a\cdot a)\,(b\cdot b)$

(By associative law)

$\Rightarrow \quad (a\cdot b)^2 = a^2\cdot b^2$

Hence, $(a\cdot b)^2 = a^2\cdot b^2\ \forall\, a, b \in \mathrm{G}$ iff G is Abelian.

Example 24. Prove that the centre of a group is always a normal subgroup of the group.

Proof : Let z be the centre of G so that

$z = \{z \in \mathrm{G} : zx = xz\ \forall x \in \mathrm{G}\}$

Let $z_1, z_2 \in z$ then, $z_1, z_2 \in z$

$\Rightarrow \quad z_1x = xz_1$

and $\quad z_2x = xz_2 \forall x \in \mathrm{G}$

Now $\quad z_2x = xz_2 \forall x \in \mathrm{G}$

$\Rightarrow \quad z_2^{-1}z_2xz_2^{-1} = z_2^{-1}xz_2z_2^{-1}\ \forall x \in \mathrm{G}$

$\Rightarrow \quad xz_2^{-1} = z_2^{-1}\,x\forall\ x \in \mathrm{G}$

But $\quad (z_1z_2^{-1})\,x = z_2\,(z_2^{-1}x)$

(Associativity)

$= z_1\,(xz_2^{-1})$

$(\because z_2^{-1}x = xz_2^{-1})$

$= (z_1x)\,z_2^{-1}$ (Associativity)

$= (xz_1)\,z_2^{-1} \quad (\because z_1x = xz_1)$

$= x\,(z_1z_2^{-1})\ \forall x \in \mathrm{G}$

$\therefore\ z_1z_2^{-1} \in z$

Hence $z_1 \in z \cdot z_2 \in z \rightarrow z_1 z_2^{-1} \in z$ and therefore, z is a subgroup of G.

Again let $x \in$ G and $z \in z$, then

$$\begin{aligned} xzx^{-1} &= (xz)\,x^{-1} && \text{(Associativity)} \\ &= (zx)\,x^{-1} && (\because xz = zx) \\ &= z(xx^{-1}) && \text{(Associativity)} \\ &= ze = z \in z \end{aligned}$$

$\therefore\ xzx^{-1} \in z\ \forall x \in$ G and $z \in z$.

Hence, z is a normal in G. Thus, z is a normal subgroup of G.

Example 25. If a, b are any two elements of a group G and H is any subgroup of G, then

$$a \in Hb \text{ iff } Ha = Hb.$$

Solution : $a \in Hb$

$$\begin{aligned} \Rightarrow\quad ab^{-1} &\in Hbb^{-1} \\ \Rightarrow\quad ab^{-1} &\in He && (\because bb^{-1} = e) \\ \Rightarrow\quad ab^{-1} &\in H && (\because He = H) \\ \Rightarrow\quad Hab^{-1} &= H \\ \Rightarrow\quad Hab^{-1}b &= Hb \end{aligned}$$

(Multiplying both sides on the left by b)

$$\begin{aligned} \Rightarrow\quad Hae &= Hb && (\because b^{-1}b = e) \\ \Rightarrow\quad H\cdot a &= Hb && (\because ac = a) \end{aligned}$$

Conversely let Ha = Hb. Since a $\in$ Ha, therefore $a \in$ Hb.

Example 26. Prove that if H is any subgroup of G, then $H^{-1} = H$.

Solution : Let $h^{-1} \in H^{-1}$, then $h \in H$

Since H is a subgroup of G

$$h \in H \rightarrow h^{-1} \in H$$

(By inverse axiom)

Therefore, $h^{-1} \in H^{-1} \rightarrow h^{-1} \in H$

$$\therefore\quad H^{-1} \le H$$

Again $\quad h \in H \rightarrow h^{-1} \in H$

[$\because$ H itself is a group]

$$\begin{aligned} \Rightarrow\quad (h^{-1})^{-1} &\in H^{-1} \\ \Rightarrow\quad h &\in H^{-1} \\ H &\le H^{-1} \end{aligned}$$

Hence, from (1) and (2), we get

$$H^{-1} = H$$

Example 27. Prove that the normalizer of any element of a group is always a subgroup of the same.

Solution : Let G be any group and N (a) the normalizer of a ($\in$ G) in G. Let $x, y \in$ N (a), then

$$x \in N(a) \text{ and } z \in N(a)$$

$$\begin{aligned} \Rightarrow\quad ax &= xa \text{ and } ay = ya \\ \text{Now}\quad ay &= ya \rightarrow y^{-1}\, ayy^{-1} = y^{-1}yay^{-1} \\ \Rightarrow\quad y^{-1}a &= ay^{-1} \\ y^{-1}a &= ay^{-1} \end{aligned}$$

and therefore,

$$\begin{aligned} a\,(xy^{-1}) &= (ax)\,y^{-1} \\ &= (xa)\,y^{-1} \\ &= x\,(ay^{-1}) \\ x\,(y^{-1}a) &= (xy^{-1})\,a \end{aligned}$$

Which shows that $xy^{-1} \in$ N (a)

Hence, N (a) is a subgroup of G.

Example 28. Prove that if R is a Euclidean ring and $b \in$ R is not unit, then $d\,(a) < d\,(ab)\ \forall a \in$ R.

Solution : Let

$$a\,(\neq 0) \in R$$

Consider the ideal U = (a) by the definition of Euclidean ring $d\,(a) \le d\,(xa)$ for any non zero $x \in$ R

$$\begin{aligned} \text{Also}\quad ab &\in U \\ \text{and if}\quad d\,(a) &= d\,(ad) \\ \text{then}\quad (a) &= (ab) = U \end{aligned}$$

i.e., every element of U is a multiple of ab. In particular a is also a multiple of ab, *i.e.*,

$$a = abx \quad \text{for some } x \text{ in R}$$

Now $\quad a = abx$

$\Rightarrow a\cdot 1 = abx \rightarrow 1 = bx \qquad (\because\ a \neq 0)$

$\Rightarrow b$ is a unit in R

Thus if b is not unit in R then

$$d\,(a) \neq d\,(ab)$$

and hence we conclude that

$$d\,(a) < d\,(ab)$$

Example 29. Prove that the union of two subgroups is a subgroup iff one is contained in other. The union of two subgroups H_1 and H_2 is a subgroup if and only if one is contained in the other.

Solution : Let H_1 and H_2 are two subgroups of a group.

$$\begin{aligned} \text{(i) Let}\quad H_1 &\subseteq H_2 \\ \text{or}\quad H_2 &\subseteq H_2 \\ \text{then}\quad H_1 \cup H_2 &= H_2 \text{ or } H_1 \end{aligned}$$

$\therefore\ H_1 \cup H_2$ is a subgroup as $H_1 \cdot H_2$ are subgroups

(ii) Suppose $H_1 \cup H_2$ is a subgroup

If possible let us assume that H_1 is not contained in H or H_2 is not contained in H_1.

If H_1 is not contained in H_2

$\Rightarrow$ $a \in H_1$, and $a \notin H_2$ ...(1)

and H_2 is not contained in H_1

$\Rightarrow$ $b \notin H_2$ and $b \notin H_1$ ...(2)

$\therefore$ From (1) and (2), we get

$$a \in H_1 \cup H_2 \text{ and } b \in H_1 \cup H_2$$

As $H_1 \cup H_2$ is a subgroup so ab is also an element of $H_1 \cup H_2$

But $\quad ab \in H_1 \cup H_2$

$\Rightarrow \quad ab \in H_1$

or $\quad ab \in H_2$

Let $ab \in H_1$ then $a^{-1}\,ab \in H_1$ as $a \in H_1$ and H_1 is a subgroup. So that $a^{-1}\,ab = b \in H_1$, which is a contradiction of the assumption that

$$a \notin H_1$$

Hence either

$$H_1 \subseteq H_2$$

or $\quad H_2 \subseteq H_1$

Example 30. If G is a group such that $(ab)^m = a^m b^m$, for three consecutive integers $m \forall a, b \in G$ then prove that the group G is Abelian.

Solution : Let the three consecutive integral valves of m be $n-1$, n and $n+1$, then for

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

$$(ab)^{n-1} = a^{n-1}\,b^{n-1}$$

$$(ab)^n = a^n b^n$$

and $\quad (ab)^{n+1} = a^{n+1}\,b^{n+1}$

Now $\quad (ab)^{n+1} = (ab)^n\,(ab)$

$\Rightarrow \quad a^{n+1}\,b^{n+1} = a^n b^n\,(ab)$

$$(\because (ab)^m = a^m b^m)$$

For $m = n, n+1$

$\Rightarrow \quad a^n ab^n = a^n b^n ab$

$\Rightarrow \quad ab^n b = b^n ab$

(By left cancellation law)

$\Rightarrow \quad ab^n = b^n a$

(By right cancellation law)

$\Rightarrow \quad a^{n-1}\,(ab^n) = a^{n-1}\,(b^n a)$

Multiplying both sides

(by a^{n-1} on the left)

$\Rightarrow \quad (a^{n-1}a)b^n = a^{n-1}\,(b^{n-1}\,ba)$

(By associative law)

$\Rightarrow \quad a^n b^n = a^{n-1}\,b^{n-1}\,(ba)$

$\Rightarrow \quad (ab)^n = (ab)^{n-1}\,(ba)$

$$(\because (ab)^m = a^m b^m)$$

(for $m = n, n-1$)

$\Rightarrow \quad (ab)^{n-1}\,(ab) = (ab)^{n-1}\,(ba)$

$\Rightarrow \quad ab = ba$

(By left cancellation law)

$\Rightarrow$ G is an Abelian group.

Example 31. Let f be a homomorphism from G into G, then prove that

(i) $f(e) = e$ where e is the unit element of G

(ii) $f(a^{-1}) = f(a)^{-1}$ for each $a \in G$.

Solution : (i) For each $a \in G$

$$f(a)\bar{e} = f(a) = f(ae) = f(a)\,f(e)$$

and hence $f(e) = e$

(ii) For each $a \in G$

$$f(a)\,f(a^{-1}) = f(aa^{-1}) = f(e) = \bar{e}$$

$$= f(a)\,f(a)^{-1}$$

and hence $f(a^{-1}) = f(a)^{-1}$

Example 32. Prove that a non empty subset H of a group G is a subgroup iff $HH^{-1} \subseteq H$.

Solution : Let H is subgroup of G.

Let ab^{-1} be any element of HH^{-1}

then $a \in H$ and $b \in H$

Also $b \in H \to b^{-1} \in H$ as H is a subgroup.

Thus $a \in H$, $b^{-1} \in H \to ab^{-1} \in H$

(By closure property)

$\therefore\ ab^{-1} \in HH^{-1} \to ab^{-1} \in H$

Hence $\quad HH^{-1} \subseteq H$

Let $\quad HH^{-1} \subseteq H$

Let $\quad a \in H$, $b \subseteq H$, then $ab^{-1} \in HH^{-1}$

$\because\ HH^{-1} \subseteq H$ so $ab^{-1} \in HH^{-1}$

$\Rightarrow \quad ab^{-1} \in H$

i.e. $\quad a \in H,\ b \in H \to ab^{-1} \in H$

$\therefore$ H is a subgroup of G.

Example 33. The mapping $I \to I(n)$ defined by $f(a) = \{a\}\ \forall a \in I$ is a homomorphism of I onto I (n) I being the set of all integers and I (n) is the set of residue classes modulo n.

Solution : Let x, y be any two element of I then

$$x + y \in I \text{ and } xy \in I \text{ and we have}$$

$$f(a+b) = \{a+b\}$$

$$(\because f(a) = \{a\}\ \forall a \in I)$$

$$= \{a\}_n\,\{b\}$$

or $\quad f(ab) = f(a) f(b) \quad \ldots(2)$

$\therefore$ From (1) and (2) we conclude that the mapping f is a homomorphism of I into I (n), as $\forall \{a\} \in$ I (n) there exists an element $a \in$ I such that

$$f(a) = \{a\}$$

Example 34. Show that a set

S = {am : $am \in z$ and m any fixed integer} is an additive group.

Solution : Here

$$S = \{am : m \text{ fixed integer } a \in z\}$$
$$= \{\ldots -3m - 2m - m, 0m\ 2m\ 3m, \ldots\}$$

To prove that S is a group it satisfies group postulate.

Closure : If and bm be any two elements of S where $a, b \in z$, then we get $am + bm = (a + b)m$ $\quad (\because a + b \in z)$

Associativity : $\forall abc \in z$, we get

$$am + (bm + cm) = am + (b + c)m$$
$$= (a + b + c)m \quad \ldots(1)$$

and $(am + bm) + cm = (a + b)m + cm$

$$= (a + b + c)m \quad \ldots(2)$$

$\therefore$ From (1) and (2) we find that

$$(m + (bm + cm)) = (am + bm) + cm$$

Hence, the operation of addition is associative in S.

Existence of identity : Since

$$0 + am = am = am + 0 \forall\ am \in s$$

So 0 is the identity of S for addition.

Existence of inverse : $am = 0 = (am) + (-am)$

Hence, the inverse of each elements of s exists.

Since all group postulates are satisfied and so the set S form a group under addition.

Example 35. The order of an element of a group is the same as that of its inverse.

Solution : Let $a \in$ G and let n and m be the orders of a and a^{-1} respectively.

Therefore, $\quad a^n = e, (a^{-1})^m = c \quad \ldots(1)$

Now $\quad a^n = e \Rightarrow (a^n)^{-1} = e^{-1}$

$\Rightarrow \quad (a^{-1})^n = e$

$\Rightarrow \quad m \leq n \quad$ (as m is order of a^{-1})

Again $(a^{-1})^m = e \Rightarrow (a^m)^{-1} = e$

$\Rightarrow \quad a^m = e \quad [\because x^{-1} = e \Rightarrow x = e]$

$\Rightarrow \quad n \leq m \quad$ [as n in order of a]

Thus $m \leq n$ and $n \leq m \Rightarrow m = n$

Example 36. Use Lagrange's theorem to show that any group of prime order can have no proper subgroups.

Solution : Let o (G) = P where P is a prime number

Let H be a subgroup of G and let o (H) = m

By Lagrange's theorem we know o (H)/o (G)

$\therefore$ m is a divisor of P.

Also P being prime, we find that either

$$m = 1 \text{ or } m = P$$

Now $\quad m = 1 \Rightarrow o(H) = 1$

$\Rightarrow \quad H = \{e\}$

and $\quad m = P \Rightarrow o(H) = o(G)$

$\Rightarrow \quad H = G$

$\therefore$ Either H = {e} or H = G *i.e.* H is not a proper subgroup of G.

Hence, any group of prime order can have no proper subgroups.

Example 37. If a and b are any elements of a group G, then $(bab^{-1})^n = ba^nb^{-1}$, for any integer n.

Solution : (i) Let $n = 0$

If e be the identity element, then by definition, we have $(bab^{-1})^0 = e$

Also $\quad ba^0b^{-1} = bb^{-1} = bb^{-1} = e$

$\therefore \quad (bab^{-1})^0 = ba^0b^{-1}$

(ii) Let $n > 0$

Here we get $(bab^{-1})^1 = bab^{-1} = ba^1b^{-1}$ $\quad (\because a^1 = a)$

$\Rightarrow$ $(bab^{-1})^n = ba^nb^{-1}$ is true for $n = 1$

Let us now suppose that this result is true for $n = k$, *i.e.* suppose

$$(bab^{-1})^k = ba^kb^{-1} \quad \ldots(1)$$

then $(bab^{-1})^{k+1} = (bab^{-1})^k (bab^{-1})^1$

$= (ba^kb^{-1})(bab^{-1})$ from (1)

$= ba^kb - 1\ bab^{-1}$

$= ba^k\ eab^{-1}$

$= ba^kab^{-1}$

$= ba^k + 1\ b - 1$

$\therefore$ The result is true for $n = k + 1$ also if it is true for $n = k$ also the result is true for $n = 1$

$\therefore$ By mathematical induction it is true for all values $opn > 0$.

(iii) Let $\quad n < 0$

Let $n = -k$, where $k > 0$

then $(bab^{-1})^n = (bab^{-1})^{-k}$

$= [(bab^{-1})^k]^{-1}$

$= [ba^k b^{-1}]^{-1}$

$= (b^{-1})^{-1} (a^k)^{-1} (b)^{-1}$

(By reversal rule)

$= ba^{-k}b^{-1}$

$= ba^n b^{-1}$ $(\because -k = n)$

Hence, $(bab - 1)^n = ba^n b^{-1}$

Example 38. If R is an integral domain, then prove that :

(i) R $[x]$ is also an integral domain.

(ii) R $[x]$ is not a field.

Solution : (i) Let R be an integral domain and let P $(x) \neq 0$ and $q(x) \neq 0$ be in R $[x]$ since R is an integral domain we have

deg (P (x) q (x)) = *deg* P (x) + *deg* q (x) now it is impossible to have P (x) q $(x) = 0$ and therefore, R $[x]$ is an integral domain.

(ii) Let P $(x) \in$ R $[x]$ and *deg* P $(x) > 0$. Since degree of the identity polynomial 1 is 0 there exists no q $(x) \in$ R $[x]$ such that *deg* P (x) + *deg* q (x) = *deg* 1 = 0. Thus no polynomial of non-zero degree has a multiplicative inverse and thus R $[x]$ in not a field.

Example 39. Write down the cyclic groups of order 2, 3 and 4 from the symmetric groups 4 on four symbols.

Solution : The required cyclic groups of order 2 are

$H_1 = \{(12)\ (1)\ (2)\ (3)\ (4) = 1\}$

Here if $a = (1, 2)$, then

$a^2 = (1)\ (2)\ (3)\ (4)$

$H_2 = \{(13)\ (1)\ (2)\ (3)\ (4) = I\}$

$H_3 = \{(14)\ (1)\ (2)\ (3)\ (4) = I\}$

$H_4 = \{(23)\ (1)\ (2)\ (3)\ (4) = I\}$

$H_5 = \{(24)\ (1)\ (2)\ (3)\ (4) = I\}$

$H_6 = \{(34)\ (1)\ (2)\ (3)\ (4) = I\}$

The required cyclic groups of order 3 are

$H_1 = \{(123), (132)\ (1)\ (2)\ (3)\ (4) = I\}$

IP$a = (123)$ then $a^2 = (132)$ and $a^3 = I$

$H_2 = \{(124)\ (142)\ (1)\ (2)\ (3)\ (4) = I\}$

$H_3 = \{(134)\ (143)\ (1)\ (2)\ (3)\ (4) = I\}$

$H_4 = \{(234)\ (243)\ (1)\ (2)\ (3)\ (4) = I\}$

and the required cyclic groups of order 4 are

$H_1 = \{(1234)\ (13)\ (24)\ (1432)$

$(1)\ (2)\ (3)\ (4) = I]$

($\because$ IPa = (1234), then $a^2 = (13)\ (24)$ a^3 = (1432) and $a^4 = I$)

$H_2 = \{(1243)\ (14)\ (23)\ (1342)$

$(1)\ (2)\ (3)\ (4) = I\}$

$H_3 = \{(1324)\ (12)\ (34)\ (1423)$

$(1)\ (2)\ (3)\ (4) = I\}$

Example 40. If R be commutative ring with unity and I an ideal in R, then prove that R/I is a field iff I is a maximal ideal in R.

Solution : Let I be a maximal ideal in R, then I < R and R/I is a commutative ring with unity.

Let x be any element of R/I and let us consider a subset S of R where

$$S = \{a + xb : a \in I\ b \in I\}$$

Now $\quad Y \in R$

$a + xb \in S$

$\Rightarrow \quad (a + xb)\ y \in S$

$\Rightarrow \quad ay + x\ (by) \in S$

Similarly $y\ (a + xb) \in S$

$\therefore$ S is an ideal in R

Also as $I \subset S$ so $S = R$.

Hence any element $z \in$ R can be written as

$$z = a + xc \text{ where } c \in R$$

Let c be the unity in R and $c = a + x, d$, where $d \in R$

Again as $e + I = (a + I) + (xc + I)$

$= (a + I) + (x + I)\ (c + I)$

$= (x + I)\ (c + I)$

So $(c + I)$ is the multiplicative inverse of $(x + I)$

$\therefore$ The ring of co-sets R/I is a field as x is any element of R/I

On the contrary assume let R/I be a field and suppose I is not maximal in R.

Let I' be another ideal in R such that

$$I \subset I \subset R$$

Let z be any element of R and let

$$q \in I' - I$$

Then if, we define

$(q + I)^{-1}\ (z + I) = (p + I)$

We get $\quad (z + I) = (q + I\ (p + I)$

Now as $z - qp \in I$ and $I \subset I$ so $z - qp \in I$

But $P \in I'$, so $z \in I$ also $z \in R$

$\therefore$ I = R which contradicts that fact $I \subset R$

Hence, 0 or supposition is wrong and so I is a maximal in R.

Example 41. Prove that if R is a commutative ring and $a \in$ R, then

Ra = $\{ra : r \in R\}$ is an ideal of R

Solution : If x, y be any two arbitrary elements of Ra

then $x = r_1 a$ and $y = r_2 a$

For some $r_1 r_2 \in R$

$\therefore \quad x - y = r_1 a - r_2 a = (r_1 - r_2)\, a \in Ra$

(Since $r_1 - r_2 \in R$ as $r_1 - r_2 \in R$)

$\therefore\ x \in Ra\ y \in Ra \Rightarrow x - y \in Ra$ ...(1)

Again $x - y = (r_2 a)\,(r_2 a) = (r_1 r_2)\, a \in Ra$

(Since $r_1 r_2\, a \in R$ as $a, r_1 r_2 \in R$)

$\therefore\ x \in Ra\ y \in Ra \Rightarrow xy \in Ra$ ...(2)

From (1) and (2) we conclude that Ra is a Subring of R

Again if $u \in R$

then $ux = u\,(r_1 a) = (ur_1)\, a \in Ra$

(Since $ur_1 \in R$ as $ur_1 \in R$)

Similarly we can prove that

$$xa = (r_1 a)^4$$
$$= u\,(r_1 a)$$

as R is a commutative ring

$$= (ur_1)\, a \in Ra \text{ as above}$$

Thus, we find that Ra is a subring of R and for each element $x \in Ra$ and $u \in R$ we find that $ux \in Ra$ and

$$xu \in Ra$$

$\because$ Ru is an ideal.

Example 42. Prove that a non-empty finite subset H of a group G is a subgroup of G.

If $a, b \in H$

$\Rightarrow \quad ab \in H$

being the composition in G.

Solution : The non-empty subset H of G is a subgroup of G if it satisfies group axioms.

Closure : Closure property is already given because of the given condition.

$$a, b \in H \Rightarrow ab \in H$$

Associative : Since H is a subset of the group G, the associative law holds for all elements of H.

Existence of Inverse & Identity : To prove existence of identity and inverse.

Let $a \in H$ then by closure law, we have

$a^2 \in H, a^3 \in H, \ldots a^n \in H \ldots$ *i.e.* $a, a^2, \ldots a^3 \ldots a^n \ldots \in H$.

Since H is a finite subset of G, there must be repetitions in the elements stated above otherwise H will become infinite.

Let $a^r = a^s$ for $r \neq s$ and $r > s > 0$

then $a^{r-s} = e$ (by cancellation law)

Also $a^{r-s} \in H$

$\therefore\ e$, the identity element $\in H$

Clearly $r - s \geq 1$

Therefore, $r - s - 1 \geq 0$

Hence, $a^{r-s-1} \in H$

$\Rightarrow \quad a^r - soa^{-1} \in H$

$\Rightarrow \quad eoa^{-1} \in H$

$\Rightarrow \quad a^{-1} \in H$

($\because a^{r-s} = e$ already proved)

All the axioms of a group are satisfied and H $\subset$ G is a subgroup of G.

Example 43. Let G be a group H a subgroup of G. Let for $x \in G$ such that

$$xHx^{-1} = \{ax^{-1} : a \in H\}$$

Prove that xHx^{-1} is a subgroup of G.

Solution : Let xa_1x^{-1} and xa_2x^{-1} be any two elements of xHx^{-1}, then $a_1 a_2 \in H$.

Now, we have

$$(xa_1x^{-1})\,(xa_2x^{-1})^{-1} = (xa_1x^{-1})\,(xa_2^{-1}x^{-1})$$
$$= xa_1\,(x^{-1}x)\,a_2^{-1}\,x^{-1}$$
$$= xa_1a_2^{-1}x^{-1}$$
$$= xax^{-1}$$

if $\quad a = a_1 a_2^{-1} \in H$

Evidently $xax^{-1} \in xHx^{-1}$

Hence, xHx^{-1} is a subgroup of G.

Example 44. Prove that

(i) Every cyclic group is Abelian group.

(ii) The order of a cyclic group is same as that of its generator.

Solution : (i) Let G = $(a) = \{e, a, a^2, a^3, \ldots\}$ be a cyclic group with a as the generator then for any

$$m, n \in z, a^m, a^n \in G$$

and
$$a^m a^n = a^{m+n}$$
$$= a^{n+m}$$
$$= a^n a^m$$

and hence, G is Abelian, in the additive rotation we write

$$G = \{1, a, 2a, 3a \ldots\}$$

In this case

$$\begin{aligned} ma + na &= (m+n)a \\ &= (n+m)a \\ &= na + ma \end{aligned}$$

and thus G is Abelian.

(ii) Let G be a cyclic group with a generator

$$a \in G$$

Let $o(a) = n$

i.e. $a^n = e$ and $a^m \neq e$ for $0 < m < n$

If $m > n$ let $m = q^{n+r}$

$$0 \leq r < N$$

so
$$\begin{aligned} a^m &= a^{q^n + r} = a^{q^n} \cdot a^r \\ &= (a^n)^q \cdot a^r \\ &= e^q \cdot a^r = e \cdot a^r \\ &= a^r \end{aligned}$$

Therefore, there are exactly n elements in the group and they are

$$\{e, aa^2 \ldots a^{n-1}\} \Rightarrow o(G) - n$$

Example 45. Let G be a finite group and $a \in G$, show that order of a, $o(a)$ is equal to the o (H) where H is the subgroup of G generated by a deduce that $o(a)$ divides $o(G)$.

Solution : The subgroup H of G generated by a is given by

$$H = \{a^r : r \in I\}$$

Where I is the set of integers

Let $o(H) = n$

We can show that H has exactly m distinct elements $a, a^2, a^3 \ldots a^3$ and that every element of H is equal to one of these m elements.

so $o(H) = o(a) = m$

By Lagrange's theorem

$$o(H) \mid o(G)$$

Hence $o(a) \mid o(G)$

Example 46. Prove that the mapping

$f : V_3(F) \rightarrow V_2(F)$ defined by

$$f(a_1 a_2 a_3) = (a_1, a_2)$$

is a homomorphism ?

Solution : Let $\alpha = (a_1, a_2, a_3)$ and $\beta = (b_1, b_2, b_3)$ be any two elements of V_3 (V)

Let a, b be any two elements of F, then

$$\begin{aligned} f(a\alpha + b\beta) &= f[(a_1, a_2, a_3) + b(b_1, b_2, b_3)] \\ &= f[aa_1 + bb_1, aa_2 + bb_2, aa_3 + bb_3)] \\ &= (aa_1 + bb_1, aa_2 + bb_2) \\ &= a(a_1, a_2) + b(b_1, b_2) \\ &= af(a_1, a_2, a_3) + bf(b_1, b_2, b_3) \\ &= af(\alpha) + bf(\beta) \end{aligned}$$

$\therefore f$ is a linear transformation

Let $(a_1 a_2)$ be an element of V (F), then $(a_1, a_2, 0) \in (-V_3 F)$ and $f(a_1, a_2, 0) = (a_1, a_2)$

Hence f is onto

Thus f is a homomorphism of V_3 (F) onto V_2 (F)

If W is the Kernel of this homomorphism then

$$W = \{0, 0, a) : a \in F\}$$

Thus $f(0, 0, a) = (0\,0)$

The zero vector of V_2 (F) $\forall a \in F$

Also if $f(a_1, a_2, a_3) = (0, 0)$

Then $f(a_1, a_2, a_3) = (a_1, a_2) = (0, 0)$

i.e., $a_1 = 0 = a_2$

Hence $(a_1, a_2, a_3) \in W$

The W is the Kernel of f.

Example 47. Prove that the relation of isomorphism in the set of all groups in an equivalence relation.

Solution : If G and $\bar{G}$ are isomorphic

i.e. $G = \bar{G}$

The $G \approx \bar{G}$ is a equivalence a relation if its satisfies the following axioms :

(i) $G \approx \bar{G}$ (reflexivity)

(ii) $G \approx G\bar{G} \approx \bar{\bar{G}}$ implies $\bar{G} \approx \bar{\bar{G}}$ (symmetry)

(iii) $G \approx G\bar{G} \approx \bar{\bar{G}}$ implies $\bar{G} \approx \bar{\bar{G}}$ (Transitivity)

For each $x \in G$ define $f : G - G$ by $f(x) = x$

Then f is an isomorphism of G onto itself and hence $G = G$.

Let $G \approx \bar{G}$, then there exists an isomorphism.

f from G onto $\bar{G}$ since f is 1 – 1 and onto, the map

$f^{-1} : \bar{G} \rightarrow G$ exists and is 1 – 1 and onto

Let

$a, b \in \bar{G}$ and let $f(x) = 4$

$f(y) = b$ for $x, y \in G$

Now $x = f^{-1}(a)$, $y = f^{-1}(b)$

$$f(xy) = f(x)f(y) = ab$$

and so $f^{-1}(ab) = xy = f^{-1}(a)f^{-1}(b)$

Then f^{-1} is also a homomorphism and so $\bar{G} \approx G$.

Let $G \approx \bar{G}$ and $\bar{G} \approx \bar{\bar{G}}$ thus there exist isomorphisms f and g from G onto $\bar{G}$ and from $\bar{G}$ onto $\bar{\bar{G}}$ respectively since f and g are one-one and onto, the composition g of : $G \Rightarrow \bar{\bar{G}}$ is 1 – 1 and onto

Further from $x, y = \in G$

$$\begin{aligned}(gof)(xy) &= g(f(xy)) \\ &= g(f(x)f(y)) \\ &= g(f(x))\,g(f(y))\end{aligned}$$

Thus g of is a homomorphism and hence $G \approx \bar{G}$

Example 48. Prove that the left cosets of a subgroup are either disjoint or identical.

Solution : Let H be a subgroup of a group G and $a, b \in G$.

If there is no element common to aH and bH, then $aH \cap bH = \phi$, the null set.

i.e. aH and bH are disjoint.

If there is an element c (say) common to aH then $aH \cap bH =$ then we have

$$\begin{aligned} c &= ah_1, h_1 \in H \\ c &= bh_2, h_2 \in H \\ ah_1 &= bh_2 \\ \Rightarrow \quad (ah_1)h_2^{-1} &= (bh_2)\,h_2^{-1} \\ \Rightarrow \quad a\,(h_1h_2^{-1}) &= b\,(h_2h_2^{-1}) \\ \Rightarrow \quad a\,(h_1h_2^{-1}) &= b \\ \Rightarrow \quad a^{-1}\,a\,(h_1h_2^{-1}) &= a^{-1}b \\ \Rightarrow \quad (a^{-1}a)\,(h_1h_2^{-1}) &= a^{-1}b \\ h_1h_2^{-1} &= a^{-1}b \end{aligned}$$

$\therefore$ $a^{-1}b \in H$ since $h_1h_2^{-1} \in H$

Hence, $aH = bH$

Hence, two left cosets which are not disjoint are identical.

Example 49. In any group G show that $e^n = e$ for any integer n.

Solution : (i) Let $n = 0$

If $n = 0$, then $e^n = e^0 = e$

(ii) Let $n > 0$ (*i.e.* n is a positive integer)

Let $e^n = e$ be true for $n = m$ *i.e.* $e^m = e$

Now $e^{m+1} = e^m \cdot e^1 = e^m e = e \cdot e$ $\quad (\because e^m = e)$

or $\quad e^{n+1} = e \quad (\because a \cdot e = a \forall a \in G)$

This shows that $e^n = e$ is true for $n = m + 1$ if it is true for $n = m$.

Obviously $e^1 = e$ *i.e.* $e^n = e$ is true for $n = 1$

Hence if is true for $n = 1 + 1$ *i.e.* 2 if is true for $n = 1$ and proceeding in this way we can show that it is true for $n = 3$, 4 etc.

Hence $e^n = e$ is for all positive integral values of n.

(iii) Let $n < 0$ (*i.e.* n is a negative integer)

Let $n = k$ where k is a positive integer

Then $e^n = e^{-k} = (e^k)^{-1} = (e)^{-1}$ $\quad (\because ek = e)$

For $\quad k > 0 = e^{-1} = e$

Hence, in any group $e^n = e$ for any integer n.

Example 50. Prove that the set {1, 2, 3, 4} form a group under multiplication modul.

Solution : Under multiplication modulo the composition table is

s	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Closure—This table shows that the product of any two elements of the given set under multiplication modulos as composition belongs to the set and therefore under the given operation the set is closed.

Associative—(ab). c and a $(b{\cdot}c)$ both denote zero or that least non-negative integer obtained on dividing the ordinary multiplication of a, b and c by 5. *i.e.* the composition is associative.

Existence of Identity—From the table it is evident that 1 is the identity.

Existence of Inverse—The inverse of 1, 2, 3 and 4 are 1, 3, 2 and 4 respectively because $1 \cdot 1 = 1$, $2 \cdot 3 = 6 = 1$ (mod 5) $3 \cdot 2 = 1$ (mod 5) and $4 \cdot 4 = 1$ (mod 5) this is also evident from the composition table.

Commutative—$ab = ba$ any two elements a, b in the given set.

Hence, all the group postulates are satisfied and so the given set is a finite Abelian group of order 4 under multiplication.

Example 51. If a is of order n and p is prime to n, then the order of ap is also n.

Solution : Let n' be the order of ap

then we have $n' \le n$ ...(1)

Again p is prime to n, so there exist integers α and β such that

$$\alpha n + \beta n = 1$$

Hence, we can write

$$a = \alpha = \alpha^{an} + \beta^{n}$$
$$= a^{ap} \cdot \alpha\beta^{n}$$
$$= \alpha^{ap}$$

as $a^{n} = e$ then identity element

$$= (ap)^{a}$$

a is a power of a', hence, we have

$$n \le n$$

$\therefore$ a is a power of ap hence, we have

From (1) and (2) whaven $n' = n$

Example 52. Let G be the group of all real numbers under addition and G be the group of all non-zero real numbers under multiplication. Prove that the mapping ϕ: G $\to$ G is such that $\phi(x) = z^{x}$, $x \in$ G, then show that ϕ is homomorphism.

Solution : Let $m, n \in$ G, then $\phi(m) = 2^{m}$

$$\phi(n) = 2^{n}$$

Since $\phi(x) = 2^{x}\ x \in G$

Now $\phi(m+n) = 2^{m+n} = 2^{m}\,2^{n}$

$$= \phi(m)\,\phi(n)$$

i.e. $\phi(m+n) = \phi(m)\,\phi(n)$

Hence, the mapping ϕ is a homomorphism.

Example 53. Prove that if S is any ideal of ring R and T any subring of R then S is ideal of S + T.

Solution : If $a, b \in$ S and $a\beta \in$ T

$\Rightarrow$ $a + a \in$ S + T and $b + \beta \in$ S + T

Also $(a+\alpha)(b+\beta) \equiv ab + a\beta + \alpha b + \alpha\beta$

$\Rightarrow$ $(a+a)(b+\beta) - a\beta = ab + a\beta + \alpha b \in$ S

S being an idea, we get

$ab \in$ S, $ab \in$ S and $a\beta \equiv$ S

Also $a\beta \in$ T

$\therefore$ $(a+a)(b+\beta) \in$ S + T

Again $(a+a) - (b+\beta) = (a-b) + (\alpha\beta) \in$ S + T

$\therefore$ S + T is a subring of R

Also we have

$$S \subset S + T \subset R$$

Hence, S is an ideal of S + T

Example 54. Prove that the order of every element of a finite group G is finite.

Solution : Let o (G) = n and let $a \in$ G be arbitrary.

The element $e, a, a^{2} \ldots a^{n}$ are $(n+1)$ in number and o (G) = n and hence they are not all $\le$ S $\le n$ such that $a^{r} = a^{s}$. Hence, $e = a^{r}a^{-r} = a^{sa-r} = as - r = a^{k}$ where $k = s - r$, $1 \le k \le n$.

Therefore, $o(a)$ is finite.

Example 55. Prove that if H, K are two subgroup of a group G, then HK is a subgroup of G iff HK = KH.

Solution : Suppose that HK is a subgroup then

Then $(HK)^{-1} = HK$

$\Rightarrow$ $K^{-1}H^{-1} = HK$

$$KH = HK$$

[$\because$ H is subgroup $\Rightarrow$ $H^{-1} = H$ and K is a subgroup $\Rightarrow K^{-1} = K$]

Let HK = KH then, we have to prove that HK is a subgroup of G for this it is sufficient to prove

$$(HK)(HK)^{-1} = HK$$

Now $(HK)(HK^{-1}) = HK(K^{-1}H^{-1})$ (Reversal law)

$= H(KK^{-1})H^{-1}$ (Associativity)

$$= (HK)H^{-1}$$

[$\because$ K is a subgroup $\because$ $KK^{-1} = K$]

$$= (KH) - H^{-1}$$

[$\because$ HK = KH]

$$= K[HH^{-1}]$$
$$= KH$$

[$\because$ H is a subgroup $\therefore$ $HM^{-1} = H$]

$$HK = KH$$

$\Rightarrow$ HK is subgroup

Example 56. Prove that the only element of order one in a group. Then by the definition of order of an element of a group.

Solution : We have

$$a^{-1} = e \text{ or } a = e$$

which is the possible let $a \ne e$ be an element of order of an element of a group, we have

$$a^{-1} = e \text{ or } a = e$$

which is the contradiction to assumption that $a \ne e$

Hence, the identity element e is the only element of order one in any group.

Example 57. Let R be a system satisfying all the conditions of a ring except commulativity of addition. If there exists an element $x \in$ R which can be right cancelled in the sense $a{\cdot}x = b{\cdot}x \Rightarrow a = b$ them show that (R + , .) is a ring.

Solution : Here

$(a + b) \cdot (x + x) = (a + b)\, x + (a + b) \cdot x$ and also

$(a + b) \cdot (x + x) = a{\cdot}x + b{\cdot}x + a{\cdot}x + bx$

$\because\ ax + b{\cdot}x + ax + b{\cdot}x$

$= a{\cdot}x + ax + b{\cdot}x + b{\cdot}x$

$\Rightarrow \quad b{\cdot}x + ax = a{\cdot}x + b{\cdot}x$

$\Rightarrow \quad (b + a)\, x = (a + b)\, x$

$\Rightarrow \quad b + a = a + b$

$(\because\ ax = bx \Rightarrow a = b)$

Hence, commutative law of addition also holds in R besides the other conditions of a ring.

Hence (R + •) is a ring.

Example 58. Prove that a field has no proper ideal.

Solution : Let I be an ideal of a field F

Now if F has no proper ideal, then by definition either I is the null ideal {0} or I is the unit ideal F

i.e. either I = {0} or I = F

If I = {0} the null ideal, then nothing is left to be proved

If I ≠ {0} then there exists atleast one non zero element a in such that

$1 = a^{-1} a \in$ I

Also $\forall\ b \in$ F, we have $b = b\ 1 \in$ F

i.e. all element of F $\in$ I

$\Rightarrow \quad$ F $\subseteq$ I ...(i)

But by definition of idea, we know that every ideal of F $\subseteq$ F

i.e. I $\subseteq$ F ...(ii)

$\because$ From (i) and (ii) we get

I = F

Example 59. Prove that intersection of two subgroup is again a subgroup.

Solution : Let H_1 and H_2 or e two subgroups of group G

Let $a \in H_1 \cap H_2$

and $b \in H_1 \cap H_2$

then $a \in H_1 \cap H_2$

$b \in H_1 \cap H_2$

$\Rightarrow \quad a \in H_1\, a \in H_2$

and $b \in H_1\, b \in H_2$

$\Rightarrow \quad a \in H_1\, b \in H_1$

and $a \in H_2\, b \in H_2$

$\Rightarrow \quad ab^{-1} \in H_1$

and $ab^{-1} \in H_2$

[$\because$ H_1 and H_2 are subgroups]

$\Rightarrow \quad ab^{-1} \in H_1 \cap H_2$

Hence, $H_1 \cap H_2$ is a subgroup.

OBJECTIVE TYPE QUESTIONS

1. Which of the following is false ?
   (A) $(z, +)$ is a group
   (B) $(z, +, \bullet)$ is a ring
   (C) $(z, +, \bullet)$ is a commutative ring
   (D) $(z, +, \bullet)$ is not an integral domain
2. Every finite integral domain is a—
   (A) Group (B) Ring
   (C) Field (D) Both ring and field
3. Which of the following is not an integral domain ?
   (A) (N, +, •) (B) (C, +, •)
   (C) (Q, +, •) (D) (R, +, •)
4. The set of residue classes (modulo n) is a ring without zero divisor w.r.t. addition and multiplication, iff—
   (A) n is prime (B) n is even
   (C) n is add (D) None of these
5. A boolean ring—
   (A) Is commutative (B) Has a unity
   (C) Has zero divisor (D) None of these
6. An integral domain S is—
   (A) Field when S is finite
   (B) Always a field
   (C) Never field
   (D) None of these
7. A divisor ring has at least—
   (A) Two elements
   (B) Three elements
   (C) One element
   (D) None of these

8. If (R, +, •) is a ring such that $x \cdot x = x \ \forall \ x \in$ R, then—
   (A) $x + y = 0 \Rightarrow x = y$
   (B) $x + x \neq 0$
   (C) $x \neq y \Rightarrow x + y = 0$
   (D) None of these

9. An integral domain—
   (A) Necessarily possesses multiplicative inverse of its non-zero elements
   (B) Is a commutative ring
   (C) Is a division ring
   (D) None of these

10. The ring of integers is also a—
   (A) Field (B) Integral domain
   (C) Division ring (D) None of these

11. The ring of even integers is also a—
   (A) Field
   (B) Division ring
   (C) Integral domain
   (D) None of these

12. Which of the following is false ?
   (A) Every field is an integral domain
   (B) Every integral domain is a commutative ring
   (C) Every commutative ring is a ring
   (D) At least one of the above is false

13. The set $\{14r : r \in z\}$ is—
   (A) Maximal ideal of z
   (B) Just a principal ideal of z
   (C) Prime ideal of z
   (D) None of these

14. The condition for none existence of zero divisor is—
   (A) $a^2 = a \ \forall \ a \in$ R
   (B) The cancellation laws holds for multiplication in R
   (C) $(a + b)^2 = a^2 + b^2 + 2ab, \forall \ a, b \in$ R
   (D) None of these

15. An ideal P = $\{Pr : r \in z\}$ which is a proper ideal of ring z is a prime ideal iff—
   (A) P is prime
   (B) P is odd
   (C) P is a multiple of 3
   (D) P is even

16. The set of residue classes mod m ($m \in$ N) is a ring without zero divisors under addition and multiplication for—
   (A) m prime (B) m odd
   (C) m any integer (D) m composite

17. If r is a system such that it is a group under addition and multiplication obeys the closure and distributive laws, then—
   (A) R need not be a ring
   (B) R has to be a ring
   (C) R is not a ring
   (D) R is necessarily a field

18. Which of the following integral domains is not ordered ?
   (A) The integers
   (B) The rational numbers
   (C) The real numbers
   (D) The complex numbers

19. Which of the following is not a prime field ?
   (A) The set of rational numbers
   (B) The set of residue classes mod 5
   (C) The set of residue classes mod 6
   (D) All of the above

20. Which of the following statement is correct ?
   (A) In a ring $ab = 0 \Rightarrow$ either $a = 0$ or $b = 0$
   (B) Every finite ring is an integral domain
   (C) Every finite integral domain is a field
   (D) The set of natural numbers is a ring with respect to the usual addition and multiplication

21. Let R {0, 1, 2, 3}, under addition and multiplication modulo 4 is—
   (A) A field
   (B) A ring with zero divisors
   (C) A ring without zero divisors
   (D) A division ring

22. Let (R = {0, 1, 2, 3, 4, 5} + 6, × 6). The R is—
   (A) A ring with zero divisors
   (B) A field
   (C) A division ring
   (D) A ring without zero divisors

23. Set residue classes modulo P, where P is prime, under addition and multiplication of residue classes is—
   (A) Field

(B) Skew field under
(C) Integral domain
(D) None of these

24. Let P be a prime number set of integers $I_A = \{0, 1, 2, \ldots P^{-1}\}$ under addition and multiplication modulo P forms—
(A) Ring without zero divisors
(B) Field
(C) Integral domain
(D) All above are correct

25. A mapping f of a ring R onto a ring R' is called homomorphism if for each $a \in$ R, $b \in$ R—
(A) $f(a+b) = f(a) + f(b)$
(B) $f(a+b) = f(a) - f(b)$
(C) $f(ab) = f(a) - f(b)$
(D) $f(a+b) = f(a) + b$ and $f(ab) = f(a) \cdot f(b)$

26. Let M be the ring 2 × 2 matrices over the set of integers, let L = $\left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \middle| \, a, b \in z \right\}$, and K = $\left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} a, b \in z \right\}$, then—
(A) L and K both left ideal of M
(B) L and K both right ideals of M
(C) L is left ideal of M and K is right ideal of M
(D) L is right ideal of M and K is left ideal of M

27. The set of all 2 × 2 matrices over the field of real number under the usual addition and multiplication of matrices is—
(A) Not a ring
(B) A ring with unity
(C) A commutative ring
(D) An integral domain

28. If Q and z are the sets of rational numbers and integers respective then which one of the following triples is a field ?
(A) (Q, +, ×) (B) (Q, –, ×)
(C) (Z, +, ×) (D) (Z, –, ×)

29. The set of integers under ordinary addition and multiplication—
(A) Forms a group
(B) Forms a ring
(C) Forms a field
(D) Does not form integral domain

30. Which of the following algebric operations is a field ?
(A) (R, +, •) (B) (R, –, •)
(C) (R, •, ÷) (D) (R, ÷, •)

31. The set of all rational numbers is—
(A) An additive group
(B) A multiplication group
(C) A cyclic group
(D) A finite group

32. The supremum of the function $f(x) = x - \frac{1}{x}$ in the internal $\left[\frac{1}{2}, 2\right]$ is—
(A) 2 (B) 1
(C) 3/2 (D) Does not exist

33. To form a 'Ring' we required, at least—
(A) One element
(B) Two elements
(C) Three elements
(D) One element which is additive identity

34. $(z_P, + P, P)$ is a field, if and only if—
(A) P is composite number
(B) P is prime number
(C) P is an even number
(D) P is add number

35. Consider the statements—
(a) The product of two rational numbers is always a rational number
(b) The product of two irrational numbers is always an irrational number. Then—
(A) Both (a) and (b) are correct
(B) (a) is incorrect and (b) is correct
(C) (a) is correct (b) is in correct
(D) (a) and (b) are in correct

36. The set S of square matrices of same order with respect to matrix addition is a—
(A) Quasi-group (B) Semi-group
(C) Group (D) Abelian group

37. The set of square matrices order 2, with respect to matrix multiplication is a—

(A) Quasi-group (B) Semi-group
(C) Monoid (D) Group

38. The set of all non-singular square matrices of same order with respect to matrix multiplication is—
(A) Quasi-group (B) Monoid
(C) Group (D) Abelian group

39. If order of group G is P^2, where P is prime then—
(A) G is Abelian (B) G is not Abelian
(C) G is ring (D) None of these

40. (a) If G is group, for $a \in$ G, N (a) is the normalizer of a, then $\forall x \in$ N (a)—
(A) $xa = ax$ (B) $xa = e$
(C) $ax = e$ (D) $xa \neq ax$

41. If G is a group, then for all a, $b \in$ G—
(A) $(ab)^{-1} = a^{-1}b^{-1}$ (B) $(ab)^{-1} = b^{-1}a^{-1}$
(C) $(ab)^{-1} = ab$ (D) $(ab)^{-1} = ba$

42. If G is a set of integers and $a{\cdot}b \equiv a - b$, then G is—
(A) Quasi group (B) Semi-group
(C) Monoid (D) Group

43. In a group G, for each element $a \in$ G, there is—
(A) No inverse
(B) A unique inverse $a^{-1} \in$ G
(C) More than one inverse
(D) None of these

44. If a, $b \in$ G, a group then b is conjugate to a if exist $c \in$ G…
(A) $b = c^{-1}ac$ (B) $a = cb$
(C) $b = ac^{-1}$ (D) $b = ac^{-1}a$

45. If P is prime number and P|o (G), then $a \in$ G—
(A) $ap \in$ G (B) $ap \notin$ G
(C) $ap \subset$ G (D) $ap \supset$ G

46. If G is a group of order n then, order of identity elements is—
(A) One (B) Greater than one
(C) n (D) None of these

47. If $a \in$ G is order n and P is prime to n, then the order of ap is—
(A) n (B) One
(C) Less than n (D) Greater than n

48. If the orders of elements a, $a^{-1} \in$ G are m and n respectively then—
(A) $m = n$ (B) $m \neq n$
(C) $m = n = 0$ (D) None of these

49. If in a group G, $a \in$ G the order of a is n and order of ap is m, then—
(A) $m \leq n$ (B) $m \geq n$
(C) $m = 0$ (D) None of these

50. The identity permutation is—
(A) Even permutation
(B) Odd permutation
(C) Neither even nor odd
(D) None of these

51. The product of even permutation is—
(A) Even permutation
(B) Odd permutation
(C) Neither even nor odd
(D) None of these

52. The inverse of an even permutation is—
(A) Odd permutation
(B) Even permutation
(C) Even or odd permutation
(D) None of these

53. The product of (1245) (32154) is—
(A) (23) (B) (15)
(C) (341) (D) (1531)

54. The inverse of an odd permutation is—
(A) Odd permutation
(B) Even permutation
(C) Even or odd
(D) None of these

55. If b and c are the inverse of some element $a \in$ G, then—
(A) $b = c$
(B) $b \neq c$
(C) $b = ac$ for same a
(D) None of these

56. Let Z be a set of integers, then under ordinary multiplication (Z) is—
(A) Monoid
(B) Semi-group
(C) Quasi-group
(D) Group

57. If N is a set of natural numbers then under binary operation $a - b = a - b$, (N) is—
(A) Quasi-group (B) Semi-group
(C) Monoid (D) Group

58. If G is a finite group and order of group is m then $\forall\, a \in$ G—
(A) $a^m = e$ an identity
(B) $a^n \neq e$
(C) $a^m = a$
(D) $a^m = a^{-1}$

59. HK is a sub-group of G iff—
(A) HK = KH (B) HK $\subset$ KH
(C) HK $\supset$ KH (D) HK $\neq$ KH

60. If G is group and $a \in$ G such that $a^2 = a$, then a is equal to—
(A) Identity element (B) Inverse
(C) Zero element (D) None of these

61. The generators of a group G = $\{a, a^2, a^3, a^4, a^5, a^6 = e\}$ are—
(A) a and a^5 (B) a^2 and a^4
(C) a^3 and a^5 (D) a^2 and a^3

62. If G = $\{1 - 1, i - i\}$ is a multiplicative group then order of i is—
(A) One (B) Two
(C) Three (D) Four

63. If G = {0, 1, 2, 3, 4) + 5}, the order of 2 is—
(A) One (B) Two
(C) Three (D) Five

64. If G is a group of even order, $\forall a \neq e$ if $a^2 = e$, then G is—
(A) Abelian group (B) Sub-group
(C) Normal group (D) None of these

65. Every group of prime order is—
(A) Cyclic (B) A belian
(C) Sub-group (D) Normal group

66. If H_1 and H_2 are two right coset sets of sub-group H, then—
(A) $H_1 \cap H_2\ \phi$ or $H_1 = H_2$
(B) $H_1 \cap H_2 \neq \phi$
(C) $H_1 \cup H_2 = \phi$
(D) $H_1 \neq H_2$ and $H_1 \cap H_2 \neq \phi$

67. The number of elements in a group is—
(A) Identity of group
(B) Order of group
(C) Inverse of group
(D) None of these

68. A one-one mapping of a finite group onto itself is—
(A) Isomorphism (B) Homomorphism
(C) Automorphism (D) None of these

69. If in a group G, $\forall\, a \in$ G—
(A) $(a^{-1})^{-1} = a$ (B) $(a^{-1})^{-1} = a^{-1}$
(C) $(a^{-1})^{-1} = a^2$ (D) None of these

70. If $f = (23)$ and $g = (45)$ be two permutation of five symbols 1, 2, 3, 4, 5 then gf is—
(A) $\begin{pmatrix} 1\,2\,3\,4\,5 \\ 1\,3\,5\,4\,2 \end{pmatrix}$ (B) $\begin{pmatrix} 1\,2\,3\,5\,6 \\ 1\,4\,6\,5\,4 \end{pmatrix}$
(C) $\begin{pmatrix} 1\,2\,3\,5\,7 \\ 1\,4\,6\,4\,1 \end{pmatrix}$ (D) $\begin{pmatrix} 1\,2\,3\,4\,5 \\ 1\,3\,2\,5\,4 \end{pmatrix}$

71. Given permutation $\begin{pmatrix} 1\,2\,3\,4\,5\,6 \\ 6\,1\,2\,5\,4\,6 \end{pmatrix}$ is equivalent to—
(A) (1632) (21) (B) (1632) (11)
(C) (1632) (45) (D) (1632) (54)

72. If given permutation are A = $\begin{pmatrix} 1\,2\,3\,4\,5 \\ 2\,3\,1\,5\,4 \end{pmatrix}$, B = $\begin{pmatrix} 1\,2\,3\,4\,5 \\ 1\,3\,4\,5\,2 \end{pmatrix}$, find BA—
(A) $\begin{pmatrix} 1\,2\,3\,4\,5 \\ 2\,1\,5\,4\,3 \end{pmatrix}$ (B) $\begin{pmatrix} 2\,1\,5\,3\,5 \\ 1\,6\,4\,2\,1 \end{pmatrix}$
(C) $\begin{pmatrix} 1\,2\,3\,4\,5 \\ 1\,2\,5\,4\,1 \end{pmatrix}$ (D) $\begin{pmatrix} 1\,2\,3\,4\,5 \\ 1\,2\,3\,4\,5 \end{pmatrix}$

73. If number of left cosets of H in G are n and the number of right cosets of H in G are m then—
(A) $m = n$ (B) $m \geq n$
(C) $m \leq n$ (D) None of these

74. If H is a subgroup of finite group G and order of H and G are respectively m and n, then—
(A) $m|n$ (B) $n|m$
(C) $m \times n$ (D) None of these

75. If G is a finite group of order n then for every $a \in$ G, we have—
(A) $a^n = e$, an identity element
(B) $a^n = a^1$
(C) $a^n = a$
(D) None of these

76. If H_1 and H_2 are two subgroups of G, then following is also a subgroup of G—
(A) $H_1 \cap H_2$ (B) $H_1 \cup H_2$
(C) H_1H_2 (D) None of these

77. The set M of square matrices (of same order) with respect to matrix multiplication is—
(A) Group (B) Semi-group
(C) Monoid (D) Quasi-group

78. If (G, *) is a group and $\forall\ a, b \in G\ b^{-1} * a^{-1} * b * a = e$, then G is—
(A) Abelian group (B) Non-Abelian
(C) Ring (D) Field

79. If G is a group such that $a^2 = e$, $\forall\ a \in G$, then G is—
(A) Abelian group
(B) Non-Abelian group
(C) Ring
(D) Field

80. If $f = (23)$ and $g = (45)$ are two permutations on 1, 2, 3, 4, 5 then fg is—
(A) $\begin{pmatrix} 1\,2\,3\,4\,5 \\ 1\,3\,2\,5\,4 \end{pmatrix}$ (B) $\begin{pmatrix} 1\,2\,3\,4\,5 \\ 1\,2\,2\,5\,6 \end{pmatrix}$
(C) $\begin{pmatrix} 1\,2\,3\,4\,5 \\ 1\,2\,4\,5\,6 \end{pmatrix}$ (D) $\begin{pmatrix} 1\,2\,3\,4\,5 \\ 1\,2\,3\,4\,5 \end{pmatrix}$

81. If n is the order of element a of group G, then $a^m = e$, an identity element iff—
(A) $m|n$ (B) $n|n$
(C) $m \times n$ (D) $n \times m$

82. The order of identity element in a group G is—
(A) One
(B) Zero
(C) Order of group
(D) Less than order of group

83. If $a, a^{-1} \in$ G a group and order of a and a^{-1} are m and n respectively, then—
(A) $m > n$ (B) $m < n$
(C) $m = n$ (D) None of these

84. If $a, b \in$ G a group of order m, then order of ab and ba are—
(A) Same (B) Equal to m
(C) Unequal (D) None of these

85. If G = {1, –1} is a group, then order of 1 is—
(A) One (B) Two
(C) Zero (D) None of these

86. The product of permutations (123) (243) (134) is equal to—
(A) I (B) $\begin{pmatrix} 1\,2\,3\,4 \\ 5\,6\,2\,1 \end{pmatrix}$
(C) $\begin{pmatrix} 1\,2\,5\,1 \\ 1\,6\,5\,1 \end{pmatrix}$ (D) $\begin{pmatrix} 1\,2\,5\,3 \\ 1\,2\,3\,4 \end{pmatrix}$

87. The permutation $\begin{pmatrix} 1\,2\,5\,3\,4 \\ 3\,4\,1\,5\,2 \end{pmatrix}$ is equal to—
(A) (15) (13) (24) (B) (1) (2) (3)
(C) (135) (56) (D) (142) (53)

88. Given the permutation $c = (1234567)$, then c^3 is—
(A) (135724) (B) (1473625)
(C) (1765432) (D) I

89. If $c = (1234)$, then c^3 is—
(A) (13) (24) (B) (13)
(C) (24) (D) (23) (31)

90. Statement A : All cyclic group are Abelian statement B : The order of cyclic group is same as the order of its generator—
(A) A and B are false
(B) A is true, B is false
(C) B is true, A is false
(D) A and B are true

91. Statement A : Every isomorphic image of a cyclic group is cyclic.
Statement B : Every homomorphic image of a cyclic group is cyclic
(A) Both A and B are true
(B) Both A and B are false
(C) A is true only
(D) B is true only

92. A element ap of a finite cyclic group G of order n is a generator of G iff $0 < p < n$ and also—
(A) P is prime to n
(B) P is the multiple of n
(C) n is the multiple of n
(D) None of these

93. If G is a finite group of order n, $a \in$ G and order of a is m, if is cyclic, then—

(A) $m = n$ (B) $m > n$
(C) $m < n$ (D) None of these

94. If $a \in G$ is a generator of a cyclic group and order of a is $n < \infty$, then order of a cyclic group m is—
(A) Infinity (B) $m = n$
(C) $m > n$ (D) $m < n$

95. If e_1 and e_2 are two identity elements of a group G, then—
(A) $e_1 = e_2$
(B) $e_1 \neq e_2$
(C) $e_1 = ce_2$, for some
(D) None of these

96. The idempotent element in a group are—
(A) Inverse elements
(B) Identity element of a group
(C) Any element of a group
(D) None of these

97. Let $G = \{1 \; -1\}$, then under ordinary multiplication (G) is—
(A) Monoid (B) Semi-group
(C) Quasi-group (D) Group

98. Let G be a set of rational numbers then under ordinary addition (Q +) is—
(A) Monoid (B) Semi-group
(C) Quasi-group (D) Group

99. Let G be a group of square matrices of same order with respect to matrix multiplication then it is not a—
(A) Quasi-group (B) Abelian group
(C) Semi-group (D) None of these

100. If G is a finite group, then for every $a \in G$ the order of a is—
(A) Finite (B) Infinite
(C) Zero (D) None of these

101. In the additive of integers, the order of every element $a \neq 0$ is—
(A) Infinity (B) One
(C) Zero (D) None of these

102. In the additive group of integers, the order of identity element is—
(A) Zero (B) One
(C) Infinity (D) None of these

103. In the additive group G of integers, the order of inverse element a^{-1}, $\forall a \in G$ is—
(A) Zero (B) One
(C) Infinity (D) None of these

104. The singleton {0} with binary operations additive and multiplication is ring and it is called—
(A) Zero ring (B) Division ring
(C) Singleton ring (D) None of these

105. The element $a \neq 0 \in R$, the commutative ring is an integral domain if—
(A) $ab = 0, b \in R$ and $b = 0$
(B) $ab = 0, b \in R$ and $b \neq 0$
(C) $ab \neq 0 \; b \in R$ and $b = 0$
(D) $ab = 0, b \in R$ and $b = 0$

106. A ring R is an integral domain if—
(A) R is commutative ring
(B) R is commutative ring with zero divisor
(C) R is commutative ring with non-zero divisor
(D) R is a ring with zero divisor

107. A ring R with binary operation addition is an Abelian group. It with binary operation multiplication, $\forall a, b \in R, a{\cdot}b = b{\cdot}a$, then R is—
(A) Commutative ring
(B) Integral domain
(C) Field
(D) Null ring

108. An integral domain D is of characteristic zero if—
(A) $ma = 0, a \neq 0 \in D \rightarrow m = 0$
(B) $ma = 0{\cdot}a \neq 0 \in D \rightarrow m \neq 0$
(C) $ma = 0 \; a \neq 0 \in D \rightarrow m = a$
(D) $ma = 0 \; a \neq 0 \in D \rightarrow m \neq a$

109. E is the set of even integers under ordinary addition and multiplication, then E is a ring, E is also a—
(A) Commutative ring
(B) Integral domain
(C) Field
(D) None of these

110. I is the set of integers and define $a \oplus b = a + b + 1$ and $a \odot b = a + b + ab$, then the ring $\{I \oplus \cdot \odot\}$ is—

(A) Commutative (B) Integral domain
(C) Field (D) None of these

111. If the ring R has left identity e_1 and right, identity e_2, then—
(A) $e_1 = e_2$ (B) $e_1 \neq e_2$
(C) $e_1 = me_2$ (D) None of these

112. If a ring R $\neq \{0\}$ has the multiplicative identity, then—
(A) $1 > 0$ (B) $1 = 0$
(C) $1 \neq 0$ (D) None of these

113. If the ring R has unites e_1 and e_2, then—
(A) $e_1 = e_2$ (B) $e_1 = me_2$
(C) $e_1 = e_2$ (D) None of these

114. A ring (R, +,) is said to have zero divisor if—
(A) $a, b \in$ R, $ab = 0 \rightarrow a \neq 0$ or $b \neq 0$
(B) $a, b \in$ R $a \cdot b = 0 \rightarrow a \neq 0$ and $b \neq 0$
(C) $a, b \in$ R $a \cdot b = 0 \rightarrow a = 0$ or $b = 0$
(D) $a, b \in$ R, $a \cdot b = 0 \rightarrow a = 0$ and $b = 0$

115. A ring (R +) is said to have a ring without rero divisor if—
(A) $ab \in$ R, $a \cdot b = 0 \rightarrow a \neq 0$ or $b \neq 0$
(B) $a, b \in$ R, $a \cdot b = 0 \rightarrow a \neq 0$ and $b \neq 0$
(C) $a, b \in$ R $= 0 \rightarrow a = 0$ or $b = 0$ or both are zero
(D) $a, b \in$ R, $a \cdot b = 0 \rightarrow a = 0$ and $b \neq 0$

116. An element $a \in$ (R, +,) a ring is nilpotent if for some positive integer n—
(A) $a^n = 0$ (B) $a^n = a$
(C) $a^n = 1$ (D) None of these

117. The non zero elements a, b of ring (R, +) are called zero divisors if—
(A) $a \cdot b = 0$ (B) $a \cdot b = 1$
(C) $a \cdot b \neq 0$ (D) $a \cdot b \neq 1$

118. A skew field have—
(A) Non-zero divisors
(B) Zero divisors
(C) a, b $a \cdot b = 0 : a \neq 0, b \neq 0$
(D) None of these

119. The following statement is false—
(A) The intersection of two non-empty sub-ring is a sub-ring
(B) The intersection of two non-empty sub-group is a sub-group
(C) A skew field have zero divisors
(D) An integral domain have zero divisors

120. If f is an isomorphism of a ring (R_1 +,) onto a ring (R_1 + , ·) and
(a) Isomorphic image of a field is a field
(b) Isomorphic image of a division ring is a division ring
(c) Isomorphic image of a ring with unity, is a ring with unity

then—
(A) a, b, c are true
(B) a and b are false
(C) b and c are false
(D) a is false

121. A field having no proper subfield is—
(A) Prime field
(B) Division ring
(C) Integral domain
(D) None of these

122. Every finite integral of domain is—
(A) Of finite characteristic
(B) Of not finite characteristic
(C) Not a field
(D) None of these

123. Let (D, + ·) is an integral domain D is a field if—
(A) For $\forall a \in$ D, there exist $a^{-1} \in$ D : $aa^{-1} = 1$
(B) For $\forall a \in$ D, there exist $a^{-1} \in$ D : $a + a^{-1} = 0$
(C) For $\forall a \in$ D, there exist $b \in$ D : $ab = 0$
(D) None of these

124. The set of rational numbers Q with ordinary addition and multiplication is a commutative ring with unit element it is a field if for $\frac{a}{b} \in$ G
There exist—
(A) $a + b \in$ Q (B) $\frac{b}{a} \in$ Q
(C) $ab \in$ Q (D) None of these

125. The set C of complex number of the form $x + iy$ is a field with respect to ordinary addition and multiplication, then the unit and zero elements are respectively—

(A) $1 + i0$ and $0 + i0$
(B) $0 + i$ and $1 + i0$
(C) 0 and 1
(D) i and $-i$

126. If $C = \{x + iy : xy \in R, i = \sqrt{-1}\}$ is a field with respect to ordinary addition and multiplication, then the multiplication inverse of non-zero element of $a + ib \in C$ is—
(A) $a + b$
(B) $\left(\frac{a}{a^2 + b^2}\right) + i\left(\frac{-b}{a^2 + b^2}\right)$
(C) $\frac{a + ib}{a^2 + b^2}$
(D) None of these

127. If in a ring with unity $(xy)^2 = x^2y^2, \forall x, y = \in R$, then—
(A) R is a commutative ring
(B) R is an integral domain
(C) R is field
(D) None of these

128. Every non-zero nilpotent element of the ring R is—
(A) Zero divisor
(B) Non-zero divisor
(C) Unity
(D) $AB \neq 0$

129. $A = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$ and $B = \begin{bmatrix} 1 & 0 \\ -1 & 0 \end{bmatrix}$ are—
(A) Zero-divisors
(B) Non-zero divisors
(C) $A = 0$ or $B = 0$
(D) $AB \neq 0$

130. If a_1^{-1}, a_2^{-1} are two multiplicative inverse of non-zero elements $a \in F$, a field then—
(A) $a_1^{-1} \neq a_2^{-1}$ (B) $a_1^{-1} = a_2^{-1}$
(C) $a_1^{-1} < a_2^{-1}$ (D) None of these

131. The following statement is false—
(A) Every field is an integral domain
(B) Every integral domain is a field
(C) Every field is a ring
(D) Every ring is a group

132. The following statement is false—
(A) Every field is an integral domain
(B) Every finite integral domain is a field
(C) Every field is a ring
(D) Every integral domain is a field

133. A field is defined as—
(A) Division ring
(B) Commutative ring
(C) Integral domain
(D) Finite integral domain

134. A commutative ring R with unity is called integral domain if $a, b \in R$—
(A) $ab = 0 \rightarrow a \neq 0, b \neq 0$
(B) $ab = 0 \rightarrow a = 0 \cdot b = 0$
(C) $ab = 0 \rightarrow a = b$
(D) None of these

135. If $a, b \in D$, D is an ordered set than following is true—
(A) $a > b \rightarrow a > -b$
(B) $a > 0 \rightarrow ab > ac \rightarrow b < c$
(C) $a > b \rightarrow -a < -b$
(D) $a \geq |a|$

136. The generators of the group $G = \{a, a^2, a^3, a^4 = e\}$ are—
(A) a only (B) a and a^2
(C) a and a^3 (D) a and a^4

137. If $G = \{1 \ -1\}$ is a group with ordinary multiplication the order of -1 is—
(A) One (B) Two
(C) Zero (D) None of these

138. The ring of complex numbers $C = \{x + iy : x\,y$ are real number $i = \sqrt{-1}\}$ is—
(A) Not an integral domain
(B) An integral domain
(C) Ordered set
(D) None of these

139. If is an integral domain and $a \neq 0 \in I$, then—
(A) $a^2 = 0$ (B) $a^2 \geq 0$
(C) $a^2 \neq 0$ (D) None of these

140. If $a, b \in D$, where D is an ordered set, then the following is false—
(A) $a < b \rightarrow -a > -b$
(B) $(ab) = |a|\,|b|$
(C) $-|a| \leq a \leq |a|$
(D) $|a + b| \geq |a| + |b|$

141. Let R and R be two arbitrary ring $\phi : R \to R$ defined as $\phi(a) = 0$ for all $a \in R$, then—
 (A) ϕ is homomorphism
 (B) ϕ is automorphism
 (C) ϕ is isomorphism
 (D) None of these

142. The homomorphism ϕ of rings R into R is an isomorphism iff the Kernel I (ϕ) is—
 (A) $I(\phi) = (0)$ (B) $I(\phi) = R$
 (C) $I(\phi) \neq R$ (D) None of these

143. Let R be a ring $U \neq \phi \subset R$ is ideal of then—
 A : U is a subgroup of R under addition
 B : $\forall u \in U$ and $r \in R$, ur, $ru \in U$
 (A) A and B both are true
 (B) Only A is true
 (C) Only B is true
 (D) Both A and B are false

144. If U is an ideal of ring R, then—
 (A) U/R is a ring (B) R/U is a ring
 (C) RU is a ring (D) None of these

145. An ideal $M \neq R$ in a ring R is maximal ideal of R if U is an ideal of Q and $M \subset U \subset R$, then—
 (A) Either M = U or R = U
 (B) M = U = R
 (C) $M = U \neq R$
 (D) $M \neq U + R$

146. A field is a—
 (A) Vector space
 (B) Integral domain
 (C) Division ring
 (D) Commutative division ring

147. An integral domain D is of finite characteristic, if $\forall a \in D$ there exist m a positive integer such that—
 (A) $ma = 1$ (B) $ma = 0$
 (C) $ma = a$ (D) None of these

148. If integral domain D is of finite characteristic, then its characteristic is—
 (A) Odd number (B) Even number
 (C) Prime number (D) Natural number

149. If integral domain I is of finite characteristic, then—
 (A) I is finite only
 (B) I is infinite only
 (C) I is finite or infinite
 (D) None of these

150. A : F is a field
 B : F an integral domain—
 (A) $A \to B$ (B) $B \to A$
 (C) $A \leftrightarrow B$ (D) $A \not\leftrightarrow B$

151. A commutative division ring is—
 (A) Vector space
 (B) Group
 (C) Integral domain
 (D) Field

152. A commutative division ring is—
 (A) Finite integral domain
 (B) Integral domain
 (C) Zero ring
 (D) None of these

153. If R is a commutative ring with unit element M is maximum ideal of iff—
 (A) R/M is a field (B) M/R is a field
 (C) RM is a field (D) None of these

154. If F is field then its only ideals are—
 (a) F, a field itself
 (b) (0)
 (A) (a) and (b) are true
 (B) (a) is true (b) is false
 (C) (a) is false (b) is true
 (D) (a) and (b) false

155. If U is an ideal of ring R and $1 \in U$, then—
 (A) U is a proper subset of R
 (B) U is equal to R
 (C) U is a super set of R
 (D) $U = \phi$

156. Let R is commutative ring with unit element whose only ideals are (0) and R itself, then—
 (A) R is finite integral domain
 (B) R is integral domain
 (C) Division ring
 (D) None of these

157. If R is a commutative ring with unit element M is an ideal of and R/M is finite integral domain, then—

(A) M is a maximal ideal of R
(B) M is not a maximal ideal of R
(C) M is minimal ideal or R
(D) None of these

158. If R is an Eudidean ring and $a, b \in$ R. If $b \neq 0$ is not a unit in R, then—
(A) $d(a) < d(ab)$ (B) $d(a) > d(ab)$
(C) $d(a) = d(ab)$ (D) None of these

159. If r is a prime element in Eudidean ring R and r/ab $a, b \in$ R then—
(A) $x \times a$ or $r \times b$
(B) $r \times a$ and $x \times b$
(C) $ab \neq mr$ for some $m \in$ R
(D) None of these

160. If $f\,x)$ and $g\,(x)$ are two polynomials, then—
(A) deg $(f(x)\,g(x)) \leq$ deg $f(x)$, $g(x) \neq 0$
(B) deg $(f(x)\,g(x) \geq$ deg $f(x)$, $g(x) \neq 0$
(C) deg $(f(x)\,g(x)$ = deg $f(x)$ deg $g(x)$, $g(x) \neq 0$
(D) deg $(f(x)\,g(x)$ = deg $f(x)$ – deg $g(x)$ $g(x) \neq 0$

161. Given a polynomial $f(x) = a_0 + a_1x + \ldots + a_nx^n$ where as are integer, then content of $f(x)$ is—
(A) $g.c.d.$ of integers $a_0 \ldots a_n$
(B) Mean of integers $a_0 \ldots, a_n$
(C) Mode of integers $a_0 \ldots a_n$
(D) None of these

162. If R is a commutative ring, with unit element then—
(A) Every maximal ideal is prime ideal
(B) Every prime ideal is maximal ideal
(C) Every ideal is prime ideal
(D) Every ideal is maximal

163. If R is an integral domain with unit element, then—
(A) R $[x]$ is not a commutative ring
(B) R $[x]$ have a unit element
(C) Any unit in R $[x]$ is unit in R
(D) Any unit in R $[x]$ is not an unit in R

164. If K is an extension of F, then degree of K over F is—
(A) Dimension of K as vector space over F
(B) Number of element in K as vector space over F
(C) Degree of K
(D) Order of K

165. The set of all even integers is ring it is also a—
(A) Commutative ring
(B) Integral domain
(C) Field
(D) None of these

166. Every integral domain is not a—
(A) Field
(B) Commutative ring
(C) Ring
(D) Abelian group with respect to addition

167. I is an ordered integral domain and $a, b \in$ I, if $a > b$, then—
(A) $a + c \geq b + c$, $\forall c \in$ I
(B) $a + c \leq b + c$, $\forall c \in$ I
(C) $a + c < b + c$, $\forall c \in$ I
(D) $a + c > b + c$, $\forall c \in$ I

168. If R is ring in which $a^4 = a$, $\forall a \in$ R, then—
(A) R is commutative
(B) R is not commutative
(C) R is zero ring
(D) None of these

169. If the ring R is such that $(ab^2) = a^2b^2$, $ab \in$ R, then—
(A) R is commutative
(B) R is non commutative
(C) R is zero ring
(D) None of these

170. Given the polynomial P $(x) = a_0 + a_1x + \ldots + a_mx^m$ its degree is m if—
(A) $a_m = 0$ (B) $a_m \neq 0$
(C) $a_m^{-1} = 0$ (D) $a_m^{-1} \neq 0$

171. If $f(x)$ and $g(x)$ are two non-zero polynomials of $f\,[x]$ then—
(A) deg $(f(x)\,g(x))$ = deg = $(f(x)$ deg $(g(x))$
(B) deg $(f(x))$ = deg $f(x)$ + deg $g(x)$
(C) deg $(f(x)$ = deg $f(x)$ – deg $g(x)$
(D) deg $(f(x)$ = deg $f(x)$ + deg $g(x)$

172. The polynomial $f(x) = a_0 + a_1x + a_2x + \ldots + a_nx^n$ where $a_0, a_1 \ldots\ldots, a_n$ are integers, is primitive polynomial if—

(A) $g.c.\ d$ of $(a_0 \ldots\ldots a_n) = 0$
(B) $g.c.d$ of $(a_0 \ldots\ldots a_n) = 1$
(C) $g.c.d.$ of $(a_0 \ldots\ldots a_n) = 2$
(D) $g.c.d.$ of $(a_0 \ldots\ldots a_n) =$ prime number

173. A polynomial is said to be integer monic if—
(A) Its coefficients are integers and highest coefficient is 1
(B) Its coefficients are real numbers and highest coefficient is 0
(C) Its coefficients are real numbers and highest coefficient 0
(D) Its coefficients are integers and highest coefficients is 2

174. An integers monic polynomial is a—
(A) Primitive polynomial
(B) Non primitive polynomial
(C) Polynomial with lowest coefficient as 1
(D) Polynomial without lowest coefficient as 1

175. Let R is a commutative ring with unit element whose only ideals are (0) and R itself, then—
(A) R is integral domain
(B) R is field
(C) Division ring
(D) None of these

176. Which of the following statement is false ?
(A) F $[x]$ is an integral domain
(B) F $[x]$ is Eudidean ring
(C) F $[x]$ principal ideal ring
(D) F $[x]$ is not a group

177. A polynomials $f(x)$ and $g(x)$ are primitive polynomial, then—
(A) $f(x)\, g(x)$ is a primitive polynomial
(B) $f(x) + g(x)$ is primitive polynomial
(C) $f(x) - g(x)$ is a primitive polynomial
(D) $f(x)/g(x)$ is a primitive polynomial

178. If the ring R is an integral domain, then—
(A) R $[x]$ is an integral domain
(B) R $[x]$ is not an integral domain
(C) R $[x]$ is a field
(D) None of these

179. If the ring R is finite and commutative with unit element, then—
(A) Every prime ideal is a maximal ideal
(B) Every ideal is maximal ideal
(C) Every maximal ideal is prime ideal
(D) (A) and (C) are both true

180. If is a finite extension of K and K is a finite extension of field F, then—
(A) F is a finite extension of L
(B) L is a finite extension of F
(C) K is a subfield of F
(D) L is subfield of K

181. If is a finite extension of F and K is a sub field of L which contains F, then—
(A) [L : F] [K : F] (B) [K : F]/[L : F]
(C) [K : F]/[F : L] (D) [F : K]/[L : F]

182. If K is an extension of F and $a \in$ K, F (a) is a finite extension, then—
(A) a is algebraic over F
(B) a is not algebraic over F
(C) F (a) is the largest subfield of K
(D) None of these

183. If a and b in K (where K is an extension of field F) are algebraic over F of degree m and n respectively, the following is false—
(A) ab is algebraic over F
(B) $a + b$ is algebraic over F
(C) $a - b$ is algebraic over F
(D) None of these

184. If F is a subfield of L and K is a subfield of L which contains F, then—
(A) [K : F]/[L : F] (B) [K : F] $\times$ [L : F]
(C) [F : K]/[F : L] (D) [F : K] $\times$ [F : L]

185. An element $a \in$ K is algebraic over field F if for $a_0 \ldots a_n \in$ F all not zero—
(A) $a_0a^n + a_1a^{n-1} + \ldots + a_n \neq 0$
(B) $a_0a^n + a_1a^{n-1} + \ldots + a_na^{n-1} = 0$
(C) $a_0a^n + a_1a^{n-1} + \ldots + a_n = 0$
(D) $a_0a^n + a_1a^{n-1} + \ldots + a_n = 0$

186. If K is an extension of field F and $a \in$ K is algebraic over F if—
(A) F (a) is an extension of F
(B) F (a) is a subfield of F
(C) F (a) is a finite extension of F
(D) F (a) is infinite of F

187. If K is an extension of field F and $a \in$ K is algebraic of degree n over F, then—

(A) $[F(a) : F] = n$ (B) $[F(a) : K] = n$
(C) $[K : F(a)] = n$ (D) $[F : F(a)] = n$

188. The extension K of field F is an algebraic extension of F—

(A) Every element $a \in$ K is algebraic over F
(B) For some $a \in$ K is algebraic over F
(C) Zero element is algebraic over F
(D) None of these

189. A complex number is algebraic number if—

(A) It is algebraic over real numbers
(B) It is algebraic over rational numbers
(C) It is algebraic over integers
(D) It is algebraic over natural numbers

190. If $f(x) \in F[x]$, then there is a finite extension E of F such that—

(A) $[E : F] \leq \deg, f(x)$
(B) $[E : F] \geq \deg f(x)$
(C) $[F : E] \geq \deg f(x)$
(D) $[F : E] \leq \deg f(x)$

191. If I is a ideal in a ring R them—

(A) R/I is a ring (B) RI is a ring
(C) R + I is a ring (D) RI is a ring

192. Let S be a non-empty set. Any function o from S × S to S is called a.........., if $o : S \times S \to S$, defined as $o(ab) = a_o b \in S, \forall a, b \in S$.

(A) Unary (B) Binary
(C) Quardraut (D) None of these

193. Let S be a non empty set. Let o be an operation on S then (S, o) is a .... structure—

(A) Mathematical (B) Trigonometrical
(C) Differential (D) None of these

194. Mathematical structure (S, o) is said to be … if o is binary operation *i.e.*, $\forall a, b \in S \Rightarrow aob \in S$—

(A) Groupoid (B) Monoid
(C) Semi-group (D) None of these

195. A groupoid (S, o) is … if o is associative *i.e.*, $(aob)\, oc = ao\, (boc), \forall a, b, c \in S$—

(A) Group (B) Monoid
(C) Semi-group (D) None of these

196. If identity element $e \in$ S exists in a semi-group (S, o), then it is …, *i.e.*, $\forall a \in S, \exists e \in S : aoe = a = e^o a$—

(A) Group (B) Monoid
(C) Groupoid (D) None of these

197. If inverse element exists for every element in a monoid (S, o), then it is a …, *i.e.*, $\forall a \in S, \exists a^{-1} \in S : aoa^{-1} = e = a^{-1}\, {}^o a$.

(A) Group (B) Monoid
(C) Semi-group (D) None of these

198. A group (S, o), is a … if $\forall a, b \in S$, $aob = boa$—

(A) Commutative group
(B) Monoid
(C) Semi-group
(D) None of these

199. A commutative group is known as—

(A) Abelian group (B) Monoid
(C) Semi-group (D) None of these

200. 1. Identity element in a group is unique.
2. Inverse of each element of a group is unique

(A) 1 is true only
(B) 2 is true only
(C) Both 1 and 2 are true
(D) None 1 and 2 are true

201. If $a, b \in$ G a group, then $(ab)^{-1} = b^{-1} a^{-1}$. This law is known as—

(A) Reversal rule
(B) Closure rule
(C) Associative rule
(D) None of these

202. Let G be a group. Let $a \in$ G, then n is called … denoted by $o(a) = n$, if $a^n = e$, where n is least positive integer—

(A) Order of element a
(B) Order of group G
(C) Both (A) and (B)
(D) None of these

203. 1. The order of every element of finite group is infinite.
2. If their is no positive integer n such that $a^n = e$, then order of a $o(a)$ is infinite or zero.

(A) Only 1 is true
(B) Both 1 and 2 are true
(C) Only 2 is true
(D) None of 1 and 2 are true

204. 1. The order of every element of finite group is less than or equal to the order of the group.
2. The order of an element of a group is same as that of its inverse.
3. Order of any integral power of an element $a \in G$ cannot exceed the order of a.
(A) Only 1 is true (B) Only 3 is true
(C) Only 2 is true (D) All 1, 2, 3 are true

205. If $a, b \ldots \in G$ a group and $(abc \ldots z)^{-1} = z^{-1} \ldots c^{-1}b^{-1}a^{-1}$. This law is known as—
(A) Reversal rule
(B) Closure rule
(C) Associative rule
(D) None of these

206. A group G is called …… if for some $a \in G$ every element $x = G$ is of the form $x = a^n$, where n is some integer—
(A) Cyclic (B) Ring
(C) Abelian (D) None of these

207. There may be …… generator of a cyclic group—
(A) More than one (B) No
(C) Only one (D) Maximum two

208. 1. Every cyclic group is an abelian group.
2. The order of cyclic group is same as the order of its generator.
(A) Only 1 is true
(B) Both 1 and 2 are true
(C) Only 2 is true
(D) None of 1 and 2 is true

209. 1. If a is a generator of a cyclic group G, then a^{-1} is also generator of G.
2. The generator of cyclic group of order n are all elements a^p, p being prime to n and
$O < P < n$.
(A) Only 1 is true
(B) Both 1 and 2 are true
(C) Only 2 is true
(D) None of 1 and 2 is true

210. Every group of …… order is cyclic—
(A) Prime (B) Odd
(C) Even (D) Any

211. 1. If G is finite group of order n and contains a such that $o(a) = n$, then G is cyclic group.
2. If a cyclic group G is generated by an element a of order n, then a^m is a generator of G, iff ged of m and n is 1.
3. Every group of order 3 is cyclic.
(A) Only 1 is true (B) Only 3 is true
(C) Only 2 is true (D) All 1, 2, 3 are true

212. 1. An Abelian group of order six is cyclic.
2. If a cyclic group G is generated by an element a, $o(G) = n$, then

$$a' \in G, a' = \begin{cases} a^0 - a^n = e, & i = 0, n \\ a' & i < n \\ a^{1-n} & i > n \end{cases}$$

(A) Only 1 is true
(B) Both 1 and 2 are true
(C) Only 2 is true
(D) None of 1 and 2 is true

213. A permutation is said to be an … permutation if it can be expressed as a product of an even number of transpositions, otherwise it is an … permutation—
(A) Even, even (B) Even, odd
(C) Odd, odd (D) Odd, even

214. Every permutation can be expressed as a product of transpositions in … many ways—
(A) Infinitely
(B) Finitely
(C) Both (A) and (B)
(D) None of these

215. 1. A permutation can not be both even or odd *i.e.*, permutation f is expressed as product of transpositions, then the number of transpositions is either always even or always odd.
2. Identity permutation is always an even permutation.
(A) Only 1 is true
(B) Both 1 and 2 are true
(C) Only 2 is true
(D) None of 1 and 2 is true

216. 1. The product of two even permutations is an even permutations.
    2. The product of two odd permutations is an even permutation.
    (A) Only 1 is true
    (B) Both 1 and 2 are true
    (C) Only 2 is true
    (D) None of 1 and 2 is true

217. The product of an even permutation and an odd permutation is …… permutation.
    (A) Even
    (B) Odd
    (C) Both (A) and (B)
    (D) None of these

218. The inverse of an even permutation is …… permutation.
    (A) Even
    (B) Odd
    (C) Both (A) and (B)
    (D) None of these

219. The inverse of an odd permutation is an …… permutation.
    (A) Even
    (B) Odd
    (C) Both (A) and (B)
    (D) None of these

220. 1. A cycle of length n can be expressed as the product of $n-1$ transpositions.
    2. Out of n ! permutation on n symbols $\frac{1}{2}n$! are even and $\frac{1}{2}n$! are odd—
    (A) Only 1 is true
    (B) Both 1 and 2 are true
    (C) Only 2 is true
    (D) None of 1 and 2 is true

221. The product of two odd permutations is an ………… permutation—
    (A) Even
    (B) Odd
    (C) Both (A) and (B)
    (D) None of these

222. A permutation is even if it can be expressed as a product of an ………… number of transpositions—
    (A) Even
    (B) Odd
    (C) Both (A) and (B)
    (D) None of these

223. A permutation is odd if it can be expressed as a product of an …… number of transpositions—
    (A) Even
    (B) Odd
    (C) Both (A) and (B)
    (D) None of these

224. Identity permutation is always …… permutation—
    (A) Even
    (B) Odd
    (C) Both (A) and (B)
    (D) None of these

225. 1. If G and G' are isomorphic groups, the identity elements in the groups does not correspond to one another.
    2. If a and b are corresponding elements of two isomorphic groups, then a^{-1} corresponds to b^{-1}.
    (A) Only 1 is true
    (B) Both 1 and 2 are true
    (C) Only 2 is true
    (D) None of 1 and 2 are true

226. 1. All groups which are isomorphic to a given group are isomorphic to each other.
    2. All cyclic groups of the same order are isomorphic to each other.
    3. A cyclic group G with generator of finite order n is isomorphic to the multiplicative group of n, nth root of unity.
    (A) Only 1 is true
    (B) Only 3 is true
    (C) Only 2 is true
    (D) All 1, 2 and 3 are true

227. A non-empty subset H of a group G is said to be a …… of G. If under the operation defined on G. H itself forms a group—
    (A) Subgroup (B) Abelian group
    (C) Cyclic group (D) None of these

228. 1. Since every set is a subset of itself group G is a subgroup of itself called trivial subgroup.
   2. If e is the identity of G. then the subset of G containing only one element e is also a subgroup of G.
   3. If H is a subgroup of G and K is a subgroup of H, then K is also a subgroup of G and transitive law acts here.
   (A) Only 1 is true
   (B) Only 3 is true
   (C) Only 2 is true
   (D) All 1, 2 and 3 are true

229. A subset H of a group G is a subgroup of G if and only if (i) $a, b \in H \Rightarrow ab \in H$ (ii) $a \in H \Rightarrow a^{-1} \in H$, where a^{-1}, is the inverse of a in G—
   (A) (i) is true only
   (B) Both (i) and (ii) are true
   (C) (ii) is true only
   (D) None of these

230. 1. A necessary and sufficient condition for an on empty subset H of a group G to be a subgroup is that $a, b \in H \Rightarrow ab^{-1} \in H$ where b^{-1} the inverse of b in G.
   2. A necessary and sufficient condition for a non-empty finite subset H of a group G to be a sub-group is that H must be closed with respect to multiplication *i.e.*, $a, b \in H \Rightarrow ab \in H$.
   (A) 1 is true only
   (B) Both 1 and 2 are true
   (C) 2 is true only
   (D) None of these is true

231. 1. The identity of a subgroup is the same as that of the group.
   2. The inverse of any element of subgroup is the same as the inverse of the same regarded as an element of the group.
   3. The intersection of two subgroup of a group G is a subgroup of G.
   (A) 1 is true only
   (B) 3 is true only
   (C) 2 is true only
   (D) All 1, 2 and 3 are true

232. 1. The union of two subgroups is not necessarily a subgroup.
   2. The union of two subgroups is a subgroup. If and only if one is contained in the other.
   3. A subgroup of a cyclic group is also cyclic.
   (A) 1 is true only
   (B) 3 is true only
   (C) 2 is true only
   (D) All 1, 2 and 3 are true

233. 1. Every proper subgroup of an infinite cyclic group is finite.
   2. A subgroup of an abelian group is not abelian.
   3. If G if finite cyclic group of order n and m is divisor of n, then there exists one and only one subgroup of order m which is also cyclic.
   (A) 1 is true only
   (B) 3 is true only
   (C) 2 is true only
   (D) All 1, 2 and 3 are true

234. 1. Every abelian group has abelian subgroups.
   2. Every group G has two trivial subgroup *viz* $\{e\}$ and G itself.
   (A) 1 is true only
   (B) Both 1 and 2 are true
   (C) 2 is true only
   (D) None of these is true

235. 1. A non abelian group can have an abelian subgroup.
   2. A non abelian group can have a non abelian subgroup.
   3. Every finite group of composite order possesses proper subgroups.
   (A) 1 is true only
   (B) 3 is true only
   (C) 2 is true only
   (D) All 1, 2 and 3 are true

236. Let H be subgroup of G, then $\forall a \in G$. $Ha = \{ha : h \in H\}$ is called …… coset of in G and $aH = \{ah : h \in H\}$ is called left coset of H in G—

(A) Right, left (B) Left, right
(C) Right, right (D) Left, left

237. 1. If G is abelian group then $Ha = aH\ \forall a = \in G$.
2. H is also a left (right) coset of G as H = He, where e is identity of G.
(A) 1 is true only
(B) Both 1 and 2 are true
(C) 2 is true only
(D) None of these is true

238. (1) Let $a, b \in G$ (group) and $H \subseteq G$ (subgroup of G), then $a \in Hb \Leftrightarrow Ha = Hb$ and $a \in bH \Leftrightarrow aH = bH$.
(2) Any two right cosets of a subgroup are either disjoint or identical.
(A) 1 is true only
(B) Both 1 and 2 are true
(C) 2 is true only
(D) None of these is true

239. Cayley Theorem states—
(A) A finite group G is isomorphic to a permutation group
(B) Order of each subgroup of finite group is a divisor of the order of the group
(C) If P is prime number and a is any integer, then $a^p = a\ (mod p)$
(D) None of these

240. Fermat Theorem states—
(A) A finite group G is isomorphic to a permutation group
(B) Order of each subgroup of a finite group is a divisor of the order of the group
(C) If P is prime number and a any integer the $a^p = a\ (mod\ p)$
(D) None of these

241. Lagrange's Theorem states—
(A) A finite group G is isomorphic to a permutation group
(B) Order of each subgroup of a finite group is a divisor of the order of the group
(C) If P is prime number and a is any integer, then $a^p = a\ (mod p)$
(D) None of these

242. 1. If G is finite group and $a \in G$, then order of a divides the order of G.
2. If G is a finite group and $a \in G$, then $a^{\circ(G)} = e$.
(A) 1 is true only
(B) Both 1 and 2 are true
(C) 2 is true only
(D) None of these is true

243. 1. If G is a finite group where order is a prime number then G is a Cyclic group.
2. The order of every element of a finite group is a divisor of the order of the group.
(A) 1 is true only
(B) Both 1 and 2 are true
(C) 2 is true only
(D) None of these

244. A subgroup H of a group G is said to be *a* …… of G, if for every $x \in G$ and for every $h \in H$, $xhx^{-1} \in H$.
(A) Normal subgroup
(B) Simple group
(C) Abelian subgroup
(D) None of these

245. A group having no proper normal subgroup is called a—
(A) Normal subgroup
(B) Abelian subgroup
(C) Simple group
(D) None of these

246. 1. Every group of prime order is not simple.
2. A subgroup H of a group G is normal, iff $\forall x \in G, xHx^{-1} = H$.
(A) 1 is true only
(B) Both 1 and 2 are true
(C) 2 is true only
(D) None of these is true

247. A subgroup H of a group G is a normal subgroup of G, iff the product of two right cosets of H in G is …… of H is G.
(A) Right coset
(B) Left coset
(C) Both (A) and (B)
(D) None of these

248. The intersection of any two normal subgroup of a group is—
   (A) Normal subgroup
   (B) Abelian subgroup
   (C) Simple group
   (D) None of these

249. Every subgroup of an Abelian group is—
   (A) Normal subgroup
   (B) Abelian subgroup
   (C) Simple subgroup
   (D) None of these

250. Every subgroup of a cyclic group is—
   (A) Normal subgroup
   (B) Abelian subgroup
   (C) Simple group
   (D) None of these

251. If H is a subgroup of G and N is a normal subgroup of G, then $H \cap N$ is …… of G.
   (A) Normal subgroup
   (B) Abelian subgroup
   (C) Simple group
   (D) None of these

252. If N is a …… of G and H is a subgroup of G, then NH is a subgroup of G.
   (A) Normal subgroup
   (B) Abelian subgroup
   (C) Simple group
   (D) None of these

253. If M and N are normal subgroup of G, then MN is also …… of G.
   (A) Normal subgroup
   (B) Abelian subgroup
   (C) Simple group
   (D) None of these

254. If H is the only subgroup of finite order m in the group G, then H is a …… of G.
   (A) Normal subgroup
   (B) Abelian subgroup
   (C) Simple group
   (D) None of these

255. If a cyclic subgroup N of G is normal in G, then every subgroup of N is …… in G.
   (A) Normal subgroup
   (B) Abelian subgroup
   (C) Simple group
   (D) None of these

256. 1. Every quotient group of an abelian group is abelian but converse is not true.
   2. Every quotient group of a cyclic group is cyclic but the converse is not true.
   3. If N is normal in G and $a \in$ G is of order n, then order of Na in G/N is a divisor of n.
   (A) 1 is true only (B) 3 is true only
   (C) 2 is true only (D) 1, 2, 3 are true

257. 1. A mapping f from a group G into a group G' is said to be homomorphism of G into G' if $f(ab) = f(ab) = f(a) f(b)$ $\forall a, b \in$ G.
   2. A mapping f from a group G onto a group G' is said to be homomorphism of G onto G' if $f(ab) = f(a) f(b)$ $\forall a, b \in$ G.
   (A) 1 is true only
   (B) Both 1 and 2 are true
   (C) 2 is true only
   (D) Now of 1 and 2 are true

258. Every ...... image of a group G is isomorphic to some quotient group of G—
   (A) Homomorphic (B) Automorphic
   (C) Isomorphic (D) None of these

259. Every .... image of an abelian group is abelian but converse is not true.
   (A) Homomorphic (B) Automorphic
   (C) Isomorphic (D) None of these

260. If f is .... mapping of a group G into a group G and $f(a)$ is homomorphic image of G in G′, then f(G) is a subgroup of G.
   (A) Homomorphic (B) Automorphic
   (C) Isomorphic (D) None of these

261. The necessary and sufficient condition for a .... f of a group G into G' with Kernel K to be isomorphic is that $K = \{e\}$.
   (A) Homomorphic (B) Automorphic
   (C) Isomorphic (D) None of these

262. A .... from a simple group is either trivial or one to one.

(A) Homomorphism
(B) Automorphism
(C) Isomorphism
(D) None of these

263. The set of all .... of a group forms a group with respect to composite of functions as the composition.
(A) Homomorphism
(B) Automorphism
(C) Isomorphism
(D) None of these

264. A normal subgroup H of a group G is said to be ...., if there exists no normal subgroup K of G which properly contains H.
(A) Normal subgroup
(B) Maximal subgroup
(C) Simple group
(D) None of these

265. Cauchy Theorem for Abelian group states—
(A) Suppose G is a finite abelian group and P/*o* (G) where P is a prime number. Then there is an element $a \neq e \in$ G, such that $a^P = e$
(B) A normal subgroup H of a group G is said to be maximal subgroup, if there exists no normal subgroup K of G which properly contains H
(C) Every homomorphic image of a group G is isomorphic to some quotient group of G
(D) None of these

266. General Cauchy theorem—
(A) Suppose G is a finite group and P/*o* (G), where P is a prime number. Then there is an element a in G such that $o(a) = P$
(B) Suppose G is a finite abelian group and P/o (G), where P is a prime number. Then there is an element $a \neq e \in$ G, such that $a^P = e$
(C) A normal subgroup H of a group G is said to be maximal subgroup, if there exists no normal subgroup K of G which properly contains H
(D) Every homomorphic image of a group G is isomorphic to some quotient group of G

267. For (R, + ;) closure law states—
(A) $\forall a, b \in R \Rightarrow a + b \in R$
(B) $(a + b) + c = a + (b + c) \; \forall a, b, c \in R$
(C) $\forall a \in R, \exists 0 \in R : a + 0 = a = 0 + a$
(D) None of these

268. For (R, + , .) associative law states—
(A) $\forall a, b \in R \Rightarrow a + b \in R$
(B) $(a + b) + c = a + (b + c), \forall a, b, c \in R$
(C) $\forall a \in R, \exists 0 \in R : a + 0 = a = 0 + a$
(D) None of these

269. For (R, +, .) existence of additive identity 0 states—
(A) $\forall a \cdot b \in R \Rightarrow a + b \in R$
(B) $(a + b) + c = a + (b + c) \; \forall a, b \cdot c \in R$
(C) $\forall a \in R, \exists 0 \in R : a + 0 = a = 0 + a$
(D) None of these

270. For (R, +, .) existence of additive inverse, states—
(A) $\forall a \in R, \exists -a \in R : a + (-a) = 0 = (-a) + a$
(B) $(a + b) + c = a + (b + c), \forall a, b, c \in R$
(C) $\forall a \in R, \exists 0 \in R : a + 0 = a = 0 + a$
(D) None of these

271. For (R, + , .) commutative law, states—
(A) $\forall a \in R, \exists -a \in R : a + (-a) = 0 = (-a) + a$
(B) $(a + b) + c = a + (b + c), \forall a, b, c \in R$
(C) $\forall a \in R, \exists 0 \in R : a + 0 = a = 0 + a$
(D) $\forall a, b \in R, a + b = b + a$

272. The ring (R, +, .) is called .... if in R multiplication is commutative, *i.e.*, $\forall a, b \in R, a \cdot b = b \cdot a$.
(A) Commutative ring
(B) Boolean ring
(C) Ring with unity
(D) None of these

273. The ring (R, +, .) is said to .... if there exist a multiplicative identity I $\in$ R, *i.e.*, $\forall a \in R, \exists 1 \in R : a \cdot 1 = a = 1 \cdot a$.
(A) Commutative ring
(B) Ring with unity
(C) Boolean ring
(D) None of these

274. A ring whose every element a is idempotent *i.e.*, $a^2 = a$ is known as ....
(A) Commutative ring
(B) Boolean ring
(C) Ring with unity
(D) None of these

275. If R is a commutative ring, then $a \neq 0 \in$ R is called a .... If there exist an element $b \neq 0 \in$ R such that $ab = 0$—
(A) Zero divisor (B) Prime divisor
(C) Single divisor (D) None of these

276. If in a ring R there exists non-zero elements $a \neq 0$, $b \neq 0 \in$ R such that $ab = 0$, then R is said to be a ring with—
(A) Zero divisor (B) Prime divisor
(C) Single divisor (D) None of these

277. If R be a ring, an element $a \neq 0 \in$ R called .... If $ab = 0$ for some non zero $b \neq 0 \in$ R.
(A) Left zero divisor
(B) Right zero divisor
(C) Both (A) and (B)
(D) None of these

278. If R be a ring, an element $a \neq 0 \in$ R is called ....if $ba = 0$ for some non zero $b \neq 0 \in$ R.
(A) Left zero divisor
(B) Right zero divisor
(C) Both (A) and (B)
(D) None of these

279. A ring R is said to be a ring .... if $ab = 0$, either $a = 0$ or $b = 0$, $a, b \in$ R—
(A) Without zero divisors
(B) With zero divisor
(C) Both (A) and (B)
(D) None of these

280. Let (R, +, .) be any ring and S a subring of R, then S is said to be a .... of R if $Sr \in$ S. $\forall r \in$ S, $\forall r \in$ R, S $\in$ S S and .... if rS $\in$ S, $\forall r \in$ R, S $\in$ S.
(A) Right ideal, left ideal
(B) Left ideal, left ideal
(C) Right ideal, right ideal
(D) Left ideal, right ideal

281. A non-empty subset S of R is said to be ideal of R, if—
(A) S is a subgroup of R under addition
(B) Both A and B
(C) Sr, rS $\in$ S, $\forall r \in$ R, S $\in$ S
(D) None of these

282. Let R be a commutative ring. An ideal P of ring R is said to be a .... if for $p, q \in$ R, $pq \in$ P $\Rightarrow$ P $\in$ P or $q \in$ P.
(A) Prime ideal of R
(B) Integral Domain
(C) Maximal ideal
(D) None of these

283. An ideal S $\neq$ R in a ring R is said to be a .... if whenever A is an ideal of R such that S $\subseteq$ A $\subseteq$ R, then either R = A or S = A.
(A) Prime ideal of R
(B) Integral domain
(C) Maximal ideal
(D) None of these

284. A commutative ring with unity is said to be an ...., if it is without zero divisors.
(A) Prime ideal of R
(B) Integral domain
(C) Maximal ideal
(D) None of these

285. An integral domain (D, +, .) is called an ordered integral domain, if D contains a subset D+ such that—
(A) D+ is closed with respect to addition and multiplication as defined on D
(B) If $a \in$ D, one and only one of the following is true : $a = 0$ or $a \in$ D+ or $-a \in$ D+
(C) Both A and B
(D) None of these

286. A commutative ring with unity is called a .... if its every non zero element possesses a multiplicative inverse.
(A) Field (B) Integral domain
(C) Group (D) None of these

287. A ring with unity is said to be .... or division ring if each non-zero element possesses multiplicative inverse.
(A) Skew field (B) Group
(C) Field (D) Integral domain

288. 1. Every field is also a division ring but every division ring is not a field.
   2. The multiplicative inverse of a non-zero element of a field is unique.
   3. A field is necessarily an integral domain.
   (A) Only 1 is true (B) Only 3 is true
   (C) One 2 is true (D) All 1, 2, 3 are true

289. 1. Every finite integral domain is a field.
   2. An infinite integral domain need not be a field.
   (A) 1 is true, but 2 is false
   (B) Both 1 and 2 are true
   (C) 1 is false, but 2 is true
   (D) Both 1 and 2 are false

290. A necessary and sufficient conditions for a non-empty subset K of a field F to be a subfield are—
   (A) $a, b \in K \Rightarrow a - b \in K$
   (B) $a, b \neq 0 \in K \Rightarrow ab^{-1} \in K$
   (C) Both A and B
   (D) None of these

291. Prime field is—
   (A) A field which does not contains any proper subfield
   (B) A field when it is ordered as integral domain
   (C) Both (A) and (B)
   (D) None of these

292. Ordered field is—
   (A) A field which contains a subset of positive elements, satisfying the additive and multicative closure and trichatomy
   (B) A field which does not contains any proper subfield
   (C) Both (A) and (B)
   (D) None of these

Answers with Explanation

1. (D) Since $(z, +, .)$ is a commutative ring with unity and it has no zero divisors. Hence $(z, +, .)$ is also an integral domain. Thus, (A), (B) and (C) all are correct but (D) is not correct. Hence the correct answer of this question is (D).

2. (D)

3. (A) Since the set of natural number does not have any additive identity. Thus (N, +, .) is not a ring. Hence (N, +, .) will not be an integral domain.

4. (A) 5. (A) 6. (A)

7. (A) Division ring is Abelian group under '+' and group under multiplication hence two elements *viz* identity under '+' and identity under multiplication '.' is must. Hence at least two elements in division ring is must.

8. (A) $x \in R \Rightarrow x + x \in R$

Now` $(x+x)^2 = (x+x)$ (given)

$\Rightarrow (x+x)(x+x) = (x+x)$

$\Rightarrow (x+x)\cdot x + (x+x)\cdot x = x + x$

(Left distributive law)

$\Rightarrow (x^2+x^2)+(x^2+x^2) = x + x$

(Right distributive law)

$\Rightarrow (x+x)+(x+x) = x+x$

$[\because x^2 = x]$

$\Rightarrow (x+x)+(x+x) = (x+x)+0$

$[\because x + 0 = x]$

$\Rightarrow x + x = 0$ ...(1)

[By left concellation law for addition in R]

Now $x + y = 0$

$\Rightarrow x + y = x + x$ [from (1)]

$\Rightarrow y = x$

[By left concellation law for addition in R]

9. (B)

10. (B) Since the ring of integers does not have multiplicative inverse so the ring of integers can not be field and division ring. The ring of integers is commutative without zero divisor. Hence it is an integral domain.

11. (C)

12. (D) Since all (A), (B) and (C) are correct. Thus (D) is false. Hence (D) is correct option.

13. (B) Since the set of integers is a commutative ring with unity and $14 \in R$ (ring of integers). Thus, the ideal $\{14r : r \in I\}$ is the principle ideal generated by 14.

14. (B)

15. (A) In the commutative ring of integer z the ideal $\{pr : r \in z\}$ is a prime ideal if p is prime because if $ab \in p$, then $p/ab \Rightarrow p/a$ or p/b.

Hence either $a \in p$ or $b \in p\ \forall a, b \in z$.

16. (A) Suppose m is a prime and let $[a], [b], \in z$.
Then $[a]\,[b] = 0 \Rightarrow \ ab = 0 \pmod m$
$\Rightarrow ab$ is divisible by m
$\Rightarrow$ either m/a or m/b, thus, $ab = 0 \Rightarrow$ either $a = 0 \pmod m$
or, $\qquad b \equiv 0 \pmod m$
$\therefore$ Set of residue classes mod m is a ring without zero divisors again suppose m is not prime, then let.
$m = rs$ where $1 < r < m$, $1 < s < n$
Therefore, $[r]\,[s] = [rs] = [0] \pmod m$
while $[r] \neq [0]$ and $[s] \neq [0]$
$\therefore$ The set of residue classes (mod m) is a ring with zero divisors.
$\therefore$ The correct answer is (A).

17. (B)

18. (D) Complex number are not ordered as, if $x_1 + iy_1, x_2 + iy_2 \in c$ we can not say $(x_1 + iy_1) <$ or $> x_2 + iy_2$.

19. (C)

20. (C) Statement (A) is not correct as a ring may have zero divisors, statement (B) is also not correct always.
Statement (D) is not correct as natural numbers set N has no additive identity hence N is not a ring
(C) is correct it is a will known theorem.

21. (B) [R = {0, 1, 2, 3}, $+_4, \times_4$] is a ring. For check the postulates by following tables.

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\times_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	3

Since, $2, \times_4 2 = 0 \Rightarrow 2$ is a zero divisor

22. (A) Similar to 26, R is not a field as '6' is not prime. It is ring with zero divisors as—$2{\cdot}3 = 0$

23. (A) Since, P is prime, hence option (A) is correct.

24. (D) Since, P is prime hence I_P is field so (A), (B), (C) are all correct. Hence option (D) is correct.

25. (D)

26. (C) Let $L_1 = \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}, L_2 = \begin{bmatrix} c & 0 \\ d & 0 \end{bmatrix}$

be any low elements of, then

$$L_1 - L_2 = \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} - \begin{bmatrix} c & 0 \\ d & 0 \end{bmatrix}$$
$$= \begin{bmatrix} a-c & 0 \\ b-d & 0 \end{bmatrix} \in L$$

$\therefore$ N is a subgroup of M under addition

Now, Let $U = \begin{bmatrix} w & x \\ y & z \end{bmatrix}$ be any element of M

$$\therefore \qquad UL_1 = \begin{bmatrix} w & x \\ y & z \end{bmatrix}\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}$$
$$= \begin{bmatrix} wa+xb & 0 \\ ya+zb & 0 \end{bmatrix} \in L$$

$\therefore$ L is a left ideal of R.

Since $\begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 1 & 2 \end{bmatrix} \notin L$

$\therefore$ L is not right ideal.
Similarly we can prove that k is right ideal but not left ideal on M.

27. (B) 28. (A) 29. (B)

30. (A) Since, (R, +, .) is a ring and non-zero element of the set of real numbers possesses multiplicative inverse in R.
Hence, (R, +, .) is a field.

31. (A)

32. (C) When $x \in \left[\frac{1}{2}, 2\right]$, $f(x) \in \left[-\frac{3}{2}, \frac{3}{2}\right]$
Hence, supremum of $f(x)$ is 3/2.

33. (D) To form a ring, we required at least one element which is 0.
$\therefore$ R {0} form a ring with composition.
$$0 + 0 = 0, \ 0{\cdot}0 = 0$$
This ring known as zero ring

34. (B) We know that set of integers modulo P form a ring with unity to prove that z_p is a field we will have to show that every non zero element of z_p is invertible.

Let $r \in z_p$ and $r \neq 0$,

Now, $r \pm 0 \Rightarrow r \neq 0 \pmod{p}$

$\Rightarrow$ r is not divisible by p

$\Rightarrow$ r and p are relatively prime

i.e., there exist integers x, y such that

$$rx + py = 1$$

$\Rightarrow rx \in 1 \pmod{p}$ as $py = 0 \pmod{p}$

Thus, x is inverse of r in z_p.

$\therefore$ z_p is a field if p is prime.

35. (C) Let $3 + \sqrt{2}$ and $3 - \sqrt{2}$ are two irrational numbers and their product $= (3+\sqrt{2})(3-\sqrt{2}) = 1$ which is a rational number

$\therefore$ The statement (C) is false.

36. (D)	37. (B)	38. (C)	39. (A)	40. (A)
41. (B)	42. (A)	43. (B)	44. (A)	45. (A)
46. (A)	47. (A)	48. (A)	49. (A)	50. (A)
51. (A)	52. (A)	53. (A)	54. (A)	55. (A)
56. (A)	57. (A)	58. (A)	59. (A)	60. (A)

61. (A) Here a is one generator of the group

The order of G is 6.

ap is a generator of G of order n iff p is prime to n, *i.e.*,

$$(n, p) = 1$$

Hence $\qquad (6, 5) = 1$

$\therefore$ $p = 5$ and a^5 is also a generator.

62. (D) Here 1 is a identity as $(-i)^4 = 1$

$\Rightarrow \qquad 0(-i) = 4 \qquad [\because\ 0(a) = p]$

$\Rightarrow p$ is the least positive integer : $a^p = e$, an identity.

63. (D) $\qquad 5(2) = 2 + 5^2 + 5^2 + 5^2 + 5^2 = 0$

so $\qquad 0(2) = 5$

64. (A) $a, b \in G \Rightarrow ab \in G, \forall, a, b \in G$

$$\begin{aligned}
\Rightarrow \quad (ab)^2 &= e \\
\Rightarrow \quad (ab)(ab) &= e \\
\Rightarrow \quad (ab)^{-1} &= ab \\
\Rightarrow \quad b^{-1}a^{-1} &= ab \qquad \ldots(1) \\
\text{But} \quad a^2 &= e \\
\Rightarrow \quad a \cdot a &= e \\
\Rightarrow \quad a^{-1} &= a \qquad \ldots(2) \\
\text{and} \quad b^2 &= e \\
\Rightarrow \quad b^{-1} &= b \qquad \ldots(3)
\end{aligned}$$

$\therefore$ By (2), (3) and (1), we have

$$ab = ba$$

$\therefore$ G is Abelian group.

65. (A)	66. (A)	67. (B)	68. (C)	69. (B)
70. (D)	71. (C)	72. (A)	73. (A)	74. (A)
75. (A)	76. (A)			

77. (C) The inverse of matrix exist only when it is non-singular (M, .) satisfies closure, associative and existence of identity so M is a monoid.

78. (A) We have

$$\begin{aligned}
a * b &= a * b * e \\
&= a * b * (b^{-1} * a^{-1} * b * a) \\
&\qquad [\because\ b^{-1} * a^{-1} * b * a = e] \\
&= a * (b * b^{-1}) * a^{-1} * b * a \\
&= a * e * a^{-1} * b * a \\
&= (a * a^{-1}) * b * a \\
&= e * b * a = b * a
\end{aligned}$$

79. (A) $\forall a \in G, a^2 = e \Rightarrow a \cdot a = a \cdot a^{-1} = e$

$\Rightarrow \qquad a = a^{-1}$

$\therefore \qquad \forall a \cdot b \in G$

$$\begin{aligned}
ab &= (ab)^{-1} \qquad \ldots(1) \\
\Rightarrow \quad a \cdot b &= b^{-1}a^{-1} \\
&= b \cdot a \quad [\because\ a = a^{-1}, b = b^{-1}]
\end{aligned}$$

$\therefore$ Abelian group.

80. (A)
$$\begin{aligned}
fg &= \begin{pmatrix} 1\,2\,3\,4\,5 \\ 1\,3\,2\,4\,5 \end{pmatrix} \begin{pmatrix} 1\,2\,3\,4\,5 \\ 1\,2\,3\,4\,5 \end{pmatrix} \\
&= \begin{pmatrix} 1\,2\,3\,4\,5 \\ 1\,3\,2\,4\,5 \end{pmatrix} \begin{pmatrix} 1\,3\,2\,4\,5 \\ 1\,3\,2\,5\,4 \end{pmatrix} \\
&= \begin{pmatrix} 1\,2\,3\,4\,5 \\ 1\,3\,2\,5\,4 \end{pmatrix}
\end{aligned}$$

81. (B)	82. (A)	83. (C)	84. (A)	85. (A)

86. (A) $(1\ 2\ 3) \cdot (2\ 4\ 3) \cdot (1\ 3\ 4)$

$$\begin{aligned}
&= \begin{pmatrix} 1\,2\,3\,4 \\ 2\,3\,1\,4 \end{pmatrix} \begin{pmatrix} 1\,2\,4\,3 \\ 1\,4\,3\,2 \end{pmatrix} \begin{pmatrix} 1\,2\,3\,4 \\ 3\,2\,4\,1 \end{pmatrix} \\
&= \begin{pmatrix} 1\,2\,3\,4 \\ 2\,3\,1\,4 \end{pmatrix} \begin{pmatrix} 2\,3\,1\,4 \\ 4\,2\,1\,3 \end{pmatrix} \begin{pmatrix} 1\,2\,3\,4 \\ 3\,2\,4\,1 \end{pmatrix} \\
&= \begin{pmatrix} 1\,2\,3\,4 \\ 4\,2\,1\,3 \end{pmatrix} \begin{pmatrix} 4\,2\,1\,3 \\ 1\,2\,3\,4 \end{pmatrix} \\
&= \begin{pmatrix} 1\,2\,3\,4 \\ 1\,2\,3\,4 \end{pmatrix}
\end{aligned}$$

87. (A) $\begin{pmatrix} 1\,2\,5\,3\,4 \\ 3\,4\,1\,5\,2 \end{pmatrix} = \begin{pmatrix} 1\,3\,5\,2\,4 \\ 3\,5\,1\,4\,2 \end{pmatrix}$

$= (1\,3\,5)(2\,4)$
$= (1\,5)(1\,3)(2\,4)$

88. (B) $c = (1\,2\,3\,4\,5\,6\,7)$
c^3 moves every symbol three places a long,
i.e., $c^3 = (1\,4\,7\,3\,6\,5)$

89. (A)
$$\begin{aligned} c^2 &= c\cdot c \\ &= \begin{pmatrix}1\,2\,3\,4\\2\,3\,4\,1\end{pmatrix}\begin{pmatrix}1\,2\,3\,4\\2\,3\,4\,1\end{pmatrix} \\ &= \begin{pmatrix}1\,2\,3\,4\\2\,3\,4\,1\end{pmatrix}\begin{pmatrix}2\,3\,4\,1\\3\,4\,1\,2\end{pmatrix} \\ &= \begin{pmatrix}1\,2\,3\,4\\3\,4\,1\,2\end{pmatrix} \\ &= (1\,3)(2\,4)\end{aligned}$$

90. (D) 91. (A) 92. (A) 93. (A) 94. (B)
95. (A) 96. (B) 97. (D) 98. (A) 99. (B)
100. (A) 101. (A) 102. (B) 103. (C) 104. (A)
105. (B) 106. (C) 107. (A) 108. (A)

109. (A) $a\cdot b = b\cdot a\ \forall\, a, b \in$ E, so (E, +, .) is commutative ring there exist no element $1 \in$ E such that
$$a\cdot 1 = 1\cdot a = a, \forall a \in \text{E}$$
$\therefore$ (E, +, .) is commutative ring, but not an integral domain.

110. (B) $a \odot b = a + b + ab = b + a + ba = b \odot a$
As addition and multiplication of integers are commutative
$\therefore \odot$ is commutative in I.
$\therefore$ I, $\oplus, \odot$ is a commutative ring.
If b is a unit element, $a\cdot b = a$
$\Rightarrow a + b + ba = a, \Rightarrow b + ba = 0, \Rightarrow b\,(1 + a) = 0, \Rightarrow b = 0$
$\therefore 0 \in$ I is a unit element
$\therefore \{$I, $\oplus, \odot\ \}$ is an integral domain.

111. (A) If $e_1 \in$R, then the right identity gives
$$e_1e_2 = e_1 \qquad \ldots(1)$$
If $e_2 \in$R, then the left identity gives
$$e_1e_2 = e_2 \qquad \ldots(2)$$
By equation (1) and (2)
$$e_1e_2 = e_1 = e_2$$
i.e., two identities are equal.

112. (C) If $1 \in$ R is an multiplicative identity then $1\cdot a = a$, and $1 = 0$
$\Rightarrow a\cdot 1 = 0$, which is the contradiction
$\therefore \quad 1 \neq 0$

113. (A) $e_1 \in$ R is unity then
$$e_1\cdot a = a\cdot e_1 = a, \forall a \in \text{R}$$
$e_2 \in$ R is unity then
$$e_2\cdot a = ae_2 = a, \forall a \in \text{R}$$
$\Rightarrow \quad e_1\cdot a = e_2\cdot a$
$\Rightarrow \quad e_1 = e_2$

114. (B) 115. (C) 116. (A) 117. (A) 118. (A)
119. (C) 120. (A) 121. (A) 122. (A) 123. (A)
124. (B) 125. (A) 126. (B)

127. (B) $xy \in$ R
$\Rightarrow (xy)(xy) = xyxy$
$= xxyy$ (if R is commutative)
$= x^2y^2$

128. (C) Let a is nilpotent element of the ring R for some positive integer n,
$a^n = 0 \Rightarrow a^{n-1}\cdot a = 0$, but $a^{n-1} \neq 0$ and also $a \neq 0$.
$\therefore a$ is a divisor of zero, *i.e.*, zero divisor

129. (A) A and B are zero divisors if AB = 0 $\Rightarrow$ A $\neq 0$ and B $\neq 0$
Here $\begin{bmatrix}1 & 1\\1 & 1\end{bmatrix}\begin{bmatrix}1 & 0\\-1 & 0\end{bmatrix} = \begin{bmatrix}0 & 0\\0 & 0\end{bmatrix}$

130. (B) Let 1 be the unity of the field F.
$a\cdot a_1^{-1} = 1$ and $a\cdot a_2^{-1} = 1$
$\Rightarrow \quad a\cdot a_1^{-1} = a\cdot a_2^{-1}$
$\Rightarrow \quad a_1^{-1} = a_2^{-1}$

131. (B) 132. (D) 133. (D) 134. (B) 135. (C)

136. (C) A is one of the generator
ap is generator of G of order n iff $(n, p) = 1$
$1 < p < n$
Here $n = 4$ and $(4, 3) = 1$
$\therefore a^3$ is also a generator of G.

137. (B) Here 1 is an identity element
also $\quad (-1)^2 = 1$
$\therefore \quad 0\,(-1) = 2$
$\because \quad 0\,(a) = p$
$\Rightarrow p$ is the least positive integer
$a^p = e$, an identity

138. (B) $c = \{x + yi : x, y$ are real numbers, $i = \sqrt{-1}\}$

c is a commutative ring.

$$(x_1 + iy_1)(x_2 + iy_2) = (x_1x_2 - y_1y_2) + i(x_1y_2 + x_2y_1)$$
$$= (x_2 + iy_2)(x_1 + iy_1)$$

The zero element is $0 + 0i$ and unit element is $1 + 0i$

Also this ring has no zero divisors because the product of non-zero complex numbers cannot be zero.

Hence c is an integral domain.

139. (C) I is an integral domain $\forall a, b \in$ I, $a \cdot b = 0 \Rightarrow a = 0$ or $b = 0$

$\therefore a^2 = a \cdot a = 0 \Rightarrow a = 0$ which is the contradiction

$\therefore \quad a^2 \neq 0$

140. (D) 141. (A) 142. (A) 143. (A) 144. (A)
145. (A) 146. (D) 147. (B) 148. (C) 149. (C)
150. (A) 151. (D) 152. (A) 153. (A) 154. (A)
155. (A) 156. (A) 157. (A) 158. (A) 159. (A)
160. (B) 161. (A) 162. (A) 163. (C) 164. (A)
165. (A)

166. (A) An integral domain is a field if it possess an multiplicative inverse.

167. (D) $a > b \Rightarrow a - b > 0, \Rightarrow (a + c) - (b + c) = a - b > 0$

$\Rightarrow \quad a + c > b + c$

168. (A) R is commutative

$$(ab)^4 = ab \cdot ab \cdot (ab)^2$$
$$= aabb \cdot ab \cdot a \cdot b$$
$$= a^2b^2 \cdot ba \cdot a \cdot b$$
$$= a^2b^3a \cdot ba$$
$$= a^2b^3 \cdot ba \cdot a$$
$$= a^2b^4 \cdot a \cdot a \quad (\because b^4 = b, \forall b \in \text{R})$$
$$= a^2b \cdot a \cdot a$$
$$= a^2 \cdot a \cdot b \cdot a = a^3ba$$
$$= a^3 \cdot a \cdot b = a^4 \cdot b$$
$$= a \cdot b$$

169. (A) R is commutative

$$(ab)^2 = ab \cdot ab$$
$$= a \cdot a \cdot b \cdot b$$
$$= a^2b^2$$

170. (B) 171. (B) 172. (B) 173. (A) 174. (A)
175. (B) 176. (D) 177. (A) 178. (A) 179. (A)
180. (B) 181. (B) 182. (A) 183. (D) 184. (A)
185. (C) 186. (C) 187. (A) 188. (A) 189. (B)
190. (A) 191. (A) 192. (C) 193. (A) 194. (A)
195. (C) 196. (B) 197. (A) 198. (A) 199. (A)
200. (B) 201. (A) 202. (A) 203. (C) 204. (D)
205. (A) 206. (A) 207. (A) 208. (B) 209. (B)
210. (A) 211. (A) 212. (B) 213. (B) 214. (A)
215. (B) 216. (B) 217. (B) 218. (A) 219. (B)
220. (B) 221. (A) 222. (A) 223. (B) 224. (A)
225. (C) 226. (D) 227. (A) 228. (D) 229. (B)
230. (B) 231. (D) 232. (D) 233. (B) 234. (B)
235. (D) 236. (A) 237. (B) 238. (B) 239. (A)
240. (C) 241. (B) 242. (B) 243. (B) 244. (A)
245. (C) 246. (C) 247. (A) 248. (A) 249. (A)
250. (A) 251. (A) 252. (A) 253. (A) 254. (A)
255. (A) 256. (A) 257. (B) 258. (A) 259. (A)
260. (A) 261. (A) 262. (A) 263. (B) 264. (B)
265. (A) 266. (A) 267. (A) 268. (B) 269. (B)
270. (A) 271. (D) 272. (A) 273. (C) 274. (B)
275. (A) 276. (A) 277. (A) 278. (B) 279. (A)
280. (A) 281. (B) 282. (A) 283. (C) 284. (C)
285. (C) 286. (B) 287. (A) 288. (D) 289. (B)
290. (B) 291. (A) 292. (C)