ABSTRACT ALGEBRA

SUB CODE: 16SCCMM12

2 MARKS:

1 Group:

A Non-empty set G together with an operation * (i.e) (G,*) is said to be a group if it satisfies the following axioms

i) closure Axiom
ii) Associative Axiom
iii) Identity Axiom
iv) Inverse Axiom

2 Abelian Group:

If a group satisfies the commutative property then it is called an abelian group.

3. Monoid:

A Non-empty set M with an operation * (i.e) (M,*) is said to be a Monoid when it satisfies closure axiom, Associative axiom and Identity axiom.

4 permutation Group:

Let A be a Finite set A. bijection from A to itself is called a permutation of A.

5. Idempotent:

An element $a \in G$ is called a Idempotent. If $a^2 = a$. thus the Identity element is the only Idempotent element.

6 Sub Groups:

A subset H of group G is called a subgroups of G. if H Forms a group with respect to the binary operation in G.

7. cyclic group:

Let G be a group. Let $a \in G$ then $H = \{a^n / n \in Z\}$ is a subgroup of G. H is called the cyclic subgroup of G generated by a and is denoted by $\langle a \rangle$.

8. Lagrange's theorem!

Let G be Finite group of Order n and H be any Subgroup of G. then the order of H diviser the order of G.

9. Euler's theorem:

If n is any integer and $(a,n) \geq 1$ then $a^{\phi n} = 1 \pmod n$

$\phi(n)$ is a Number of positives integer less n relatives prime to n.

10 Fermat's theorem:

Let P be a Prime Number and a be any integer relatively prime to P. then $a^{P-1} \equiv 1 \pmod P$

11 Normal Subgroups and Quotient Group's

A Subgroups H of G is called a Normal subgroup of G. if $aH = Ha$ For all $a \in G$.

12 Isomorphism!

Let G and G' be two groups A map $f : G \rightarrow G'$ is called an isomorphism in

i) f is a bijection

ii) $f(x,y) = f(x) f(y) \; \forall \; x,y \in G$.

13. Isomorphic:

Two groups G and G' are said to be isomorphic if there exists an isomorphic $f : G \to G'$.
It is denoted by $G \cong G'$.

14. Homomorphisms:

A map f from a group G into a group G' is called a homomorphisms if $f(ab) = f(a).f(b) \ \forall a, b \in G$
obviously Every Isomorphism is a Homomorphism is an isomorphism

15. Monomorphism:

Let $f : G \to G'$ be a Homomorphism
i) If f is one-to-one that is called a monomorphism

16. Rings:

An Non-empty R together with two binary operation denoted by '+' and '.' is called addition and multiplication which satisfy the following axioms is called ring.

17. Zero elements:

A unique Identify of additive Group $(R, +)$ is denoted 0 and is called the zero elements.

18 Rings of Gaussion integral:

Let $R = \{a+ib, a, b \in Z\}$ then R is Ring under usual addition and multiplication. This Rings is called Rings of Gaussion integral

19. Null Ring:

$\{0\}$ with binary operation + and $\cdot$ define as $0+0=0$ and $0 \cdot 0 = 0$ is a ring. this is called Null ring.

20 Isomorphism of Ring:

Let $(R, +, \circ)$ and $(R', +, \cdot)$ be two ring a bijection $f: R \to R'$ is called an Isomorphism

i) $f(a+b = f(a) + f(b)$ and

ii) $f(ab) = f(a) f(b) \forall a, b \in R$

21 Maximal Ideal:

Let R be a ring. An ideal $M \neq R$ is said to be a maximal ideal of R if whenever V is and ideal of R. Such that $M \leq V \subseteq R$ then either $U = M$ or $V = R$

22 Homomorphism of A Ring:

Let R and R' be rings A Function $F: R \to R'$ is called a homomorphism if

i) $f(a+b) = f(a) + f(b)$

ii) $f(ab) = f(a) f(b) \ \forall \ a, b \in R$.

23. prime ideal:

Let R be a commutative ring An ideal $P \neq R$ is called a prime ideal if $ab \in P \Rightarrow$ either $a \in P$ or $b \in P$.

24. kernal:

The kernal K of a homomorphism F of a ring R to ring R' is defined by $\{a / a \in R$ and $f(a) = 0\}$.

25 Relatively prime:

Two elements a and b of a Eulidean domain R are said to be relatively prime if their g.c.d is a unit in R.

5 MARKS:

1. Let G be a group let $a,b \in G$, then $(ab)^{-1} = b^{-1}a^{-1}$ and $(a^{-1})^{-1} = a$

Proof:

Let G be a group. let $a,b \in G$

To Prove: $(ab)^{-1} = b^{-1}a^{-1}$

$$ab(b^{-1}a^{-1}) = a(bb^{-1})a^{-1}$$
$$= (a \cdot e)a^{-1}$$
$$= a \cdot a^{-1}$$
$$= e \longrightarrow (1)$$

$$(ab)^{-1} = ab(ab^{-1})$$
$$= ab(b^{-1}a^{-1})$$
$$= a(bb^{-1})a^{-1}$$
$$= (a \cdot e)a^{-1}$$
$$= a \cdot a^{-1}$$
$$= e \longrightarrow (2)$$

From (1) & (2)

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

then To Prove:

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

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

It is obviously true.

2. Let G be a group then
   i) identity elements of G is unique.
   ii) For any $a \in G$ the inverse of a is unique.

Proof:

i) Let e and e' be two identity elements of G.

then $ee' = e'$ (since e is an identity)

Hence $e = e'$

(ii) Let a' and a'' be two inverse of a.

Hence $aa' = a'a = e$

$a'a'' = a''a = e$

$a' = a'e = a'(aa'')$

Hence proved.

3. In a group left and Right Cancelled laws hold i.e. i) $ab = ac \Rightarrow b = c$ and ii) $ba = ca \Rightarrow b = c$.

Proof:

i) $ab = ac$

both sides Multiplication a^{-1}

$a^{-1}(ab) = a^{-1}(ac)$

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

$eb = ec$

$b = c \longrightarrow (1)$

ii) $ba = ca$

both sides multiplication a^{-1}

$(ba)a^{-1} = (ca)a^{-1}$

$b(aa^{-1}) = c(aa^{-1})$

$be = ce$

$b = c \longrightarrow (2)$

$\therefore ab = ac \Rightarrow b = c$

Hence proved.

---

4) The set of all possitive integers less than n and prime to its a group under multiplication modulo n.

Proof:

Let $G = \{m/m < n \text{ and } (m,n) < 1\}$

Let $p, q \in G$

obviously $pq \neq n$ and $(pq, n) = 1$

Now, Let $pq = Sn + r$, $0 < r < n$

Hence $p \odot q = r$ (by definition)

We claim that $(r, n) = 1$

Suppose $(r, n) = a > 1$, then a/r and a/n

Hence $a / r + Sn$ ie) a/pq also a/n

Hence $(pq, n) \neq 1$ which is contradiction.

Hence $r \in G$. Hence G is closed under $\oplus$. We know that multiplication modulo n is associative $1 \in G$ is the identity element.

Let $a \in G$

then, $(a, n) = 1$

Hence the linear congruence

$ax \equiv 1 ; (\mod n)$ has a unique solution for x say b.

$\therefore ab \equiv 1 \pmod n$

Hence $a \odot b = 1$

Now, we have to prove that $b \in G$

Suppose $(b, n) = c$

Since $ab = 1 \pmod n$, $ab = q_n + 1$

Now, c/b and c/n

$\Rightarrow c/(ab - qn) \Rightarrow c/1 \Rightarrow c = 1$

thus $(b, n) = 1$

Hence $b \in G$ and is the inverse of a. Thus G is a group.

5. A Subgroup of cyclic group is cyclic.

Proof:

Let G be a cyclic group generator by a

Let H be a Subgroup of G

We claim that:

H is cyclic every element of H is of the form for some integer n.

Let m be the Smallest +ve integer Such that $a^m \in H$

We claim that:

a^m is a generator of H

Let $b \in H$ then $b = a^n$ for some $n \in Z$

Let $n = mq + r$. where $0 \leq r < m$

Then $b = a^n = a^{mq+r}$

$= (a^m)^q \cdot a^r$

$a^r = (a^m)^{-q} \cdot b \longrightarrow (1)$

Now, $a^m \in H$. Since H is a subgroup $(a^m)^{-q} \in H$, also $b \in H$

by (1), $a^r \in H$ and $0 \leq r < m$

but m is the least +ve integer such that $a^n \in H$

$\therefore r = 0$. Hence $b = a^n = a^{qm} = (a^m)^q$

$\therefore$ Every element of H is a Power a^m.

$\therefore H = (a^m)$ and Hence H is cyclic.

b) Let G be a group and a be an element of order in G. Then $a^m = e$ if and only if n divides m.

Proof:

Let G be a group a be an element of order n in G. $(a^n = e)$.

Suppose n divides m (ie) n/m

then,

$m = nq$ where $q \in Z$

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

Conversely:

let $a^m = e$

Let $m = nq + r$, where $0 \leq r < n$

$a^m = a^{nq+r} = a^{nq} \cdot a^r = e \cdot a^r = a^r$

$a^r = e$ and $0 \leq r < n$

Now,

Since n is the smallest positive integer such that $a^n = e$, we have $r = 0$.

Hence $m = nq$

$\therefore$ n divides m (n/m).

7. Let H be a subgroup of G the number of left cosets of H is the same as the number of Right cosets of H.

<u>Proof</u>:

Let L & R Respectively denote the set of left Right cosets of Respectively. we define a map $F: L \to R$ given by,

$$F(aH) = Ha^{-1}$$

i) <u>F is well defined</u> :-

$aH = bH \Rightarrow a^{-1}b \in H$

$\Rightarrow a^{-1} \in Hb^{-1}$

$\Rightarrow a^{-1}H = Hb^{-1}$

$\therefore$ F is well defined.

ii) <u>F is one to one</u> :-

$F(aH) = F(bH)$

$\Rightarrow Ha^{-1} = Hb^{-1}$

$\Rightarrow a^{-1} \in Hb^{-1}$

$\Rightarrow a^{-1} = hb^{-1}$ for some $h \in H$

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

$\Rightarrow a = bh^{-1} \in bH$

$\Rightarrow a \in bH \Rightarrow aH = bH$

$\therefore$ F is one - one.

Hence proved

iii) F is onto :-

For every Right coset Ha has a pre image under F namely $a^{-1}H$.

$\therefore$ F is a bijection from L to R.

Hence the number of left cosets is same as the number of Right coset.

---

8. Every subgroup of an abelian group is a normal subgroup.

Proof :-

Let G be an abelian group and let H be a subgroup of G let $a \in G$.

Claim :- $aH = Ha$

Let $x \in aH \Rightarrow x = ah$ for some $h \in H$

$x = ha$ ($\because G$ is abelian)

$\therefore x \in Ha$

Hence $aH \subset Ha$

Similarly, $Ha \subset aH$

$\therefore aH = Ha$ and

Hence H is a normal subgroup of G.

9, Let N be a normal subgroup of a group G. then G/N is a group under the operation defined by $NaNb = Nab$.

Proof:

Let N be a Normal Subgroup of G.

$$NaNb = Nab$$

Let G/N be a group

i) Let $Na, Nb, Nc \in G/N$

$$Na(NbNc) = Na(Nbc)$$
$$= Nabc$$
$$= N(ab)c$$
$$= NabNc$$

$$Na(NbNc) = (NaNb)Nc$$

the binary is associative.

ii) Let $Ne = N \in G/N$

$$NaNe = Nae = Na = NeNa$$

$\therefore$ Ne is identity element

iii) Also $NaNa^{-1} = Naa^{-1}$

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

$\therefore$ Na^{-1} is the inverse of Na

$\therefore$ G/N is a group.

10) A Subgroup N of G is normal iff the Product of two Right cosets of N is again right cosets of N.

<u>Proof:</u>

Suppose N is a Normal subgroup of G.

$$NaNb = N(aN)b$$

$$= N(Nab) \quad (N \text{ is normal subgroup i.e } Na = aN)$$

$$= NNab$$

$$= Nab \quad (\text{since } NN = N)$$

Conversely,

Suppose that the Product of two rights cosets is again right cosets of N

i.e) $NaNb = Nab$

To prove that,

N is a normal subgroup of G.

$$ab = (ea)(eb) \in NaNb$$

$\therefore$ $NaNb$ is a right cosets containing ab

i.e) $NaNb = Nab$

Let $a \in G$ and $n \in N$

$$ana^{-1} = eana^{-1} \in NaNa^{-1}$$
$$= Naa^{-1} = N$$

$\therefore ana^{-1} = N \Rightarrow ana^{-1} \in N$

$\therefore N$ is a normal subgroup of G.

---

11) In a skew field R

i) $ax = ay$, $a \neq 0 \Rightarrow x = y$

ii) $xa = ya$, $a \neq 0 \Rightarrow x = y$

iii) $ax = 0 \Leftrightarrow a = 0$ (or) $x = 0$

Proof:-

Assume that $ax = ay$, $a \neq 0$

To Prove that $x = y$

Since R is a skew field. There exist $a^{-1} \in R$, such that $aa^{-1} = a^{-1}a = 1$

i) $ax = ay \Rightarrow a^{-1}ax = a^{-1}ay$

$(aa^{-1})x = (aa^{-1})y \Rightarrow 1.x = 1.y$

$\Rightarrow x = y$

ii) $xa = ya$ (Multiply on L.H.S in a^{-1})

$xaa^{-1} = yaa^{-1}$

$x(aa^{-1}) = y(aa^{-1}) \Rightarrow x.1 = y.1$

$\Rightarrow x = y$

iii) $ax = 0 \iff a = 0$ (or) $x = 0$

Suppose that $ax = 0 \Rightarrow \alpha x = \alpha \cdot 0$

$\boxed{x = 0}$

---

12) Z_n is an integral domain. iff n is Prime number.

Proof :-

Let Z_n be the integral domain

To Prove that :- n is Prime

Suppose n is not Prime

then $n = pq$, where $1 < p < n$

$1 < q < n$

clearly $p \odot q = 0$

Hence p and q are zero devisor.

Z_n is not integral domain.

Conversely,

Suppose n is Prime.

$a, b \in Z_n$

$a \odot b = 0$

$ab = qn$

Where $q \in Z_n$

$$\Rightarrow \frac{1}{q} = \frac{n}{ab}$$

$\Rightarrow n/ab \quad (ab = 0)$

n/a (or) n/b (n is prime)

$a = 0$ (or) $b = 0$

Z_n has no zero devisors

$\therefore$ Z_n has integral domain.

---

13) Any Finite integral domain is a Field.

<u>Proof</u> :-

Let R be a integral domain. we need only to prove that, every non-zero elements are has a Multiplicate inverse

Let $a \in R$ and $a \neq 0$

Let $R = \{0, 1, a_1, a_2 \ldots a_n\}$

Consider $\{a, a.1, a.a_1, a.a_2, \ldots a.a_n\}$ and all this elements are non zero.

Hence $a a_i = 1 \ \forall \ a_i \in R$

Since R is a commutative.

$aa_i = a_i a = 1$

So that $a_i = a^{-1}$

$\therefore$ Any Finite integral domain is a Field.

---

14) Let R be any commutative Ring with identity. Let P be an ideal of R. Then P is a prime ideal $\Leftrightarrow R/P$ is an integral domain.

<u>Proof:</u>

Let P be a Prime ideal

Since, R is a commutative ring with identity R/P is also commutative ring with identity

Now, $(P+a)(P+b) = P+0$

$\Rightarrow P+ab = P$

$\Rightarrow ab \in P$

$\Rightarrow a \in P$ (or) $b \in P$

(Since P is Prime ideal)

$\Rightarrow P+a = P$ (or) $P+b = P$

Thus, R/P has no zero divisor

$\therefore R/P$ is an integral domain.

Conversely,

suppose R/P is a integral domain.

Claim that, P is a prime ideal of R.

Let $ab \in P$. Then $P+ab$

$\therefore (P+a)(P+b) = P$

$\therefore P+a = P$ (or) $P+b = P$

(Since, R/P has no zero divisors)

$\therefore a \in P$ (or) $b \in P$

P is a prime ideal of.

Hence proved.

---

15) $\sim$ is an equivalent relation in S.

<u>Proof:</u>

i) <u>Reflexive</u>

Let $(a,b) \in S$

$(a,b) \sim (a,b)$

Since $ab = ba = ab$

Hence $\sim$ is reflexive.

ii) Symmetric :

Now, $(a,b) \sim (c,d) \Rightarrow ad = bc$

$\Rightarrow cb = da$

$\Rightarrow (c,d) \sim (a,b)$

Hence $\sim$ is Symmetric.

iii) Transitive :-

Case (i) : Let $c = 0$

Now, $ad = bc$ and $cf = de$

$\therefore adcf = bcde$

$\therefore af = be$ (by cancellation law)

$\therefore \sim$ is transitive.

Hence $\sim$ is an equivalence

Relation on S.

10 MARKS:

1. Let G be the set of all real number except -1 define $*$ on G by $a*b = a+b+ab$ then $(G,*)$ is a group.

Proof:

i) closure:

Let $a, b \in G$. then $a \neq -1$ and $b \neq -1$

We claim that $a*b \neq -1$

Suppose $a*b = -1$

$a+b+ab = -1$

then $(a+1)(b+1) = 0$

So that either $a = -1$ (or) $b = -1$

which is contradiction

Hence $a*b \neq -1$

thus, $*$ is a binary operation

ii) Associative:

$*$ is an associative

$a*(b*c) = (a*b)*c$

$a*(b*c) = a*(b+c+bc)$

$= a+(b+c+bc)+a(b+c+bc)$

$= \underbrace{a+b+c+bc+ab+ac+abc}_{①}$

$$(a*b)*c = (a+b+ab)*c$$
$$= a+b+ab+c+c(a+b+ab)$$
$$= a+b+c+ab+ac+bc+abc \quad \text{(2)}$$

From (1) & (2)

$$a*(b*c) = (a*b)*c$$

iii) Identity:

0 is the identity

$$a*0 = a+0+a(0)$$
$$= a$$
$$0*a = 0+a+0(a)$$
$$= a$$

Hence

$$e*a = a*e = a$$

iv) Inverse:

Now, let a^{-1} be such that

$$a*a^{-1} = a^{-1}*b = e = 0$$
$$a*a^{-1} = a+a^{-1}+aa^{-1} = 0$$
$$\Rightarrow a+a^{-1}(1+a) = 0$$
$$a^{-1}(1+a) = -a$$
$$a^{-1} = \frac{-a}{1+a}$$

Since, $a \neq -1$

we have $a^{-1} \in R - \{-1\}$

$$a^{-1} * a = 0$$

$$\left(\frac{-a}{1+a}\right) * a = \left(\frac{-a}{1+a}\right) + a + \left(\frac{-a}{1+a}\right)(a)$$

$$= \frac{-a}{1+a} + a - \frac{a^2}{1+a}$$

$$= \frac{-a + a(1+a) - a^2}{1+a}$$

$$= \frac{\cancel{-a} + \cancel{a} + \cancel{a^2} - \cancel{a^2}}{1+a}$$

$$= \frac{0}{1+a}$$

$$a^{-1} * a = 0$$

Hence, $a^{-1} * a = a^{-1} * a = 0$

$$a^{-1} * a = 0$$

Hence, a^{-1} is the inverse of G thus G is a group.

2) $(Z_n, \oplus)$ is a group

Proof:

i) closure:

Clearly $\oplus$ is a binary operation Z^+.

ii) Associative :

Let $a, b, c \in Z_n$

Let $a+b = q_1 n + r_1 \longrightarrow (1)$

Where $0 \le r_1 \le n$

$b+c = q_2 n + r_2 \longrightarrow (2)$

Where $0 \le r_2 \le n$

$r_1 + c = q_3 n + r_3 \longrightarrow (3)$

Where $0 \le r_3 \le n$

$a+b+c+r_1 = q_1 n + r_1 + q_3 n + r_3$

$a+b+c = q_1 n + q_3 n + r_3 \longrightarrow (4)$

by (2) Sub in (4)

$b+c = q_2 n + r_2$

$a + q_2 n + r_2 = n(q_1 + q_3) + r_3$

$a + r_2 = n(q_1 + q_3) + r_3 - q_2 n$

$a + r_2 = n(q_1 - q_2 + q_3) + r_3$

$a + r_2 = n \cdot q_4 + r_3 \longrightarrow (5)$

(where $q_4 = q_1 - q_2 + q_3$)

Now,

$(a \oplus b) \oplus c = r_1 \oplus c = r_3$ (by (3))

Also

$$a \oplus (b \oplus c) = a \oplus r_1 = r_3 \text{ (by } \oplus)$$

Hence, $\oplus$ is associative

Clearly the identity element is 0 and the inverse of $a \in Z_n$ is $n-1$

Hence $(Z_n, \oplus)$ is a group.

---

3. Theorem:

The union of two Subgroup of a group G is a Supgroup if and only if one is contained in the other.

Proof:

Let H and K be the two Subgroups of G such that one is contained in the other.

ie) Either $K \subseteq H$ (or) $H \subseteq K$

$H \cup K = H$ (or) $H \cup K = K$

[$\because H \& K$ is Subgroup of G]

$H \cup K$ is a Subgroup of G.

Conversely,

Suppose $H \cup K$ is a Subgroup of G

To Proove

$H \subseteq K$ (or) $K \subseteq H$

Suppose that H is not contained in K and K is not contained in H

Then there exist element a, b such that

$a \in H$ and $a \notin K \longrightarrow (1)$

$b \in K$ and $b \notin H \longrightarrow (2)$

$a, b \in H \cup K$

Since, $H \cup K$ is a subgroup of G.

$ab \in H \cup K$. Hence $ab \in H$ (or) $ab \in K$.

Case(i):

$ab \in H$

Since, $a \in H$, $a^{-1} \in H$

$a^{-1}(ab) = b \in H$ which is a contradiction for (2)

Case(ii):

Let $ab \in K$

Since, $b \in K$, $b^{-1} \in K$

$(ab)b^{-1} = a \in K$ which is a contradiction of (1) Hence our assumption that H is not contained in K and K is not contained in H is false.

$\therefore H \subseteq K$ (or) $K \subseteq H$

4) Let A and B be two Subgroup of a group G then AB is a Subgroup of G if and only if $AB = BA$

<u>Proof</u>:

Let AB be Subgroup of G, we Claim that $AB = BA$

Let $x \in AB$, Since AB is a Subgroup of G.

$$x^{-1} \in AB$$

Let $x = ab$ where $a \in A$ and $b \in B$

$$\therefore x^{-1} = (ab)^{-1} = b^{-1}a^{-1}$$

Since A and B are subgroups of G.

$a^{-1} \in A$ and $b^{-1} \in B$

$$\therefore x \in BA$$

Hence $AB \subseteq BA \longrightarrow (1)$

Let $x \in BA$, then $x = ba$, where $b \in B$ and $a \in A$

$$\therefore x^{-1} = (ba)^{-1} = a^{-1}b^{-1} \in AB$$

Since AB is a Subgroup and $x^{-1} \in AB$, we have $x \in AB$

$$\therefore BA \subseteq AB \longrightarrow (2)$$

From ① & ② we get $AB = BA$

Conversely :-

Let $AB = BA$ we claim that AB is a subgroup of G. Clearly $e \in AB$ and hence AB is not empty

$x, y \in AB$ then $x = a_1 b_1$ and $y = a_2 b_2$ where $a_1, a_2 \in A$ and $b_1, b_2 \in B$

$$\therefore xy^{-1} = (a_1 b_1)(a_2 b_2)^{-1}$$

$$= a_1 b_1 b_2^{-1} a_2$$

Now,

$b_2^{-1} a_2^{-1} \in BA \quad (\because BA = AB)$

$b_2^{-1} a_2^{-1} \in AB$

$\therefore b_2^{-1} a_2^{-1} = a_3 b_3$ where $a_3 \in A$ and $b_3 \in B$.

$$xy^{-1} = a_1 b_1 a_3 b_3$$

Now, $b_1 a_3 \in BA$ since $BA = AB$ $b_1 a_3 \in AB$

$\therefore b_1 a_3 = a_4 b_4$ where $a_4 \in A$ and $b_4 \in B$

$\therefore xy^{-1} = a_1 (a_4 b_4) b_3 = (a_1 a_4)(b_4 b_3) \in AB$

$\therefore AB$ is a subgroup of G.

5) State and prove necessary and Sufficient condition for a subset of a group to be Subgroup.

Statement:

Let $(G, *)$ be group. A non empty Subset H of a group G is a Subgroup of G if and only if $a, b \in H \Rightarrow ab^{-1} \in H$

Proof:

Let H be a Subgroup of G. then

$a, b \in H$.

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

Conversely,

Let H be a non-empty Subset of G. Such that $a, b \in H \Rightarrow ab^{-1} \in H$

$\therefore H \neq \phi$, there exists an element $a \in H$. Hence $aa^{-1} \in H$ thus $e \in H$

Also, Since $e, a \in H$, $aa^{-1} \in H$

Hence $a^{-1} \in H$

Let $a, b \in H$, then $a, b^{-1} \in H$

Hence, $a(b^{-1})^{-1} = ab^{-1} \in H$

Thus H is closed under the binary operation in G.

Hence H is a subgroup of G.

b) Let N be a Subgroup of G. the following condition are equivalent

i) N is a Normal subgroup of G

ii) $aNa^{-1} = N \ \forall \ a \in G$

iii) $aNa^{-1} \subseteq N \ \forall \ a \in G$

iv) $ana^{-1} \in NN \ \forall \ n \in N$ and $a \in G$

Proof:

(i) $\Rightarrow$ (ii)

Suppose N is a Normal Subgroup of G

$$aN = Na \ \forall \ a \in G$$

$$aNa^{-1} = Naa^{-1} \ \forall \ a \in G$$

$$= Ne$$

$$aNa^{-1} = N$$

(ii) $\Rightarrow$ (iii)

Let $aNa^{-1} = N \ \forall a \in G$

$$aNa^{-1} \subseteq N \ \forall \ a \in G$$

(iii) $\Rightarrow$ (iv)

Let $aNa^{-1} \subseteq N \ \forall \ a \in G$

$ana^{-1} \in N \ \forall \ n \in N$ and $a \in G$

iv) $\Rightarrow$ (i)

$ana^{-1} \in N \ \forall \ a \in G$ and $n \in N$

Claim

$$aN = Na$$

Let $x \in aN$

$x = aN$ for some $n \in N$

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

$= (ana^{-1})a \in Na$

$aN \subseteq Na \longrightarrow (1)$

Let $x \in Na$

$x = na$ for some $n \in N$

$x = aa^{-1}(na)$

$= a(a^{-1}na) \in aN$

$x \in aN$

$Na \subseteq aN \longrightarrow (2)$

From (1) & (2)

$Na = aN$

N is a Normal Subgroup of G.

---

7) State and prove Cayle's theorem.

<u>Statement:</u>

Any Finite group is isomorphic to a group of permutations.

<u>Proof:</u>

<u>Step(i):</u> Let G be a finite group of order. Let $a \in G$.

Define $f_a : G \rightarrow G'$ by $f_a(x) = ax$

Now,

(i) f_a is one to one

$$f_a(x) = f_a(y)$$

$$ax = ay$$

$$x = y$$

$\therefore$ f_a is one to one function.

ii) f_a is onto:

Since if $y \in G$ then $f_a(a^{-1}y) = a(a^{-1}y)$

$$f_a(a^{-1}y) = a(a^{-1}y)$$
$$= (aa^{-1})y$$
$$= y$$

$\therefore$ f_a is onto function.

$\therefore$ f_a is bijection.

Since G has n elements f_a is just a permutation on n symbols

Let $G' = \{f_a / a \in G\}$

Step (ii) We prove G' is a group

Let $f_a, f_b \in G'$

$$(f_a \circ f_b)(x) = f_a(f_b(x))$$
$$= f_a(bx) = a(bx)$$
$$= (ab)x = f_{ab}(x)$$

Hence $f_a \circ f_b$. Hence G' is closed under composition of mapping

$f_e \in G'$ is the identity elements.

The inverse of f_a in G' is $f_{a^{-1}}$.

$\therefore G^{-1}$ is a group.

Step(iii):

We prove $G \cong G'$

Define $\phi : G \to G'$ by $\phi(a) = f(a)$

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

$$f_a = f_b$$

$$\Rightarrow f_a(x) = f_b(x)$$

$$ax = bx$$

$$\boxed{a = b}$$

Hence ϕ is one to one obviously

ϕ is onto Also,

$$\phi(ab) = f_{ab} = f_a \cdot f_b$$

$$= \phi a \cdot \phi b$$

8) Let $f: G \to G'$ be a Homomorphism

then,

i) $f(e) = e'$

ii) $f(a^{-1}) = [f(a)]^{-1}$

iii) If H is a subgroup of G, then $f(H)$ is a subgroup of G'.

iv) If H is normal in G. $f(H)$ is normal in $f(G)$

v) If H' is a subgroup of G'. then $f'(H')$ is a subgroup of G.

vi) If H' is normal in $f'(G)$ then $f'(H')$ is normal in G.

Proof:

i) $f(e) = e'$

Let $f: G \to G'$ be a homomorphism.

Let $a \in G$.

Then $f(a) = f(ae) = f(a) \cdot f(e)$

$= f(a) \cdot f(e)$

$= f(e)$

$= e'$.

ii) $f(a^{-1}) = [f(a)]^{-1}$

Proof:-

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

$= f(e) = 0$

$f(a) \cdot f(a^{-1}) = e'$

$f(a^{-1}) = [f(a)]^{-1} \cdot e'$

$= [f(a)]^{-1}$

Hence proved.

iii) If H is a subgroup of G. Then $f(H)$ is a Subgroup of G'.

<u>Proof</u>:-

Let H be a Subgroup of G.

Since H is non empty. Also $f(H)$ is non empty

Let $x, y \in f(H)$

Then $x = f(a)$, $y = f(b)$ where $a, b \in H$

$xy^{-1} = f(a)[f(b)]^{-1}$

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

$= f(ab^{-1})$

Since H is a subgroup of G.

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

$\therefore xy^{-1} f(ab^{-1}) \in f(H)$

$\therefore xy^{-1} \in f(H)$

$\therefore f(H)$ is subgroup of G.

Hence Proved

(iv) If H is normal in G. Then $f(H)$ is normal in $f(G)$.

<u>Proof</u>: Let H be a normal in G

Let $x \in f(H)$ and $y \in f(G)$

We claim that :

$$yxy^{-1} \in f(H)$$

Now, $x = f(a)$ and $y = f(b)$

Where $a \in H$, $b \in G$

Since H is a normal in G

i.e) $bab^{-1} \in H$

$\therefore f(bab^{-1}) \in f(H)$

$f(b) \cdot f(a) \cdot f(b^{-1}) \in f(H)$

$yxy^{-1} \in f(H)$

Hence proved.

(V) If H is a Subgroup of G, then $f^{1}(H^{1})$ is a subgroup of G

Proof: since $f(e) = e' \in H'$, $e \in f^{-1}(H^{-1})$ and hence $f^{-1}(H') \neq \phi$

Now, Let $a, b \in f^{-1}(H')$

Then $f(a), f(b) \in H'$

$\therefore f(a)\,[f(b)]^{-1} \in H'$

$\therefore f(ab^{-1}) \in H'$. i.e) $(ab^{-1}) \in f^{-1}(H)$

Hence $f^{-1}(H')$ is a subgroup of G.

(Vi) If H' is normal in $f(G)$. then $f^{1}(H)$ is normal in G.

Proof: Let $x \in f^{-1}(H')$ and $a \in G$

Then $f(x) \in H'$ and $f(a) \to f(a)$

Since H' is normal in $f(G)$

$f(a) f(x) [f(a)]^{-1} \in H'$

$\therefore f(axa^{-1}) \in H'$

Hence $axa^{-1} \in f^{-1}(H')$

Thus $f^{-1}(H')$ is normal in G.

---

9) Let R be a ring and I be a Subgroup of $(R, +)$. The Multiplication in R/I given by $(I+a)(I+b) = I+ab$ is well defined iff I is an ideal of R.

Proof:

Let I be an ideal of R.

To Prove that,

Multiplication is well defined

$I+a = I+a_1$ and $I+b = I+b_1$

$a_1 \in I+a$ and $b_1 \in I+b$

$a_1 = i_1 + a$ and $b_1 = i_2 + b$

where $i_1, i_2 \in I$

$a_1 b_1 = (i_1 + a)(i_2 + b)$

$= i_1 i_2 + b i_1 + a i_2 + ab$

$i_1, i_2, i_1 b, a i_2 \in I$

I is an ideal of R.

Since $i_1 i_2 + b i_1 + a i_2 = i_3$

$$a_1 b_1 = i_3 ab$$

$$(i_1 + a)(i_2 + b) = i_3 + ab$$

where $i_1, i_2, i_3 \in I$

$$(I+a)(I+b) = I + ab$$

Conversely,

Suppose that the multiplication in R/I is given by $(I+a)(I+b) = (I+ab)$ is well defined.

To prove that i is an ideal of R

let $i \in I$ and $r \in R$

we have prove that $ir, ri \in I$

$$(I + ir) = (I+i)(I+r) = (I+0)(I+r)$$

$$= (I + 0r) = I$$

$I + ir \in I$ is $ir \in I$

$ri \in I$.

$\therefore I$ is an ideal of R.

10) Let R be a commutative ring with identity. An ideal M of R is maximal iff R/M is a field.

<u>Proof</u>:

Let M be a Maximal ideal in R.

Since, R is a commutative ring with identity and $M \neq R$

R/M is also a commutative ring with identity.

Now, Let $M+a$ be a non-zero element in R/M so that $a \notin M$

<u>Prove that</u>,

$M+a$ has a Multiplicative inverse in R/M

Let $U = \{ra + m / r \in R$ and $m \in M)$

<u>Claim that</u>,

U is an ideal of R

$(r_1 a + m_1) - (r_2 a + m_2) = (r_1 - r_2)a + (m_1 - m_2) \in U$

Also,

$r(r_1 a + m_1) = (rr_1)a + rm_1 \in U$

$\therefore U$ is an ideal of R (Since $rm_1 \in M$)

Now, let $m \in M$, Then

$$m = 0a + m \in U$$

$$M \subseteq U$$

Also $a = 1a + 0 \in U$ and $a \notin M$

$$M \neq U$$

$\therefore$ U is an ideal of R property containing M.

$\therefore$ But M is a maximal ideal of R

$\therefore U = R$. Hence $1 \in U$

$\therefore$ $1 = ba + m$ for some $b \in R$

Now,

$$M + 1 = M + ba + m$$

$$= M + ba \text{ (since } m \in M)$$

$$= (M + b)(M + a)$$

Hence $M + b$ is the inverse of $M + a$.

Thus, every non-zero element of R/M has an inverse. Hence R/M is a field.

Conversely,

Suppose R/M is field.

Let U be any ideal of R. property containing M.

$\therefore$ There exists an element $a \in U$ such that $a \notin M$

$\therefore$ $M + a$ is a non-zero element of R/M

Since, R/M is a field $M+a$ has an inverse, say $M+b$

$\therefore (M+b)(M+b) = M+1$

$\therefore M+ab = M+1$

$1-ab \in M$

But, $M \subseteq U$. Hence $1-ab \in U$

Also, $a \in U \Rightarrow ab \in U$

$\therefore 1 = (1-ab) + ab \in U$

$\therefore$ Thus $1 \in U$

$U = R$.

Thus there is no proper ideal of R property containing M.

Hence, M is a maximal ideal of R.