Counting principle:

Let H and K be a subgroups of a Group G. We define the product of H and K is HK by

$$HK = \{hk \mid h \in H \ \& \ k \in K\}$$

Lemma

① HK is a subgroup of G iff $HK = KH$.

proof

Assume that $HK = KH$

To prove that: HK is a subgroup

i.e) to prove that closed and every element in HK has its inverse in HK.

Suppose that $x = hk \in HK$

$y = h_1 k_1 \in HK$

Then $xy = hkh_1k_1$

$\because kh_1 \in KH = HK$

Now, $kh_1 = h_2k_2$ for some $h_2 \in H, k_2 \in K$

Here, $xy = hkh_1k_1$

$= h(kh_1)k_1$

$= h(h_2k_2)k_1$

$= (hh_2)(k_2k_1) \in HK$

HK is closed

Also, $x^{-1} = (hk)^{-1}$

$= k^{-1}h^{-1} \in KH = HK$

$x^{-1} \in HK$

Thus HK is a subgroup of G

Sufficient part:

Assume that HK is a subgroup of G

TPT : $HK = KH$

HK is a subgroup of G then for any

$h \in H, k \in K, h^{-1}k^{-1} \in HK$

and $kh = (h^{-1}k^{-1})^{-1} \in HK$

$KH \subset HK \rightarrow (1)$

Now if x is any element of HK

$x^{-1} = hk \in HK$

& $x = (x^{-1})^{-1} = (hk)^{-1}$

$= k^{-1}h^{-1} \in KH$

$HK \subset KH \rightarrow (2)$

From (1) & (2), we have

$HK = KH$

Note:

i) If H is a subgroup of Group G, then $H^2 = H \cdot H$ is a subgroup of G.

ii) If H & K are finite subgroup of G, then HK is a subgroup of G.

Thm: (2)

If H and K are finite subgroup of G of ~~order~~. $O(H)$ and $O(K)$ respectively. Then order of HK $[O(HK)] = \frac{O(H)\,O(K)}{O(H\cap K)}$

proof

We show that, any element $hk \in HK$ is repeated exactly $O(H\cap K)$, k times in the product of HK.

Now, $\alpha^{-1} \in H\cap K$, then $hk = h\alpha\alpha^{-1}k$

$= (h\alpha)(\alpha^{-1}k) \rightarrow (1)$

Here, $h\alpha \in H \;\forall\; h \in H \;\&\; \alpha \in H$

$\alpha^{-1}k \in K \;\forall\; \alpha^{-1} \in K \;\&\; k \in K$

Thus, hk is repeated in the product of HK.

Atleast $O(H\cap K)$, k times.

Let $hk = h_1 k_1$

$h_1^{-1}h = k^{-1}k_1$

we say that $\alpha \in H\cap K$

Also, we say that, $h_1 k_1 = h_1(\alpha\alpha^{-1})k_1$

$= (h_1\alpha)(\alpha^{-1}k_1)$

This shows that the repeat inside only in the form already considered in the form.

We conclude that hk repeated exactly $O(H\cap K)$ k-times in the product.

$\therefore O(HK) = \frac{O(H)\,O(K)}{O(H\cap K)}$

Scanned by TapScanner

Note:

Suppose H, K are subgroups of a finite group G. And $O(H) > \sqrt{O(G)}$, $O(K) > \sqrt{O(G)}$, $O(H \cap K) = 1$, then

$O(HK) = O(H)\,O(K)$ and

$O(G) = O(H)\,O(K)$

Thm

If $O(H) > \sqrt{O(G)}$ & $O(K) > \sqrt{O(G)}$.

Then $H \cap K \neq \{e\}$

Proof

W.K.T, $HK \leq O(G)$

$$O(G) \geq O(H)\,O(K)$$

$$O(G) \geq \frac{O(H)\,O(K)}{O(H \cap K)} \qquad [\because O(H \cap K) = 1$$

$$O(G) > \frac{\sqrt{O(G)}\sqrt{O(G)}}{O(H \cap K)}$$

$$O(G) > \frac{O(G)}{O(H \cap K)}$$

$$O(H \cap K) > 1$$

$$\therefore O(H \cap K) \neq e.$$

(3) Normal subgroups and Quotient groups:

Def:

A subgroup N of G is said to be Normal subgroup of G if for every $g \in G$ and $n \in N$, $gng^{-1} \in N$.

Lemma: (7)

(5)

N is a normal subgroup of G iff

$gNg^{-1} = N \ \forall \ g \in G.$

Proof

(i) Assume that $gNg^{-1} = N \ \forall g \in G$

TPT: N is a normal subgroup of G

If $gNg^{-1} = N \ \forall \ g \in G$ certainly

$gNg^{-1} \subseteq N$

$\therefore$ N is a normal subgroup of G

(ii) Assume that N is a normal subgroup of G

TPT $gNg^{-1} = N \ \forall \ g \in G$

Suppose N is a normal subgroup of G

Thus if $g \in G$ $gNg^{-1} \subseteq N$

& $g^{-1}Ng = g^{-1}N(g^{-1})^{-1} \subseteq N$

$g^{-1}Ng \subseteq N$

$N = g(g^{-1}Ng)g^{-1} \subset gNg^{-1} \subset N$

where $N = g^{-1}Ng \ \forall g \in G.$

Lemma:

The subgroup $N(G)$ is a normal subgroup of G iff every left ~~quotient~~ cosets of N in G is a right cosets of N in G.

Proof

Suppose that N is a normal subgroup of G.

TPT: Every left cosets of N in G is a right coset of N in G.

$\therefore$ N is a normal subgroup of G, then for every $g \in G$, $gNg^{-1} = N$

By

$$(gNg^{-1})g = Ng \text{ [cancellation law]}$$

$$\Rightarrow gN(g^{-1}g) = Ng$$

$$gN(e) = Ng$$

$$\therefore gN = Ng$$

Suppose conversely that every left cosets of N is a right coset of N in G.

TPT: N is a normal subgroup of G.

Thus for $g \in G$, gN being a left coset must be a right coset.

Now, $gN = Ng$

$$\Rightarrow gNg^{-1} = Ngg^{-1}$$

$$gNg^{-1} = Ne$$

$$\therefore gNg^{-1} = N$$

Hence, N is a normal subgroup of G.

Thm:

A subgroup N(G) is a normal subgroup of G iff the product of two right cosets of N in G is again a right coset of N in G.

Proof

Suppose N is a normal subgroup, then

$$NaNb = N(aN)b$$
$$= N(Na)b$$
$$= Nab$$
$$NaNb = Nab$$

Suppose that the product of any two right cosets of N is again a right cosets of N.

Then $NaNb$ is a right coset ~~containing ab~~ of N

~~Then NaNb is a right co~~

Further, $ab = (ea)(eb) \in (Na)(Nb)$

Hence, $NaNb$ is a right cosets containing ab.

$\therefore \quad NaNb = Nab$

Now, we prove that, N is a normal subgroup of G.

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

$$ana^{-1} = e\,ana^{-1}$$
$$= (ea)(na^{-1}) \in NaNa^{-1} = Naa^{-1}$$
$$= Ne$$
$$= N$$
$$ana^{-1} \in N$$

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

Quotient group:

Let N be a normal subgroup of G. Then the group G/N is called a quotient group (or) factor group.

Let G/N denote the collection of right cosets of N in G and we use the product of subsets of G. To yield for us a product of G/N.

Eg:

TP: G/N is a group.

i) Closure property:

$$x, y \in G/N \Rightarrow xy \in G/N$$

Let $x = Na$, $y = Nb$ for some $a, b \in G$

And $xy = NaNb$
$= Nab \in G/N$

(ii) Associative property:

$$x, y, z \in G/N \Rightarrow (xy)z = x(yz)$$

Let $x = Na$, $y = Nb$, $z = Nc$ for some $a, b, c \in G$

Now, $(xy)z = (NaNb)Nc$
$= (Nab)Nc$
$= N(ab)c$
$= Na(bc)$
$= Na(Nbc)$
$= Na(NbNc)$

$(xy)z = x(yz)$

iii) Identity property:

consider on element $N = Ne \in G/N$.

if $x \in G/N$, $x = Na$ for some $a \in G$.

Now, $xN = NaNe$
$= Nae$
$= Na = x$

$xN = x$

$|||^{ly}$, $Nx = x$

$\therefore xN = Nx = x$

Hence Ne is an identity element for G/N.

iv) Inverse property:

Suppose $x = Na \in G/N$, $a \in G$

Then $Na^{-1} \in G/N$ and

$$NaNa^{-1} = Naa^{-1}$$
$$= Ne$$

$|||^{ly}$, $Na^{-1}Na = Ne$

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

Here, Na^{-1} is the inverse element of Na of G/N.

$\therefore G/N$ is a group.

Homomorphism:

A mapping ϕ from a group G into a group G' is said to be a Homomorphism if for all $a, b \in G$, $\phi(ab) = \phi(a)\phi(b)$.

Eg: 1

$\phi : G \to G'$ defined by $\phi(x) = e \ \forall \ x \in G$, e is a identity element in G' is a trivial homomorphism.

i.e) $\phi(xy) = e \cdot e = \phi(x) \cdot \phi(y)$

Eg: 2

$\phi(x) = x$ for every $x \in G$ is a homomorphism.

i.e) $\phi(xy) = xy = \phi(x) \cdot \phi(y)$

$\therefore \phi$ is a homomorphism.

Eg: 3

Let G be a group of integers under addition. and let $G' = G$ for the integer $x \in G$ define ϕ by $\phi(x) = 2x$

$\phi : G \to G'$ defined by $\phi(x) = 2x$ (+)

$\phi(x+y) = 2(x+y) = 2x + 2y = \phi(x) + \phi(y)$

(5)

(4) Let G be a group of positive real numbers under multiplication and let G' be a group of all real numbers under addition. define $\phi : G \to G'$ by $\phi(x) = \log_{10} x$. ~~Then~~

$$\phi(xy) = \log_{10}(xy) = \log_{10} x + \log_{10} y$$

$$= \phi(x) + \phi(y)$$

$$\phi(xy) = \phi(x) + \phi(y)$$

Lemma:

(6) Suppose G is a group, N is a normal subgroup of G define the mapping ϕ from G to G/N by $\phi(x) = Nx \ \forall \ x \in G$. Then ϕ is a homomorphism of G onto G/N.

Proof

W.K.T, $\boxed{\phi \text{ is onto is trivial}}$.

For every element $X \in G/N \ \forall \ y \in G$

So, $X = \phi(x)$

Now, to prove that ϕ is a homomorphism

$$\phi(xy) = Nxy$$

Scanned by TapScanner

$$= Nx\,Ny$$

$$= x \cdot y$$

$$\phi(xy) = \phi(x) \cdot \phi(y)$$

$\therefore \phi$ is a Homomorphism.

Kernel: (7)

If ϕ is a homomorphism of G into G', the kernel of ϕ, K_ϕ is defined by

$$K_\phi = \{x \in G / \phi(x) = e'\}$$

[e' is the identity element of G']

Lemma:

If ϕ is a homomorphism of G onto G'. Then

i) $\phi(e) = e'$, the unit element of G'.

ii) $\phi(x^{-1}) = \phi(x)^{-1}$, $\forall x \in G$.

~~iii)~~

Proof

i) Given that ϕ is a homomorphism of $G \to G'$.

then Suppose $\phi(x)e' = \phi(x)$

$$= \phi(xe) \qquad \because \phi \text{ is homomorphism}$$

$$= \phi(x)\phi(e)$$

$$\phi(x)e' = \phi(x)\phi(e) \qquad \text{[By left Cancellation law]}$$

$$\therefore e' = \phi(e)$$

ii) W.K.T, $e' = \phi(e)$

$$= \phi(xx^{-1}) \qquad \because \phi \text{ is homomorphism}$$

$$e' = \phi(x)\phi(x^{-1})$$

$$(\phi(x))^{-1}e' = \phi(x^{-1}) \Rightarrow \therefore \phi(x^{-1}) = \phi(x)^{-1}$$

Lemma:

If ϕ is a homomorphism of G into G' with Kernel K. Then K is a normal subgroup of G.

Proof

We have to prove that K is a subgroup of G.

i.e) To prove that K is closed under multiplication and has inverse in it.

For every belonging to K.

i) K is closed:

If $x, y \in K$. Then $\phi(x) = e'$

& $\phi(y) = e'$

Where e' is the identity element in G'.

$\phi(xy) = \phi(x)\phi(y)$

$= e'.e'$

$\phi(xy) = e'$

$xy \in K$; $x, y \in K \Rightarrow xy \in K$

$\therefore K$ is closed.

ii) K is inverse:

If $x \in K$, then $\phi(x^{-1}) = \phi(x)^{-1}$

$= [\phi(x)]^{-1}$

$= [e']^{-1}$

$\phi(x^{-1}) = e'$

$\therefore x^{-1} \in K$

$\therefore x \in K \Rightarrow x^{-1} \in K$

$\therefore x^{-1}$ is a inverse element of x in K.

Hence K is a subgroup of G.

Scanned by TapScanner

TPT : K is a normal subgroup of G.

i.e) To prove that for any $g \in G$, $k \in K$, $gkg^{-1} \in K$.

Now, $\phi(gkg^{-1}) = e'$ whenever $\phi(k) = e'$.

$\Rightarrow \phi(gkg^{-1}) = \phi(g)\phi(k)\phi(g^{-1})$ $\because$ (ϕ is homomorphism)

$= \phi(g) e' \phi(g^{-1})$

$= \phi(g)\phi(g^{-1})$ $\because (\phi(g^{-1}) = \phi(g)^{-1})$

$\phi(gkg^{-1}) = e$

$\therefore gkg^{-1} \in K$

Hence K is a normal subgroup of G.

(a)

(i) Fundamental theorem of Homomorphism:

Let ϕ be a homomorphism of G onto G' with kernel K. Then $G/K \cong G'$.

Proof Let K be the kernel of the homomorphism of $\phi : G \to G'$, then K is a normal subgroup of G.

Consider the quotient group of G/K and the mapping $\phi : \frac{G}{K} \to G'$.

Given by $\phi_1(Kx) = \phi(x) \forall Kx \in G/K$

i) ϕ_1 is well defined:

Let $Kx = Ky$

$\Rightarrow xy^{-1} \in K$ $\because x \in K$ if $\phi(x) = e'$

$\phi(xy^{-1}) = e'$ $(\because \phi(x^{-1}) = \phi(x)^{-1} = [\phi(x)]^{-1}$

$\phi(x)\phi(y^{-1}) = e'$

$\phi(x)[\phi(y)]^{-1} = e'$

$\phi(x) = \phi(y)$

$\phi_1(kx) = \phi_1(ky)$

$\therefore$ ϕ is well defined.

ii) ϕ_1 is 1-1 :

Let $\phi_1(kx) = \phi(x)$ and $\phi_1(ky) = \phi(y)$

$\phi_1(kx) = \phi_1(ky)$ where $kx, ky \in G/_k$

$\Rightarrow \phi(x) = \phi(y)$

$\Rightarrow \phi(x)[\phi(y)]^{-1} = e'$

$\Rightarrow \phi(x)(\phi(y^{-1})) = e'$

($\because \phi$ is homomorphism)

$\Rightarrow \phi(xy^{-1}) = e'$

$\Rightarrow xy^{-1} \in k$

$\Rightarrow kx = ky$

$\therefore \phi_1$ is 1-1.

iii) ϕ_1 is onto :

Let $xz \in G$ $\exists$ an element $x \in G$

$\ni: \phi(x) = xz$

$\Rightarrow \phi_1(kx) = \phi(x) = xz$ $\quad \because \phi_1(kx) = \phi(x)$

$\phi_1(kx) = xz$

$\therefore \phi_1$ is onto.

IV) ϕ_1 preserves operation :

Let $kx, ky \in G/_k$ be an arbitary element.

Then, $\phi_1(kx\,ky) = \phi_1(kxy)$

$= \phi(xy)$

$= \phi(x)\phi(y)$

Scanned by TapScanner

$= \phi_1(kx)\,\phi_1(ky)$

$\phi_1(kx\,ky) = \phi_1(kx)\,\phi_1(ky)$

ϕ_1 is homomorphism.

Hence $G/K \cong G'$

Isomorphism :

Let $\phi : G \to G'$ be a group homomorphism.

We say that ϕ is an isomorphism that is to satisfy ϕ is one to one & onto.

Monomorphism & Epimorphism :

Let $\phi : G \to G'$ be a group homomorphism.

We say that ϕ is monomorphism if ϕ is one-one.

We say that ϕ is Epimorphism if ϕ is onto.

Automorphism :

A group homomorphism $\phi : G \to G'$ is isomorphism then it is called Automorphism.

Corollary :

Homomorphism ϕ of G into G' with kernel K_ϕ is an isomorphism of G into G' iff $K_\phi = \{e\} = (e)$.

Proof

Let ϕ be a isomorphism.

TPT : $K_\phi = \{e\}$

Let $x \in K_\phi$ be an arbitary element.

Scanned by TapScanner

$\Rightarrow x \in G$

$\Rightarrow \phi(x) = e'$, where e' is the identity element in G'.

$\Rightarrow \phi(x) = \phi(e) = e'$

$\phi(x) = e = e'$

$\therefore K_\phi = \{e\}$

Conversely, let $K_\phi = \{e\}$

TPT : ϕ is an isomorphism.

Suppose $\phi(x) = y$ where $x, y \in G$.

$\Rightarrow \phi(x)\,(\phi(y))^{-1} = e'$

$\phi(x)\,\phi(y^{-1}) = e$

$\phi(xy^{-1}) = e$

$xy^{-1} \in K_\phi$

$xy^{-1} = e'$

$x = y$

K_ϕ is one - one

K_ϕ is an isomorphism.

(10) Cauchy's Theorem for abelian groups:

Statement:

Suppose G is a finite abelian group and $\frac{p}{o(G)}$, p is a prime number. Then there is an element $a \neq e \in G \ni : a^p = e$

proof

We have to prove the theorem on induction of $o(G)$.

i) G has no subgroup:

If G has no subgroup $H \neq (e), G$.

But G must be cyclic of prime order.

i.e) the prime must be p and G has $p-1$ elements $a \neq e$ statisfying $a^p = a^{o(G)} = e$.

Hence $a^p = e$

ii) G has subgroups:

Suppose G has subgroups, $N \neq e, G$

If $\frac{p}{o(N)}$ by our induction hypothesis.

Since $N \subset G \Rightarrow o(N) < o(G)$, and N is abelian.

$\exists$ an element $b \in N$, $b \neq e \ni : b^p = e$

Since $b \in N \subset G$.

Assume that p does not $o(N)$

Since G is abelian, N is a normal subgroup of G

so G/N is a group.

$$o(G/N) = \frac{o(G)}{o(N)}$$

$$\Rightarrow \frac{p}{\frac{o(G)}{o(N)}} < o(G)$$

$$\Rightarrow \frac{p}{o(G)}$$

Since G is abelian, G/N is abelian.

Thus by our induction hypothesis there exist an element $x \in G/N$ satisfying $x^p = e_1$, Then the unit element of G/N.

Now, the element of G/N, $x = Nb$, $b \in G$.

$$\Rightarrow x^b = (Nb)^b \Rightarrow Nb^b$$

$$Nb^b = N, \quad N_b \neq N$$

$$b^b \in N, \quad b \notin N$$

$$\therefore [e_1 = Ne, \quad x^p = e_1, \quad x \neq G]$$

By Lagrange's theorem $(b^p)^{o(N)} = e$ (or)

$$b^{o(N)^p} = e$$

Let $c = b^{o(N)} \Rightarrow c^p = e, \quad c \neq e$

if $c = e \Rightarrow b^{o(N)} = e$

$$\Rightarrow (Nb)^{o(N)} = N \Rightarrow (Nb)^p = N$$

$p \times o(N)$, p is a prime number we find that

$N_b = N$, $b \in N$

Which is Contradiction

$$\therefore c \neq e, \quad c^p = e$$

Thm

Let ϕ be a homomorphism of G onto G' with kernel K and let N' be a normal subgroup of G', $N = \{x \in G / \phi(x) \in N'\}$. Then G/N is isomorphic to G'/N'. $[G/N \cong G'/N']$ equivalently $G'/N' \cong \dfrac{(G/K)}{(N/K)}$.

Proof

We have $\theta : G' \to G'/N'$ is a onto group homomorphism with kernel K and $\theta(g') = N'g'$.

Define $\psi : G \to G'/N'$ by $\psi(g) = N'\phi(g)\ \forall g \in G$.

i) ψ is onto:

if $g' \in G'$, $g' = \phi(g)$ for some $g \in G$

$\therefore \phi$ is homomorphism $\exists$ an element $N'g' \in G'/N'$

$\ni: N'\phi(g) = \psi(g)$

$\therefore \phi$ is onto.

ii) ψ is homomorphism:

if $a, b \in G$, $\psi(ab) = N'\phi(ab)$

ϕ is homomorphism

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

$\psi(ab) = N'\phi(a)\phi(b)$

$\psi(ab) = N'\phi(a)N'\phi(b)$

$= \psi(a)\psi(b)$

$\because \psi(ab) = \psi(a)\psi(b)$

$\therefore \psi$ is homomorphism.

Now, kernel T of ψ

If $n \in N$, $\phi(n) \in N'$ so that $\psi(n) = N'\phi(n)$
$= N'$

the identity element of G'/N'

$N \subset T$, if $t \in T$, $\psi(t) = N'\phi(t)$
$= N'$

Comparing these two evaluation element of

$\psi(t) \Rightarrow \quad N' = N'\phi(t)$

$\Rightarrow \phi(t) \in N'$ $\quad \begin{cases} (\psi(n) = N') \\ (\psi(t) = N') \end{cases}$

But this place $t \in N$ by the definition of N.

Then ψ is a homomorphism of G onto G'/N', with kernel N.

By the previous theorem, $\frac{G}{N} \cong \frac{G'}{N'}$. The last statement is $G' \cong G/K$ and $N' \cong N/K$.

$$\therefore \frac{G'}{N'} \cong \frac{(G/K)}{(N/K)}$$

UNIT-2

$A(G) \neq \phi$

Automorphism:

Let G be a group and let $\mathcal{A}(G)$ denote the set of all automorphism of G being a subset of A(G), the set of all permutation of the set G also $A(G) \neq \phi$. Since I in A(G)

Thm:

If G is a group. $\mathcal{A}(G)$ is a Automorphism of G. Then $\mathcal{A}(G)$ is a subgroup of A(G).

Proof:

If $T_1, T_2 \in \mathcal{A}(G)$, WKT $T_1 T_2 \in A(G)$

For $x, y \in G$

$$\left.\begin{aligned}(xy)T_1 &= (xT_1)(yT_1)\\ (xy)T_2 &= (xT_2)(yT_2)\end{aligned}\right\} \text{conditions}$$

$$\begin{aligned}(xy)T_1T_2 &= ((xy)T_1)T_2\\ &= ((xT_1)(yT_1))T_2\\ &= [(xT_1)T_2][(yT_1)T_2]\\ &= (xT_1T_2)(yT_1T_2)\end{aligned}$$

i.e) $T_1T_2 \in \mathcal{A}(G)$

if $T \in A(G)$ Then $T^{-1} \in \mathcal{A}(G)$

if $x, y \in G$. Then

$$\begin{aligned}((xT^{-1})(yT^{-1}))T &= ((xT^{-1})T)((yT^{-1})T)\\ &= (x(T^{-1}T))(y(T^{-1}T))\\ &= (xI)(yI)\\ &= xy\end{aligned}$$

$$(xT^{-1})(yT^{-1}) = (xy)T^{-1}$$

Hence, $\mathcal{A}(G)$ is a subgroup of A(G)

Inner Automorphism :

Let a be an element of a group G. The Automorphism $f_a : G \to G$ given by $f_a(x) = axa^{-1}$ $\forall a \in G$ is called an inner automorphism of G. determined by G.

$In(G)$ is denote the set of all inner automorphism of G.

Centre :

$Z(G) = \{ a \in G \,/\, ax = xa \ \forall x \in G \}$ is called Centre of G.

Thm :

For any group G, ~~...~~ $In(G)$ is a normal subgroup of $A(G)$. Further, $In(G) \cong G/Z(G)$ where $Z(G)$ denote the centre of G.

Proof

Clearly $I \in In(G)$ as $I(x) = x = exe^{-1}$

$$= f_e(x) \ \forall x \in G$$

Now, for any $a \in G$, $x \in G$

$$f_a \circ f_{a^{-1}}(x) = f_a(f_{a^{-1}}(x))$$

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

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

$$= a(a^{-1}xa)a^{-1} \quad [\because f_a(x) = axa^{-1}]$$

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

$$f_a \circ f_{a^{-1}}(x) = x$$

$$f_a \circ f_{a^{-1}} = I$$

|||ly,
$$f_{a^{-1}} \circ f_a = I$$

$$\therefore\ f_a \circ f_{a^{-1}} = f_{a^{-1}} \circ f_a = I$$

$$(f_a)^{-1} = f_{a^{-1}} \in In(G)$$

Also for any $f_a, f_b \in In(G) \Rightarrow f_{ab} \in In(G)$

if $x \in G$

$$\begin{aligned}(f_a \circ f_b)(x) &= f_a(f_b(x)) \\ &= f_a(bxb^{-1}) \\ &= a(bxb^{-1})a^{-1} \\ &= (ab)x(ab)^{-1} \\ &= f_{ab}(x)\end{aligned}$$

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

$$f_a \circ f_b = f_{ab} \in In(G)$$

Hence $In(G)$ is a subgroup of $A(G)$.

Next, we prove that $In(G)$ is a normal subgroup of $A(G)$. It's only remains prove that for any $f_a \in In(G)$

$$f_a \in In(G),\ \sigma \in A(G),\ \sigma \circ f_a \circ \sigma^{-1} \in In(G)$$

Let $x \in G$, then $(\sigma \circ f_a \circ \sigma^{-1})(x) = \sigma \circ f_a(\sigma^{-1}(x))$

$f_a(x)$

$f \circ (a^{-1}\sigma(x)a)$ $\quad = \sigma \circ (a\sigma^{-1}(x)a^{-1})$

axa^{-1}

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

$a \quad x \quad a^{-1}$

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

$$= f_{\sigma(a)}(x)$$

$$(\sigma \circ f_a \circ \sigma^{-1})(x) = f_{\sigma(a)}(x)$$

Scanned by TapScanner

Hence, $\sigma \circ f_a \circ \sigma^{-1} = f_{\sigma(a)} \in In(G)$

$\therefore$ $In(G)$ is a normal subgroup of $A(G)$

$$In(G) \cong \frac{G}{Z(G)} :$$

We define a mapping $g : G \to In(G)$ by

$g(a) = f_a \quad \forall a \in G$

then $g(ab) = f_{ab}$

$= f_a \circ f_b$

$= g(a) \circ g(b)$

$g(ab) = g(a) \circ g(b)$

Given that g is homomorphism, g is onto.

Since each member of inner automorphism of G is of the form f_a and by the definition $f_a = g(a)$. Then by applying fundamental theorem of homomorphism. We get, $In(G) \cong \frac{G}{\ker(g)}$

<u>Claim</u>: $\ker g = Z(G)$.

Now, $a \in \ker g \Leftrightarrow g(a) = I$, where I is identity - element

$f_a = I$

$f_a(x) = I(x)$

$axa^{-1} = x$ Centre ($Z(G)$) $\Downarrow$ $ax = xa$

$ax = xa$

Hence $\ker g = Z(G)$

$$\therefore In(G) \cong \frac{G}{Z(G)}$$

Scanned by TapScanner

(9) Cayley's theorem : 2.9

Statement :

(11) Every group is isomorphic to a Permutation group.

Proof

Let G be a group and let $A(G)$ denote the group of all Permutation of the set G.

For each $a \in G$ define a map $f_a : G \to G$ by $f_a(x) = ax$ $\forall x \in G$.

i) f_a is 1-1 :

for any $a \in G$, $f_a(x) = f_a(y)$

$$ax = ay$$

$$x = y$$

$\therefore$ $f_a(x) = f_a(y) \Rightarrow x = y$

Hence f_a is 1-1.

ii) f_a is onto :

Further, $f_a(a^{-1}x) = a^{-1}(ax)$

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

$= ex$

$= x$

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

f_a is onto.

Hence $f_a \in A(G)$.

Now for any $a, b \in G$ & $x \in G$

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

$= f_a(bx)$

$= a(bx)$

$= (ab)(x)$

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

$f_a \circ f_b = f_{ab}$

Now, $\sigma : G \to A(G)$ by $\sigma(a) = f_a \quad \forall a \in G$

Then for all $a, b \in G$

$$\sigma(ab) = f_{ab}$$
$$= f_a \circ f_b$$
$$= \sigma(a) \circ \sigma(b)$$
$$\sigma(ab) = \sigma(a) \circ \sigma(b)$$

Moreover, $\sigma(a) = \sigma(b)$

$$f_a = f_b$$
$$f_a(e) = f_b(e)$$
$$ae = be$$
$$a = b$$
$$\therefore \sigma_a = \sigma_b \Rightarrow a = b$$

Thus, σ is 1-1 and Homomorphism of G into $A(G)$.

Hence, G is isomorphic to $\sigma(G)$ which being a subgroup of $A(G)$ is a permutation group.

Thm:

If G is a group, H is a subgroup of G and S is the set of all right cosets of H in G. Then there is a homomorphism θ of G into $A(S)$ and the kernel of θ is a largest normal subgroup of G which is contained in H.

Proof

Define $\theta : G \to A(S)$ by $\theta(g) = T(g)$

where $T_g(xH) = gxH \quad \forall xH \in S$

Firstly, we show that $T_g \in A(S)$

Scanned by TapScanner

Clearly, $T_g : S \to S$

i) T_g is 1-1:

$T_g(xH) = T_g(yH) \ \forall \ xH, yH \in S$

$\Rightarrow gxH = gyH$

$\Rightarrow (gy)^{-1}(gx) \in H$

$\Rightarrow g^{-1}y^{-1}(gx) \in H$

$\Rightarrow y^{-1}x \in H$

$\Rightarrow xH = yH$

$\therefore T_g(xH) = T_g(yH) \Rightarrow xH = yH$

Since, T_g is 1-1.

ii) T_g is onto:

For any left coset $xH \in S$ can be written

us $g(g^{-1}xH)$.

i.e) $T_g(g^{-1}xH) = g(g^{-1}xH)$

$= gg^{-1}xH$

$= exH$

$T_g(g^{-1}xH) = xH$

$\therefore T_g$ is onto.

Consequently, $T_g \in A(S)$

WKT, $\theta(g) = T_g$

Again, $\theta(gh) = T_{gh}$

Where $T_{gh}(xH) = gh(xH)$

$= T_g(hxH)$

$= T_g \, h(xH)$

$T_{gh}(xH) = T_g T_h(xH)$

$T_{gh} = T_g T_h$

$\theta_{gh} = \theta_g \theta_h$

θ is homomorphism from G into $A(S)$.

Now $g \in \ker \theta \Rightarrow T_g = I$ where I is the identity element in $A(S)$.

$\Rightarrow \quad T_g(eH) = eH$

$\Rightarrow \quad geH = eH$

$\Rightarrow \quad gH = H$

$\Rightarrow \quad g \in H$

i.e) $g \in \ker\theta$ & $g \in H \Rightarrow \ker\theta \subseteq H$

Further if N is a normal subgroup of G contained in N.

Then for each $n \in N$

$\theta(n) = T_n$ where $T_n(xH) = nxH$

$= xx^{-1}nxH$

$= x(x^{-1}nx)H \quad \forall x \in G$

But $I = [br_1, [(1s_2)(1s_3)(1s_4)] \cdots (1s_t)] \rightarrow (1)$

$(b \neq r_1, \; s_2, s_2 \cdots s_t \in S)$

With none of $s_i = r_1$ and some $b \neq r_1$ in S.

Since r_1 is left fixed by $1s_2, 1s_3, \cdots$, we get in (1) that the right hand side [RHS] gives the image of r_1 is b.

Which is a contradiction, since I being identity element. The image of r_1 should be r_1 itself. Hence the result.

Now, N is a normal subgroup of G

$x^{-1}nx \in N \subseteq H$

$\Rightarrow x^{-1}nx \in H$ $\Rightarrow nxH = xH$

i.e) $T_n(xH) = xH \ \forall \ x \in G$

$\Rightarrow T_n = I$

Hence $n \in \ker\theta$

i.e) $n \in N$ & $n \in \ker\theta$ $(\because \ker\theta \subseteq H)$

$\underline{N \subseteq \ker\theta}$

Hence, the kernel θ is a normal subgroup of G which is contained in H.

__Lemma:__

If G is a finite group and $H \neq G$ is a subgroup of G. Such that $o(G) \nmid$ (does not divides) $i(H)!$. Then H must contain a non-trivial normal subgroup of G. In particular, G can't be simple.

$i(H)$ is just a value. It is given

Bijection not satisfied

__Proof__ By the previous thm, $\ker\theta \subseteq H$

$\because H \neq G \Rightarrow \ker\theta \neq G$

Further if $\underline{\ker\theta = \{e\}}$ where e is the identity element in G.

Then $\dfrac{G}{\ker\theta} \cong T$ where T is a subgroup of $A(S)$.

$\frac{G}{1} = T \Rightarrow G = T \Rightarrow o(G) = o(T)$

Given that $o(G) = o(T)$ must be factor of $o(A(S))$.

But $o(A(S)) = i(H)!$

$\Rightarrow o(G) / i(H)!$

Which is against a hypothesis.

Hence $\ker\theta \neq \{e\}$. Thus H contains a non-trivial normal subgroup of G.

Permutation groups:

Let $x \neq \phi$. For any mapping $f : x \to x$ is called transformation. Let X be a non-empty finite set. A one to one (1-1), onto mapping, $f : x \to x$ is called a permutation.

The number of elements of the finite set x, this known as degree of permutation.

~~Sample~~ Symbol of permutation:

Let $x = \{a_1, a_2 \ldots a_n\}$, $a_i \neq a_j$. Then, x contains n distinct elements. Let f be a permutation on x such that $f(a_i) = b_i$ for $1 \leq i \leq n$.

The elements $b_1, b_2 \ldots b_n$ are nothing but the arrangement at n elements of x.

i.e) $f = \{(a_1, a_2 \ldots a_n)(f(a_1) f(a_2) \ldots f(a_n))\}$

We write,

$$f = \begin{pmatrix} a_1 & a_2 & \ldots & a_n \\ b_1 & b_2 & \ldots & b_n \end{pmatrix}$$

$(f(a_1))\ (f(a_2))\ \ldots\ f(a_n)$

Equality of two Permutation :

Let f and g be two permutation on the set S. Then, we define

$$f = g \text{ if } f(x) = g(x) \quad \forall x \in S.$$

note :

A permutation $\begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ b_1 & b_2 & \cdots & b_n \end{pmatrix}$ can be expressed as follows :

$$\begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ b_1 & b_2 & \cdots & b_n \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & \cdots & a_i & \cdots & a_{n-1} & a_n \\ b_1 & b_2 & \cdots & b_i & \cdots & b_{n-1} & b_n \end{pmatrix}$$

Sometimes, the interchange of column can't use in the natural permutation

Total number of Permutation :

Let x be the set of all n distinct elements and x can be written in $n!$ different ways. If P_n be the set containing of all permutation of degree n.

Thus, $P_n = \{ x / f_i, f$ is a permutation of degree $n \}$.

This set P_n is called set of Permutation of degree n and denote the symbol S_n.

Identity Permutation :

A permutation I on X is called identity permutation if $I(x) = x, \forall x \in X$.

Scanned by TapScanner

Inverse permutation:

If $f = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ b_1 & b_2 & \cdots & b_n \end{pmatrix}$ is a

permutation on X. Then $f^{-1} = \begin{pmatrix} b_1 & b_2 & \cdots & b_n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix}$

is called inverse permutation of f.

Product Composition of two Permutation:

Let $x =$ ~~set of all~~ $\{a_1, a_2 \cdots a_n\}$ and

$f : x \to x$ and $g : x \to x$ be onto and 1-1 maps.

Then f and g are permutation of degree n.

Clearly, $g \circ f : x \to x$ and also

$f \circ g : x \to x$ are one to one and onto

belongs. Hence $f \circ g$ and $g \circ f$ are permutation of

degree n.

(13)

Eg: $\phi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$ & $\psi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}$

Find $\phi\psi$.

Soln

$$\phi\psi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$$

Cyclic permutation: [Initial & Final are same]

Let S be a finite sets. A permutation

~~f~~ of S is said to be a cyclic permutation

(or) a cyclic if there exists an elements

Scanned by TapScanner

$a_1, a_2 \cdots a_n a_1$ in S. Such that $f(a_1) = a_2$, $f(a_2), f(a_3); \cdots f(a_{n-1}) = a_n, f(a_n) = a_1$

and for any $j \in S$ different from $a_1, a_2 \cdots a_n$. $f(j) = j$, we denote f by the symbol $(a_1, a_2 \cdots a_n)$. This notation of f is called a one row notation.

Further, n is called the length of the cycle of f. A cycle of length n is also called a n-cycle

Orbit:

A Permutation f of a Set S is cycle if S has atmost f orbit having more than one element.

Eg ① Let $S = \{1, 2, 3, 4\}$. Then $(1\ 3\ 2)$ denote the permutation f of S. Such that $f(1) = 3$, $f(3) = 2$, $f(2) = 1$, $f(4) = 4$. Thus in the two rowed notation of f we have.

$$(1\ 3\ 2) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$$

$\therefore$ f is a cyclic permutation of length 3.

i.e) $(1\ 3\ 2) = (2\ 1\ 3) = (3\ 2\ 1)$

② $(1\ 2)$ is a cyclic Permutation of $\{1, 2, 3, 4\}$ of length 2.

$$(1\ 2) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$$

Eg: orbit of Permutation:

$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$. Find orbit of Permutation.

Soln: Orbit = (1 2 3) (4 5)

Transposition:

A cycle of length 2 is called Transposition

Eg: $\theta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 8 & 1 & 6 & 4 & 7 & 5 & 9 \end{pmatrix}$. Find orbit and cycle of θ.

Soln:

$1\theta = 2$; $1\theta^2 = 1\theta \cdot \theta = 2\theta = 3$

$1\theta^3 = 1\theta^2 \cdot \theta = 3\theta = 8$

$1\theta^4 = 1\theta^3 \cdot \theta = 8\theta = 5$

$1\theta^5 = 1\theta^4 \cdot \theta = 5\theta = 6$

$1\theta^6 = 1\theta^5 \cdot \theta = 6\theta = 4$

$1\theta^7 = 1\theta^6 \cdot \theta = 4\theta = 1$

$\therefore$ Orbit of 1 is the set {1 2 3 8 5 6 4}

Orbit of 7 & 9 is {7}, {9}

Cycle is (7), (9), $(1, 1\theta, 1\theta^2, 1\theta^3, 1\theta^4, 1\theta^5, 1\theta^6, 1\theta^7)$ = (1 2 3 8 5 6 4)

Disjoint permutation:

Two permutation f and g of a set X are said to be disjoint if ~~the~~ satisfied the following conditions:

i) for any $j \in X$, $f(j) \neq j \Rightarrow g(j) = j$

(ii) for any $j \in X$, $g(j) \neq j \Rightarrow f(j) = j$

(i.e) If any element of X is moved by f, then it is left fixed by g and if any element of X is moved by g, then it is left fixed by f.

Eg: Let $X = \{1, 2, 3, 4, 5\}$, $f = (1\ 3\ 2)$ and $g = (4\ 5)$

By the definition,

(i) $f(1) = 3$, $f(2) = 1$, $f(3) = 2$ but $g(1) = 1$
$g(2) = 2$, $g(3) = 3$.

(ii) $g(4) = 5$, $g(5) = 4$ but $f(4) = 4$, $f(5) = 5$

This shows that f and g are disjoint permutation.

Eg: Let $S = \{1, 2, 3, 4, 5, 6\}$ and $\theta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 5 & 6 & 4 \end{pmatrix}$

Soln:

The orbit of 1.

Consider of $1\theta = 2$

$1\theta^2 = 1\theta \cdot \theta = 2\theta = 1$

The orbit of 1 is a set of elements 1 & 2.

The orbit of 2 is a same set of elements 1 & 2

The orbit of 3 consist just of 3.

The orbit of 4 consist of a set of elements 4, 5 and 6.

$4\theta = 5$

$4\theta^2 = 4\theta \cdot \theta = 5\theta = 6$

$4\theta^3 = 4\theta^2 \cdot \theta = 6\theta = 4$

$\therefore$ The cycle of θ are $(1\ 2)$, (3), $(4\ 5\ 6)$.

Scanned by TapScanner

Even or odd permutation:

A permutation f of a finite non-empty set S is said to be even or odd according as f is expressable as a product of even or odd number of transposition.

Thm

Every permutation is a product of its cycle.

Proof

Let θ be the permutation. Then its cycles of the form $(s, s\theta, s\theta^2, \ldots s\theta^{t-1})$ by the multiplication of cycles, we know that,

The cycle of θ are disjoint.

The image of $s' \in S$ under θ which is $s'\theta$ is the same as the image of s' under the product, φ of all the distinct cycle of θ. So θ, φ have the same effect on every element on S.

Hence $\theta = \varphi$.

$\therefore$ Every permutation is a product of its cycle.

Lemma: (16)

Every permutation is a product of 2-cycles.

proof

Consider the m-cycles $(1, 2, 3 \ldots m)$.

A simple computation shows that $(1,2,3 \cdots m) = (1,2)(1,3), \ldots\ldots (1,m)$.

More generally the m cycles,

$(a, a_2 \cdots a_m) = (a, a_2)(a, a_3) \cdots\cdots (a, a_m)$.

This decomposition is not unique by this, we mean that an m cycle can be written as a product of 2-cycles is more than one way.

For instance, $(1\ 2\ 3) = (1\ 2)(1\ 3) = (3\ 2)(3\ 1)$

Since every permutation is a product of disjoint cycles and every cycle is a product of 2-cycles.

Hence the proof.

UNIT-3

Another Counting Principle

Definition: Conjugate.

If $a, b \in G$. Then b is said to be a Conjugate of a in G if there exists an element $c \in G \ni: b = c^{-1}ac$.

Symbol $a \sim b$ is denote that a is conjugate of b.

Lemma:

The relation of conjugacy is an equivalence relation on G

Proof

i) Reflexivity: $a \sim a$

$$a = a^{-1}aa \quad \forall a \in G$$

$$\Rightarrow a \sim a$$

(ii) Symmetry: $a \sim b \Rightarrow b \sim a$

Now $a \sim b \Rightarrow a = x^{-1}bx \quad \forall x \in G, a, b \in G$

$$\Rightarrow b = x^{-1}ax$$

$$b = a$$

Hence $a \sim b \Rightarrow b \sim a$

iii) Transitivity:

$$a \sim b, b \sim c \Rightarrow a \sim c$$

$a \sim b$, $b \sim c \Rightarrow a = x^{-1}bx$, $b = y^{-1}cy$

$\forall x, y \in G$

$$a = x^{-1}(y^{-1}cy)x$$

$a = x^{-1}y^{-1}(c)\, yx$

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

$a \sim c$

Hence $a \sim b,\ b \sim c \Rightarrow a \sim c$.

Definition: 19

Centralizer (or) Normalizer of an element.

For any element $a \in G$, the set

$N(a) = \{x \in G / ax = xa\}$ is called

Normalizer (or) Centralizer of a in G.

Lemma 20

N(a) is a subgroup of G.

21/8/19

Proof: If e is an identity element of G,

then $ea = ae$

$\Rightarrow e \in N(a)$

So that $N(a) \neq \phi$

Let $x, y \in N(a)$

$(xy)a = x(ya)$

$= x(ay)$

$= (xa)y$

$= (ax)y$

$(xy)a = a(xy)$

$\therefore xy \in N(a) \Rightarrow xy \in N(a)$

Again, $xa = ax$

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

$x \in N(a) \Rightarrow x^{-1} \in N(a)$

$\therefore$ N(a) is a subgroup of G.

Scanned by TapScanner

Theorem

If G is a finite group, then $C_a = \frac{O(G)}{O(N(a))}$

(Or) The number of elements conjugate to a in G is the index of the normaliser of a in G.

Proof

Let $O(G) = n$

If $N(a)$ has t distinct right cosets,

$N(a)x_1, N(a)x_2 \ldots N(a)x_t$.

Then, We know that, $t = \frac{O(G)}{O(N(a))}$

Now, for $1 \leq i, j \leq t$,

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

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

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

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

$$\Rightarrow x_i x_j^{-1} \in N(a)$$

$$\Rightarrow N(a) x_i = N(a) x_j$$

$$\Rightarrow i = j$$

Since, $N(a) x_i$'s are all distinct elements.

Hence $x_i^{-1} a x_i = x_j^{-1} a x_j$

$$\Rightarrow i = j$$

So, $x_1^{-1} a x_1, x_2^{-1} a x_2 \ldots x_t^{-1} a x_t$ are all distinct conjugate of a.

If we show that, these are the only conjugate of a.

Then, it follows that C_a (or) $C(a)$ contains only t-elements.

i.e) $C_a = t = \dfrac{o(G)}{o(N(a))}$

Consider for some $x \in G$, $b = x^{-1}ax$

Since, $G = \bigcup_{i=1}^{t} N(a)x_i$, $x = cx_i$ for some $c \in N(a)$

and some +ve integers i.

$$\therefore x^{-1}ax = (cx_i)^{-1} a (cx_i)$$
$$= x_i^{-1} c^{-1} a c x_i$$
$$= x_i^{-1} (c^{-1} a x) x_i$$
$$= x_i^{-1} a x_i$$

Hence, any conjugate b of a is equal to 1 of $x_i^{-1} a x_i$.

This proves that a has only t conjugate $x_i^{-1} a x_i$, $i = 1$ to t.

Hence the proof.

26/8/ Definition:

Let G be a finite group. The equation

$$o(G) = o(Z(G)) + \sum_a \frac{o(G)}{o(N(G))}$$

where $\sum_a$ is the sum runs over element a, taken one from each of those distinct conjugate ~~[illegible]~~ classes which contains more than one elements is called the class equation of the group G.

Thm (2)

If $O(G) = p^n$ where p is a prime number then $z(G) \neq e$

Proof

Let $O(z(G)) = z$

By the definition,

$$O(G) = O(z(G)) + \Sigma \frac{O(G)}{O(N(a))}$$

$$p^n = z + \sum_a \frac{O(G)}{O(N(a))} \longrightarrow (1)$$

Where sum runs over elements a, taken 1 from each of conjugate classes C_a (or) $C(a)$ which has more than 1 elements.

Now for each $a \notin z(G)$

$O(N(a)) < O(G) = p^n$ and

$O(N(a)) / O(G)$ gives $O(N(a)) = p^{n_a}$ for some $1 \leq n_a < n$.

$$\Rightarrow p \,/\, \frac{O(G)}{O(N(a))}$$

Further hence from equ (1) we get,

$$\frac{p}{z}$$

this proves that $\frac{p}{O(z(G))}$

$\Rightarrow O(z(G)) > 1$

$\Rightarrow z(G) \neq e$

Corollary

If $o(G) = p^2$ where p is a prime number.
Then G is abelian.

proof

A group G is abelian iff $z(G) = G$.

It is sufficient to show that ~~$o(G) = p^2$~~

$$o(G) = p^2 \Rightarrow z(G) = G$$

Given that $o(G) = p^2$

By Lagrange's thm, $o(z(G)) / p^2$

$$\therefore o(z(G)) = 1, \ p \text{ (or) } p^2$$

By the previous thm, $o(z(G)) \neq 1$.

$$o(z(G)) = p \text{ (or) } p^2$$

Suppose $o(z(G)) = p$

Consider $a \in G \ni : a \notin z(G)$

Since for every $b \in z(G)$,

$ab = ba$: $b \in N(a)$

Thus $z(G) \subseteq N(a)$

Also $a \in N(a)$ but $a \notin z(G)$

so $N(a) \neq z(G)$

Consequently, $o(N(a)) > o(z(G)) = p$

But $o(z(G)) / p^2$

Thus $o(z(G)) = p^2$ and $N(a) = G$

$\Rightarrow a \in z(G)$ which is contradiction $a \notin z(G)$

$\therefore o(z(G)) = p^2$.

Hence $G = z(G)$

Scanned by TapScanner

28/8/19 Cauchy's theorem for finite group:

Statement:

If p is a prime number and $\frac{p}{o(G)}$ then G has an element of order p.

Proof:

Suppose an element $a \neq e \in G \Rightarrow a^p = e$

To prove that, theorem by induction hypothesis on $o(G)$.

We assume that the theorem is true for all groups T such that $T \subseteq G$

$$o(T) < o(G)$$

The induction for the result is true for a group of order 1.

now, For any subgroup W of G, $W \neq G$.

i.e) $\frac{p}{o(W)}$

Then by our induction hypothesis there would exist an element of order p in W on G. Thus we may assume that p is not a divisor of the order of any proper subgroup of G.

If $a \notin Z(G)$, $N(a) \neq G$, $\frac{p}{o(G)}$

WKT, the class equation is

$$o(G) = o(Z(G)) + \sum_{N(a) \neq G} \frac{o(G)}{o(N(a))}$$

$\therefore$ $p / o(G)$, $p \nmid o(N(a))$

We have $\dfrac{P}{\dfrac{o(G)}{o(N(a))}}$

$$\Rightarrow P \Big/ \sum_{N(a) \neq G} \frac{o(G)}{o(N(a))}$$

$$\therefore \; P \big/ o(G) \Rightarrow P \Big/ \left(o(G) - \sum_{N(a) \neq G} \frac{o(G)}{o(N(a))} \right) = o(Z(G))$$

Since $Z(G)$ is a subgroup of G. whose order is divisible by P but we've assumed that p is not a divisor of the order of any proper subgroup of G.

$\Rightarrow Z(G)$ cannot be a proper subgroup of G

$\Rightarrow P \big/ o(Z(G))$

$\Rightarrow Z(G) = G$

$\therefore Z(G)$ is an abelian.

Hence G is an abelian.

Direct Product:

a) 8) Let A and B be any two groups and consider the cartesian product $G = A \times B$, G consists of all ordered pair (a, b) where $a \in A$ and $b \in B$.

We can introduce on operation "$*$" in G.

i.e) For ~~through~~ two element (a_1, b_1) and (a_2, b_2) in G.

The product is defined as

$$(a_1, b_1) * (a_2, b_2) = (a_1 a_2, b_1 b_2)$$

Scanned by TapScanner

Here, the product $a_1 a_2$ in the first component is a product of the elements a_1 and a_2 in the group A.

The product $b_1 b_2$ in the second component is a product of the elements b_1 and b_2 in the group B.

Internal direct product: 22

Let G be a group and $N_1, N_2 \cdots N_n$ be normal subgroup of a group G such that

(i) $G = N_1 N_2 \cdots N_n$

(ii) Given $g \in G$, then $g = m_1 m_2 \cdots m_n$; $m_i \in N$.

In a unique way, we say that G is a internal direct product of $N_1, N_2 \cdots N_n$.

External direct product:

Let $G_1, G_2 \cdots G_n$ be a finite number of groups and $G = G_1 \times G_2 \times \cdots \times G_n$. Then G is a group under binary composition defined by

$ab = (a_1 b_1, a_2 b_2, \cdots a_n b_n) \; \forall \; a = (a_1, a_2 \cdots a_n)$ and $b = (b_1, b_2 \cdots b_n)$.

This group is called the external direct product of $G_1, G_2 \cdots G_n$.

Lemma (25) (23)

Suppose that G is the internal direct product of $N_1, N_2 \cdots N_n$. Then for $i \neq j$, $N_i \cap N_j = (e)$ and if $a \in N_i$, $b \in N_j$. Then $ab = ba$

2018

Proof

Let $x \in N_i \cap N_j$

To prove that $x = e$

Suppose x is an element of N_i.

i.e) $x = e_1 e_2 \cdots e_{i-1} x e_{i+1} \cdots e_n$

where $e_t = e$

|||^{ly}, x is an element of N_j

i.e) $x = e_1, e_2 \cdots e_{j-1} x e_{j+1} \cdots e_n$

where $e_t = e$

Every element has a unique representation of the form $m_1 m_2 \cdots m_n$ where $m_i \in N_i \cdots m_n \in N_n$

$\therefore$ The two decomposition of x in this form must coincide.

i.e) entry form of each N_i must be equal the entry so ~~from~~ from N_i is x and in the other it is e.

Hence, $x = e$

Thus $N_i \cap N_j = (e)$ for $i \neq j$

Take the elements $a \in N_i$, $b \in N_j$ & $i \neq j$

Then, $abG^{-1} \in N_i$, N_i being normal subgroup of G.

i.e) $aba^{-1}b^{-1} \in N_i$

III^{ly}, $a^{-1} \in N_i$ and $ba^{-1}b^{-1} \in N_i$

$\Rightarrow aba^{-1}b^{-1} \in N_i$

$\Rightarrow aba^{-1}b^{-1} \in N_i$ and N_j

$\Rightarrow aba^{-1}b^{-1} \in N_i \cap N_j = (e)$

$aba^{-1}b^{-1} = e$

Hence $ab = ba$

If $K_1, K_2 \cdots\cdots K_n$ are normal subgroup of G $\ni$: $G = K_1 K_2 \cdots K_n$ and $K_i \cap K_j = (e)$ for $i \neq j$.

i.e) G becomes the internal direct product.

iff $K_i \cap (K_1 K_2 \cdots K_{i-1} K_{i+1} \cdots K_n) = (e)$, where $i = 1, 2 \cdots n$.

Statement:

Let G be a group and Suppose that G is the internal direct product of $N_1, N_2 \cdots N_n$. Let $T = N_1 \times N_2 \times \cdots \times N_n$. Then G and T are isomorphic.

proof

Define the mapping $\phi : T \rightarrow G$ defined by $\phi(x_1, x_2 \cdots x_n) = x_1 x_2 \cdots x_n$ where each $x_i \in N_i$ $(i = 1, 2 \cdots n)$

To prove that ϕ is an isomorphism of T onto G. Suppose G is the internal direct product of $N_1, N_2 \cdots\cdots N_n$.

If $x \in G$, then $x = a_1 a_2 \cdots a_n$

$a_1 \in N_1, a_2 \in N_2 \cdots a_n \in N_n$, then

$\phi(a_1 a_2 \cdots a_n) = a_1 a_2 \cdots a_n = x$

$\therefore \phi$ is onto.

Let us make use by the uniqueness property of internal direct Product to prove that ϕ is 1-1.

Suppose that $\phi(a_1, a_2 \cdots a_n) = \phi(c_1, c_2 \cdots c_n)$

where $a_i \in N_i$, $c_i \in N_i$ for $i = 1$ to n.

By the definition of ϕ, $a_1 a_2 \cdots a_n = c_1 c_2 \cdots c_n$

By uniqueness property, we have

$$a_1 = c_1, \; a_2 = c_2 \cdots a_n = c_n$$

$\therefore \phi$ is 1-1.

To prove that ϕ is homomorphism of T onto G.

Let $x = (a_1, a_2 \cdots a_n)$, $y = (b_1, b_2 \cdots b_n)$ be elements of T.

Then $\phi(xy) = \phi((a_1 a_2 \cdots a_n)(b_1 b_2 \cdots b_n))$

$= \phi(a_1 b_1 \cdot a_2 b_2 \cdots a_n b_n)$

$= a_1 b_1 \cdot a_2 b_2 \cdots a_n b_n$

By the lemma,

$$a_i b_j = b_j a_i \quad \text{if } i \neq j$$

$\Rightarrow a_1 b_1 \cdot a_2 b_2 \cdots a_n b_n = a_1 a_2 \cdots a_n \cdot b_1 b_2 \cdots b_n$

i.e) $\phi(xy) = (a_1 a_2 \cdots a_n)(b_1 b_2 \cdots b_n)$

But, $\phi(x) = a_1 a_2 \cdots a_n$ &

$\phi(y) = b_1 b_2 \cdots b_n$

$\therefore \phi(xy) = \phi(x)\phi(y)$

Hence ~~Since~~ ϕ is an isomorphism of T onto G.

Thm : 3.17

Let c be the set of all symbols (α, β) where α and β are real numbers.

23/9/19 Sylow's theorem

Sylow's first theorem:

If p is a prime number and $\frac{p^\alpha}{O(G)}$, then G has a subgroup of order p^α

Proof

The number of ways of picking a subset of k elements from a set of n elements.

i.e) $nC_k = \frac{n!}{k!(n-k)!}$

Let $n = p^\alpha m$, $k = p^\alpha$ with p is a prime number and p^r / m but $p^{r+1} \nmid m$ → does not divides

We have; $\binom{p^\alpha m}{p^\alpha} = \frac{(p^\alpha m)!}{(p^\alpha)!\,(p^\alpha m - p^\alpha)!}$

$$= \frac{p^\alpha m (p^\alpha m - 1) \cdots\cdots (p^\alpha m - i) \cdot \cdots (p^\alpha m - p^\alpha + 1)}{p^\alpha (p^\alpha - 1) \cdots (p^\alpha - i) \cdots\cdots (p^\alpha - p^\alpha + 1)}$$

$$= \frac{\dfrac{1 \cdot 2 \cdots (p^\alpha m - p^\alpha - 1)(p^\alpha m - p^\alpha)(p^\alpha m - p^\alpha + 1) \cdots (p^\alpha m - 1)(p^\alpha m)}{}}{(1 \cdot 2 \cdot 3 \cdots (p-1)^\alpha p^\alpha \, (p^\alpha m - p^\alpha)!}$$

$$= \frac{\cancel{(p^\alpha m - p^\alpha)!} \, (p^\alpha m - p^\alpha + 1 \cdots (p^\alpha m - 1) \, p^\alpha m}{(1 \cdot 2 \cdots p^\alpha) \, \cancel{(p^\alpha m - p^\alpha)!}}$$

Let us find the Power of p that divides $\binom{p^\alpha m}{p^\alpha}$.

We note that, $\dfrac{p^k}{(p^\alpha m - i)}$ iff p^k / i

i.e) iff $p^k / (p^\alpha - i)$ where $k \le \alpha$, $1 \le i \le p^\alpha - 1$

$\therefore$ All powers of p cancel out except the Powers which divides m.

Thus $p^r / \binom{p^\alpha m}{p^\alpha}$ and $p^{r+1} \nmid \binom{p^\alpha m}{p^\alpha}$

Let us now prove that

Take M set of all subsets of G which have p^α elements.

Thus, M has $\binom{p^\alpha M}{p^\alpha}$ elements. Let us define a relation $\sim$ in M.

Let M_1 and M_2 be two elements of M.

If $\exists$ an element g in $G \ni : M_1 = M_2 g$

we can show that this is an equivalence relation on M.

i) reflexive :

$\therefore M_1 = M_1 e$, where e is the identity in G.

$M_1 \sim M_1$

ii) Symmetric :

$M_1 \sim M_2 \Rightarrow M_1 = M_2 g$

$\Rightarrow M_2 = M_1 g^{-1}$

$\Rightarrow M_2 \sim M_1$

iii) Transitive :

If $M_1 \sim M_2$ and $M_2 \sim M_3$, we have

$M_1 = M_2 g_1$ and $M_2 = M_3 g_2$

i.e) $M_1 = (M_3 g_2) g_1$

$= M_3 g_2 g_1$

$\Rightarrow M_1 \sim M_3$

Hence the relation is an equivalence relation on M.

This equivalence relation gives rise to a partition of M into equivalence classes.

Scanned by TapScanner

We shall now show that $\exists$ atleast on equivalence class $\ni$: the number of elements in this class is not a multiple of p^{r+1}.

If p^{r+1} divides the number of elements in each equivalence class than p^{r+1} would divide the number of elements in M.

This is not true.

$\because$ M has $\left|\begin{matrix} p^{\alpha}M \\ p^{\alpha}\end{matrix}\right|$ elements and $p^{r+1} \not| \left(\frac{p^{\alpha}M}{p^{\alpha}}\right)$

Let $(M_1, M_2 \cdots M_n)$ be such a partition of M into equivalence classes where $p^{r+1} \not| n$.

To prove that subgroup,

Take $H = \{ g \in G / M_1 g_1 = M_1 \} \forall a, b \in H$

$M_1 ab = (M_1 a) b$

$= M_1 b$

$= M_1$

$\therefore M_1 ab = M_1$

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

ie) H is closed under multiplication.

G being a finite group.

$\therefore$ H is a subgroup

Now, we show that $O(H) = p^{\alpha}$

So that H turns to be required subgroup of G.

We show that there is a 1-1 correspondence between the elements in the equivalence class $(M_1, M_2 \ldots M_n)$ and the right cosets of H in G

$$M_1 g = M_1 g' \Rightarrow M_1 g (g')^{-1} = M_1$$

$$\Leftrightarrow (gg')^{-1} \in H$$

$$\Leftrightarrow Hg = Hg'$$

Hence, n = number of right cosets of H in G

$$= \frac{o(G)}{o(H)}$$

$|||^{ly}$ $n = \frac{o(G)}{o(H)}$

$$n\, o(H) = o(G) = p^{\alpha} m$$

$$p^{r+1} \nmid n \quad \& \quad p^{\alpha + r} / n\, o(H) = p^{\alpha} m$$

$$\Rightarrow p^{\alpha} / o(H) \quad \& \quad o(H) \geq p^{\alpha}$$

If $m_1 \in M_1$ then for all $h \in H$, $m_1 h \in M_1$

Thus M_1 has atleast $o(H)$ distinct elements.

However M_1 is a subset of G containing p^{α} elements.

$$\therefore p^{\alpha} \geq o(H)$$

we have already shown that

$$O(H) \geq p^{\alpha}$$

$$\therefore O(H) = p^{\alpha}$$

Hence H is the required subgroup of G have p^{α} elements.

Lemma:

S_{p^k} has a p-Sylow subgroup.

Proof

We use induction on k.

When $k=1$, S_p has an element $(1, 2 \cdots p)$ of order p & a subgroup of order p is generated.

Thus the result is true for $k=1$.

Suppose that the result is true.

We shall show that it is true of k

Divide the integer $1, 2 \cdots p^k$ into p sets sets each with p^{k-1} elements as follows

$(1, 2, \cdots p^{k-1}), (p^{k-1}+1, p^{k-1}+2, \cdots 2p^{k-1}) \ldots$

$((p-1)p^{k-1}+1, \cdots p^k)$

Let σ be the permutation given by

$$\sigma = (1, p^{k-1}+j, 2p^{k-1}+1 \cdots (p-1)p^{k-1}+1) \cdots$$
$$(j, p^{k-1}+j, 2p^{k-1}+j \cdots (p-1)p^{k-1}+j) \cdots$$
$$p^{k-1}, 2p^{k-1} \cdots (p-1)p^{k-1}, p^k)$$

The following properties are true.

1) $\sigma^p = e$

2) If θ is a permutation leaving all is fixed

for $i > p^{k-1}$ (θ is $1, 2 \cdots p^{k-1}$), then $\sigma^{-1}\theta\sigma$ moves elements in $(p^{k-1}+1, p^{k-1}+2, \cdots 2p^{k-1})$ & in general $\sigma^{-j}\theta\sigma_j$ moves elements in $(jp^{k-1}+1, jp^{k-1}+2, \cdots (j+1)p^{k-1})$.

Consider $A = \{\theta \in S_{p^k} / \theta(i) = i \text{ if } i > p^{k-1},$

A is a subgroup of S_{p^k} and elements in A carry out permutation (or) $1, 2 \cdots p^{k-1}$.

Thus it follows that A is isomorphic to $S_{p^{k-1}}$

By induction A has a subgroup B_1 of order $p^{n(k-1)}$.

Let $T = B_1 (\delta^{-1} B_1 \delta)(\delta^{-2} B_1 \delta^2) \cdots (\delta^{-(p-1)} B_1 \delta^{p-1})$

$= B_1 B_2 \cdots B_{n-1}$ where $B_i = \delta^{-i} B \delta^i$

Each B_i is isomorphic to B_1 & has order $p^{n(k-1)}$.

Moreover B_i are distinct & they also commutative

Thus T is a subgroup of S_{p^k}.

We have, $B_i \cap B_j = (e)$ if $0 \le i \ne j \le p-1$

We find $O(T) = O(B_i)^p = p^{p \cdot n(k-1)}$

$\because \delta^p = e$ & $\delta^{-i} B_i \delta^i = B_i$

We get $\delta^{-1} T \delta = T$

Put $P = \{ \delta^j t \,/\, t \in T, 0 \le j \le p-1 \}$

$\because \delta \notin P$ & $\delta^{-1} T \delta = T$

We get two things

(i) T is a subgroup of S_{p^k}.

(ii) $O(P) = p \cdot O(T)$

$= p \cdot p^{n(k-1)p}$

$= p^{n(k-1)p+1}$

Now P is the p-sylow subgroup of S_{p^k}

It is order in $p^{n(k-1)p+1}$

i.e) $n(k-1) = 1+p+\cdots+p^{k-2}$ & $p\,n(k-1)+1$

$= 1+p+\cdots+p^{k-1}$

$= n(k)$

Hence, $O(P) = p^{n(k)}$ & P is the p-Sylow subgroup of S_{p^k}.

$\therefore \sigma^p = e$ & $\sigma^{-1} B_i \sigma^i = B_i$

we get, $\sigma^{-1} T \sigma = T$

Put $P = \{\sigma^j t \,/\, t \in T, 0 \le j \le p-1\}$

<u>Def:</u>

Let G be a group. H, B subgroup of G.

If $x, y \in G$ define $x \sim y$ if $y = axb$ for some $a \in A$, $b \in B$.

<u>Lemma:</u> 2.12.1

$n(k) = 1+p+\cdots+p^{k-1}$

<u>Proof</u>

If $k=1$, $p! = 1\cdot 2 \cdots (p-1)p$

$\therefore p / p!$ & $p^2 \nmid p!$

Hence $n(1) = 1$

In $(p^k)!$ the multiples of p like $p, 2p, \cdots p^{k-1}, p$ Contribute to the power of p dividing $(p^k)!$

i.e) $n(k)$ is the power of p dividing $p^{(2p)(3p)\cdots}$

$p^{(k-1)p} = p\,p^{k-1}(p^{k-1})!$

i.e) $n(k) = p^{k-1} + n(k-1)$

$|||^{ly}$, $n(k-1) = p^{k-2} + n(k-2)$ & so on.

i.e) $n(k) - n(k-1) = p^{k-1}$

$n(k-1) - n(k-2) = p^{k-2}$

$n(2) - n(1) = p$

$n(1) = 1$

Adding $n(k) = 1 + p + \cdots + p^{k-1}$.

Thm: Third Part of Sylows thm

The number of p-Sylow subgroups in G for a gn prime, is of the form $1 + kp$.

Proof

Let A be a p-Sylow Subgroup of G.

Suppose that G is decomposed into double Cosets of A & A.

$$\text{Thus } G = \bigcup AxA$$

$$O(AxA) = \frac{O(A)\,O(A)}{O(A \cap xAx^{-1})}$$

$$= \frac{O(A^2)}{O(A \cap xAx^{-1})}$$

If $A \cap xAx^{-1} \neq A$, then $p^{n+1} / O(AxA)$ where $p^n = O(A)$

i.e) if $x \notin N(A)$ then $p^{n+1} / O(AxA)$

Also if $x \in N(A)$, then $AxA = A(Ax)$

$$= A^2x = Ax$$

$$\therefore O(AxA) = O(Ax)$$
$$= O(A)$$
$$= p^n$$

Now, $O(G) = \sum_{x \in N} O(AxA) + \sum O(AxA)$

where each sum runs over one element from each double coset.

If $x \in N(A)$, then $AxA = Ax$ and the first sum is $\sum_{x \in N(A)} O(Ax)$ over the distinct cosets of A in $N(A)$.

(i.e) the first sum is just $O(N(A))$

In the ~~second~~ second sum, each two is divisible by p^{n+1}, $p^{n+1} / \sum_{x \notin N(A)} O(AxA)$

Thus, we can write the second sum as

$$\sum_{x \notin N(A)} O(AxA) = p^{n+1} u$$

$$\therefore O(G) = O(N(A)) + p^{n+1} \cdot u.$$

Lemma: If A, B are finite subgroups of G then

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

Proof

Third proof of Sylow's thm.

Thm: 2.12.2 [second part of Sylow's thm]

If G is a finite group, p is prime & $p^n / o(G)$ but $p^{n+1} \not/ o(G)$ then any two subgroups of G of order p^n are conjugate.

Proof

Let A, B be subgroup of G with each of order p^n.

T.P.T : $A = gBg^{-1}$ for some $g \in G$

Decompose G into double cosets of A & B.

i.e) $G = \bigcup AxB$

We have $o(AxB) = \dfrac{o(A)\,o(B)}{o(A\cap \cdots Bx^{-1})}$

S.T $A \neq xBx^{-1}$ for every $x \in G$, then

$o(A\cap xBx^{-1}) = p^m$ where $m < n$

i.e) $o(AxB) = \dfrac{o(A)\,o(B)}{p^m} = \dfrac{p^n p^n}{p^m}$

$= \dfrac{p^{2n}}{p^m} = p^{2n-m}$

Scanned by TapScanner

We have $2n-3 \geq n+1$

i.e) $p^{n+1} / o(AxB)$ for every x

$\therefore o(G) = \sum o(AxB)$

We get $p^{n+1} / o(G)$

$\Rightarrow \Leftarrow$

$\therefore A = gBg^{-1}$ for some $g \in G$

Thus A & B are conjugate.

UNIT - 4

Thm 3.17

Let c be the set of all symbols (α, β) where α, β are real numbers. Then c is a field

Proof

We define $(\alpha, \beta) = (\gamma, \delta)$ iff $\alpha = \gamma$ & $\beta = \delta$.

Addition in c:

By define $x = (\alpha, \beta)$

$y = (\gamma, \delta)$

Addition:

$x + y = (\alpha, \beta) + (\gamma, \delta)$

$= (\alpha + \gamma), (\beta + \delta) \rightarrow ①$

$y + x = (\gamma, \delta)(\alpha, \beta)$

$= (\gamma + \alpha), (\delta + \beta) \rightarrow ②$

From ① & ②

$x + y = y + x$

$\therefore$ c is an abelian group with addition.

$(0, 0)$ is the identity element.

$(-\alpha, -\beta)$ is the inverse of (α, β)

Multiplication in c:

we define $x = (\alpha, \beta)$

$y = (\gamma, \delta)$

i) commutative ring:

$x \cdot y = (\alpha, \beta) \cdot (\gamma, \delta)$

$x \cdot y = (\alpha\gamma - \beta\delta ; \alpha\delta + \beta\gamma)$

$y \cdot x = (\gamma \cdot \delta)(\alpha, \beta)$

$= (\gamma\alpha - \delta\beta , \delta\alpha + \gamma\beta)$

$\therefore xy = yx$

Also, if $x = (\alpha, \beta) \neq (0,0)$ then

Since α, β are real and not both 0,

$\alpha^2 + \beta^2 \neq 0$; thus

$$y = \left(\frac{\alpha}{\alpha^2+\beta^2}, \frac{-\beta}{\alpha^2+\beta^2}\right) \text{ in } C$$

Then, $(\alpha, \beta) \cdot \left(\frac{\alpha}{\alpha^2+\beta^2}, \frac{-\beta}{\alpha^2+\beta^2}\right)$

$$= \left(\frac{\alpha^2}{\alpha^2+\beta^2} + \frac{\beta^2}{\alpha^2+\beta^2} \cdot \frac{-\alpha\beta}{\alpha^2+\beta^2} + \frac{\alpha\beta}{\alpha^2+\beta^2}\right)$$

$$= \left(\frac{\alpha^2+\beta^2}{\alpha^2+\beta^2}, 0\right)$$

$= (1, 0)$

C is satisfied field.

Thm 3.18

Let Q be the set of symbols $\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k$, where all the numbers $\alpha_0, \alpha_1, \alpha_2, \alpha_3$ are real numbers. We consider two symbols $\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k$ and $\beta_0 + \beta_1 i + \beta_2 j + \beta_3 k$ to be equal iff $\alpha_t = \beta_t$ for $t = 0, 1, 2 \ldots Q$ into

Scanned by TapScanner

ring: we must be define a + and a. for its element.

Proof

a +

$$X = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k$$

$$Y = \beta_0 + \beta_1 i + \beta_2 j + \beta_3 k$$

in Q.

$$x + y = (\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k) + (\beta_0 + \beta_1 i + \beta_2 j + \beta_3 k)$$

$$= (\alpha_0 + \beta_0) + (\alpha_1 + \beta_1) i + (\alpha_2 + \beta_2) j + (\alpha_3 + \beta_3) k$$

$$y + x = (\beta_0 + \beta_1 i + \beta_2 j + \beta_3 k) + (\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k)$$

$$= (\beta_0 + \alpha_0) + (\beta_1 + \alpha_1) i + (\beta_2 + \alpha_2) j + (\beta_3 + \alpha_3) k$$

$$\therefore \; x + y = y + x$$

a.

$$x \cdot y = (\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k) \cdot (\beta_0 + \beta_1 i + \beta_2 j + \beta_3 k)$$

$$= (\alpha_0\beta_0 + \alpha_0\beta_1 i + \alpha_0\beta_2 j + \alpha_0\beta_3 k) +$$

$$(\alpha_1\beta_0 i + \alpha_1\beta_1 + \alpha_1\beta_2 \underset{(-1)}{ij} + \alpha_1\beta_3 ik) +$$

$$(\alpha_2\beta_0 j + \alpha_2\beta_1 ij + \alpha_2\beta_2 j^2 + \alpha_2\beta_3 \underset{(-1)}{jk}) +$$

$$(\alpha_3\beta_0 k + \alpha_3\beta_1 ik + \alpha_3\beta_2 jk + \alpha_3\beta_3 k^2)$$

$$ijk = -1$$

$$x \cdot y = (\alpha_0\beta_0 - \alpha_1\beta_1 - \alpha_2\beta_2 - \alpha_3\beta_3) + i(\alpha_0\beta_1 + \alpha_1\beta_0 +$$

$$\alpha_2\beta_3 - \alpha_3\beta_2) + j(\alpha_0\beta_2 + \alpha_2\beta_0 + \alpha_3\beta_1 - \alpha_1\beta_3)$$

$$+ (\alpha_0\beta_3 + \alpha_3\beta_0 + \alpha_1\beta_2 - \alpha_2\beta_1) k$$

where $i^2 = j^2 = k^2 = ijk = -1$

$ij = k$	$ji = -k$
$jk = i$	$kj = -i$
$ki = j$	$ik = -j$

The elements are $\pm 1, \pm i, \pm j, \pm k$.

$\therefore\ ij \neq ji$

So, it is non-abelian group.

Also, non-commutative rings.

Q is non-commutative ring

$0 = 0 + 0i + 0j + 0k$

$1 = 1 + 0i + 0j + 0k$

$0 \cdot 1 = 1 \cdot 0 = 0$

$\therefore$ 0 is unit element

If $x = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k \neq 0$, then

$\alpha_0, \alpha_1, \alpha_2, \alpha_3$ are not 0.

Since they are real,

$\beta = \alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2 \neq 0$, thus

$$y = \frac{\alpha_0}{\beta} - \frac{\alpha_1 i}{\beta} - \frac{\alpha_2 j}{\beta} - \frac{\alpha_3 k}{\beta} \in Q$$

$$x \cdot y = (\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k) \cdot \left(\frac{\alpha_0}{\beta} - \frac{\alpha_1 i}{\beta} - \frac{\alpha_2 j}{\beta} - \frac{\alpha_3 k}{\beta}\right)$$

$$= \left(\frac{\alpha_0^2}{\beta} - \cancel{\frac{\alpha_0\alpha_1}{\beta}} i - \cancel{\frac{\alpha_0\alpha_2}{\beta}} j - \cancel{\frac{\alpha_0\alpha_3}{\beta}} k\right) +$$

$$\left(\cancel{\frac{\alpha_1\alpha_0}{\beta}} i + \frac{\alpha_1^2}{\beta} - \cancel{\frac{\alpha_1\alpha_2}{\beta}} ij - \cancel{\frac{\alpha_1\alpha_3}{\beta}} ik\right) +$$

$$\left(\cancel{\frac{\alpha_0\alpha_2}{\beta}} j + \cancel{\frac{\alpha_1\alpha_2}{\beta}} ij + \frac{\alpha_2^2}{\beta} - \cancel{\frac{\alpha_2\alpha_3}{\beta}} jk\right) +$$

$$\left(\cancel{\frac{\alpha_0\alpha_3}{\beta}} k + \cancel{\frac{\alpha_1\alpha_3}{\beta}} ik + \cancel{\frac{\alpha_2\alpha_3}{\beta}} jk + \frac{\alpha_3^2}{\beta}\right)$$

$$= \frac{\alpha_0^2}{\beta} + \frac{\alpha_1^2}{\beta} + \frac{\alpha_2^2}{\beta} + \frac{\alpha_3^2}{\beta}$$

$$= \frac{\alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2}{\beta}$$

$$= \frac{\alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2}{\alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2}$$

$$= 1$$

$x \cdot y = 1$

$\therefore$ Q is non - abelian group under multiplication.

Some Special classes of rings:

Definition: (24)

If R is a commutative ring, then $a \neq 0 \in R$ is said to be a zero-divisor. If there exists $ab \in R$, $b \neq 0$ such that $ab = 0$.

Eg:

$(Z_6, \otimes_6)$ is a zero-divisor.

$Z_6 = \{0, 1, 2, 3, 4, 5\}$

$2 \otimes_6 3 = 0$

(25)

Definition: [Integral domain]

A commutative ring is an integral domain if it has no zero-divisor.

Eg: $Z_6 = \{0, 1, 2, 3, 4, 5\}$

$a = 2$ and $b = 3$

$ab = 2 \cdot 3 = 6 \Rightarrow ab \neq 0$

Scanned by TapScanner

$ba = 3 \cdot 2 = 6 \Rightarrow ba \neq 0$

25

Definition: [Division ring (or) Skew field]

A ring R is said to be a division ring if it's non-zero element form a group under multiplication.

The unit element under multiplication will be written as 1.

The inverse of an element a under multiplication will be denoted by a^{-1}.

Lemma: 26

(A) If R is a ring, then for all $a, b \in R$

(i) $a0 = 0a = 0$

Proof

(i) If $a \in R$, then $a0 = a(0+0)$

$= a0 + a0$

$a0 = 0$ ($\because$ Right distributive law)

Since R is a group under addition.

$\therefore a0 = 0$.

$|||^{ly}$,

$0a = (0+0)a$

$= 0a + 0a$

$0a = 0$ ($\because$ Left distributive law)

$\therefore a0 = 0a = 0$

Scanned by TapScanner

ii) $a(-b) = -a(b) = -ab$

In order to show that $a(-b) = -ab$

We must demonstrate that,

$$ab + a(-b) = 0$$

But, $ab + a(-b) = a(b + (-b))$

$= a0$

$= 0$ (∵ distributive law)

$|||^{ly}$, $(-a)b = -ab$

iii) $(-a)(-b) = ab$. If in addition, R has a ~~unit element 1~~.

$(-a)(-b) = ab$ is really a special case of Part-2, We single it out since its analog in the case of real numbers has been so stressed in our early education. So on with

$$(-a)(-b) = -a(-b)$$

$$= -(-ab)$$

$$= ab$$

$$\therefore (-a)(-b) = ab$$

iv) $(-1)a = -a$

If in addition, R has a unit element 1.

proof

Suppose that R has a unit element 1.

Then,

$$a + (-1)a = [1 + (-1)]a$$

$$= 0a$$

$$= 0$$

Hence $(-1)a = -a$

v) $(-1)(-1) = 1$

Proof

WKT, $(-1)a = -a$

if $a = -1$

$\Rightarrow (-1)(-1) = -(-1)$

$1 = 1$

Hence the proof.

The pigeonhole principle: 28

Definition:

If n objects are distributed over m places and if $n > m$, then some places receives atleast two objects.

Lemma: 29

A finite integral domain is a field.

Proof

An integral domain is commutative ring such ~~as~~ that $ab = 0$.

If atleast one of a (or) b is itself 0.

A field on the other hand is a commutative ring with unit element in which every non-zero element has a multiplicative inverse in the ring.

Let D be a finite integral domain. In order to prove that D is a field, we must

1. Produce an element $1 \in D$ such that $a1 = a$ for every $a \in D$.

2. for every element $a \neq 0 \in D$, produce an element $b \in D$ such that $ab = 1$.

Let $x_1, x_2 \dots x_n$ be all the elements of D and suppose that $a \neq 0 \in D$.

Consider the elements $x_1 a, x_2 a \dots x_n a$.

They are all in D.

We claim that they are all distinct for suppose that $x_i a = x_j a$ for $i \neq j$, then $(x_i - x_j) a = 0$.

Since D is an integral domain and $a \neq 0$ their forces $x_i - x_j = 0$ and so $x_i = x_j$ contradicting $i \neq j$.

Thus $x_1 a, x_2 a \dots x_n a$ are n distinct element lying in D, which has exactly n elements.

By the pigeonhole principle, these must for all the elements of D stated otherwise every element $y \in D$ can be written as

$x_i a$ for some x_i

In particular since $a \in D$, $a = x_{i_0} a$

for some $x_{i_0} \in D$. Since D is commutative

$$a = x_{i_0} a = a x_{i_0}$$

We propose to show that x_{i_0} acts

as a limit element for some $x_i \in D$ and

so $y x_{i_0} = (x_i a) x_{i_0} = x_i (a x_{i_0}) = x_i a = y$

Thus x_{i_0} is a unit element for D and

we write it as 1.

Now $1 \in D$ so by our previous argument,

it too is realizable as a multiple of a that is

there exists $ab \in D$ such that $1 = ba$.

Now, lemma is proved.

Corollary:

If p is a prime number, then J_p, the

ring of integers mod p is a field.

Proof

By the lemma, it is enough to prove

that J_p is an integral domain.

Since it only has a finite number of elements.

If $a, b \in J_p$ and $ab = 0$, then p must divide the ordinary integer ab and so p being a prime must divide a (or) b.

But then either $a = 0$ and p (or) $b = 0$ mod p hence in J_p one of these is 0.

The corollary above assures as that we can find an infinity of fields having a finite number of elements. Such fields are called finite fields.

The fields J_p do not give all the examples of finite fields, there others. In fact in Sec 7.1. we gives a complete discription of all finite fields.

We point out a striking difference between finite fields and fields such as the rational numbers, real numbers and complex numbers with which we are more familiar.

Let f be a finite field having q elements. viewing F morely as a group under addition. Since F has q elements (by corollary 2 to thm 2.4.1)

$$a + a + \cdots + a = qa = 0$$

For any $a \in F$. Thus in F we have $qa = 0$.

for some positive integer q even if $a \neq 0$.

This certainly cannot happen in the field of rational numbers for instance. We formalize this distinction in the definitions.

We gives below in this definitions instead of taking just about fields.

We choose to widen the scope a little and talk about integral domain.

Definitions:

An integral domain D is said to be of characteristic 0 if the relation $ma = 0$ where $a \neq 0$ is in D and where m is an integer can hold only if $m = 0$.

The ring of integers i.e) Thus of characteristic 0 as the other familiar rings such as the integers or the rational.

Definition:

An integral domain D is said to be of finite characteristic if there exists a positive integer in such that $ma = 0 \ \forall \ a \in D$.

Scanned by TapScanner

Lemma:

If ϕ is a homomorphism of R into R'.

i) $\phi(0) = 0$.

ii) $\phi(-a) = -\phi(a)$ for every $a \in R$.

Proof

If both R and R' have the respective unit elements 1 and $1'$. For their multiplication in need not follow that $\phi(1) = 1'$.

However, if R' is an integral domain, or if R' is arbitrary but ϕ is onto, then

$\phi(1) = 1'$ is indeed true.

26/9/19 In the case of groups, given a homomorphism we associated with this homomorphism a certain subset of the group which we called the kernel of the homomorphism.

After all, the rings has two, operations addition and multiplication and it might be natural to ask which of these should be singled out as the basis for definition.

However, the choice is clear. But into the definition of an arbitrary ring is the condition that the ring forms an abelian group under addition.

The ring multiplication was left much more unrestricted, and so in a sense much less under our control than is the addition.

For this reason the emphasis is given to the operation of addition.

Definition:

If ϕ is a homomorphism of R into R', then kernel $\phi \cdot I(\phi)$ is the set of all elements $a \in R$ such that $\phi(a) = 0$, the zero-element of R.

Lemma: 3.3

If ϕ is a homomorphism of R into R' with kernel $I(\phi)$, then

1) $I(\phi)$ is a subgroup of R under addition

2) If $a \in I(\phi)$ and $r \in R$ then both ar & ra are in $I(\phi)$.

Proof

Since ϕ is in particular, a homomorphism of R, as an additive group, into R' as an additive group.

Suppose that $a \in I(\phi), r \in R$, then $\phi(a) = 0$

so that

$$\phi(ar) = \phi(a)\,\phi(r)$$
$$= 0\,\phi(r)$$
$$= 0$$

$|||^{ly}$, $\phi(ra) = 0$

By defining property of $I(\phi)$ both ar and ra in $I(\phi)$.

Definition:

A homomorphism of R into R' is said to be an isomorphism if it is a one-to-one mapping

Definition:

Two rings are said to be isomorphic if there is an isomorphism of one onto the other.

Ideal and Quotient Rings

Ideal:

Let R be a ring. A non-empty subset of R is called a left ideal of R if

i) $a, b \in I \Rightarrow a - b \in I$

ii) $a \in I$ and $r \in R \Rightarrow ra \in I$

I is called a right ideal of R if

i) $a, b \in I \Rightarrow a - b \in I$

ii) $a \in I$ and $r \in R \Rightarrow ar \in I$

I is called an ideal of R if I is both a left ideal and right ideal.

Quotient Rings

Let R be any ring and I be an ideal of R, we have two well defined binary operations in R/I given by

$$(I+a)+(I+b) = I+(a+b) \text{ and}$$

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

The ring R/I is called the quotient ring of R modulo I.

Definition:

A non-empty subset U of R is said to be a (two-sided) ideal of R if

1) U is a subgroup of R under addition'

2) For every $u \in U$ and $r \in R$ both ur and ru are in U.

1)
Soln

If $x = a+U$, $y = b+U$, $z = c+U$ are there element of R/U, where $a, b, c \in R$ then

$$(x+y)z = [(a+U)+(b+U)](c+U)$$

$$= [(a+b)+U][c+U]$$

$$= (U + (a+b)c]$$

$$= (U + ac + bc)$$

$$= (U+ac) + (U+bc)$$

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

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

$(x+y)z = xz + yz$

$\therefore$ R/G has now been made into a ring.

Clearly if R is commutative there so is R/U for

$$(a+U)(b+U) = ab+U$$
$$= ba+U$$
$$= (b+U)(a+U)$$

If R has a unit element 1. Then R/U has a unit element $1+U$. There is a homomorphism ϕ of R onto R', given by $\phi(u) = a+u$ for every $a \in R$, whose kernel is exactly U.

Lemma 3.4.1

If U is an ideal of the ring R then R/U is a ring and is a homomorphic image of R.

Proof Let R, R' be rings and ϕ a homomorphism of R onto R' with kernel U. Then R' is isomorphic to R/U.

Moreover, there is a one-to-one correspondence between the set of ideals of R' and the set of ideals of ~~R~~ R which contain U.

This correspondence can be achieved by associating with an ideal W in R' the ideal W

in R' the ideal W in R defined by

$W = \{ x \in R \,/\, \phi(x) \in W' \}$ with W so

defined R/W is isomorphic to $\frac{R'}{W'}$.

Lemma

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

Proof

For any $a \neq 0 \in R$

we must be produce an element $b \neq 0 \in R$ such that $ab = 1$.

So, suppose that $a \neq 0 \in R$

Consider the set $Ra = \{ xa \,/\, x \in R \}$

we claim that, Ra is an ideal of R.

In order to establish this as fact, we must show that it is a subgroup of R under addition and that if $u \in R$ and $r \in R$ then ra is also in R.

Now, we check that ra is in Ra for then ar also is

$\therefore ra = ar$

Now, if $u, v \in Ra$

then $u = r_1 a \quad v = r_2 a$ for some $r_1, r_2 \in R$

Thus, $u + v = r_1 a + r_2 a$

$= (r_1 + r_2) a \in Ra$

$|||^{ly}$, $(-u) = -r_1 a$

$= -(r_1) a \in Ra$

Hence, Ra is an additive subgroup of R.

Moreover, if $r \in R$

$ru = r(r_1 a)$

$= (r r_1) a \in Ra$

$\therefore$ Ra satisfies all definely conditions for an ideal of R.

Hence Ra is an ideal of R.

By our assumptions on R,

$Ra = (0)$ or

$Ra = R$

$\because 0 \neq a = 1a \in Ra$

$Ra \neq (0)$

Thus, we are left with the only other possibility, namely that

$Ra = R$

This last equation states that every element in R is multiple of a by element of R.

Scanned by TapScanner

In particular $I \in R$ and so it can be realized as a multiple of a. that is there exists an element $b \in R$ such that

$$ba = 1.$$

Definition: Maximal ideal

An ideal $M \neq R$ in a ring R is said to be a maximal ideal of R if whenever U is an ideal of R such that $M \subset U \subset R$ then either $R = U$ (or) $M = U$.

Example: Let R be the ring integers and let U be an ideal of R.

Since U is a subgroup of R under addition. WKT, U consists of all multiples of a fixed integer n_0.

We write, $U = (n_0)$

We first assert that if p is a prime number Then $P = (p)$ is a maximal ideal of R

For if U is an ideal of R and $U \supset P$, then $U = (n_0)$ for some integers.

Since, $p \in P \subset U$, $p = mn_0$ for some integers m. Because p is a prime this implies that

$n_0 = 1$ (or) $n_0 = p$.

If $n_0 = p$, then $P \subset U = (n_0) \subset P$

So that $U = P$, if $n_0 = 1$ then $1 \in U$.

Hence, $r = 1r \in U \quad \forall\, r \in R$

Whence $V = R$. Thus no ideal other then R (or) P. which itself can be put between P and R from which

we ~~deduced~~ deduce.

Suppose, one the other hand that $M = (n_0)$ is maximal ideal of R.

We claim that n_0 must be prime numbers.

For if $n_0 = ab$ whence a, b are positive integer, then $U = (a) \supset M$

Hence $U = R$ or $U = M$

If $U = R$, then $a = 1$ is an easy consequence.

If $U = M$, then $a \in M$ and so $a = r n_0$ for some integer r.

Since every element of M is multiple of n_0 but then

$n_0 = ab = r n_0$ from which, we get

$rb = 1$ so that $b = 1$.

$n_0 = a$

Thus n_0 is a prime number.

Eg:

Let R be the ring of all the real valued continuous functions on the closed unit interval.

Let $M = \left\{ f(x) \in R \,/\, f(1/2) = 0 \right\}$

M is ideal of R

Moreover, it is a max. ideal of R for if the ideal U contains M and $V \neq M$.

Then, there is a function $g(x) \in U$.

$$g(x) \notin M$$

$$\therefore g(1/2) \neq 0$$

$$g(1/2) = \alpha$$

Take $h(x) = g(x) - \alpha$

$$\Rightarrow h(1/2) = g(1/2) - \alpha$$

$$\alpha - \alpha = 0$$

$$\Rightarrow$$

$$h(x) \in M \subset U$$

also $g(x) \in U$

Hence, $g(x) - h(x) \in U$

$$\therefore \alpha \in U$$

So, $1 = \alpha\alpha^{-1} \in U$

Thus, for any function $t(x) \in R$, $U \subset R$, $r \in R$, $a \in I$.

$$1 \in U.$$

Scanned by TapScanner

$1 \cdot t(x) = t(x) \in U$ in

Consequence of which $U = R$.

$\therefore$ M is a max. ideal of R.

III^{ly}, γ is a real number $0 \leq \gamma \leq 1$, then

$M_\gamma = \{ f(x) \in R / f(\gamma) = 0 \}$ is a maximal ideal of R.

$\therefore$ Every maximal ideal is of this form.

Thus, the maximal ideal correspond to the points on the unit interval.

10m Thm (32)

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

Proof

(i) Neccessary part:

Suppose, M is an ideal of R $\ni$: R/M is a field.

$\because R/M$ is a field its only ideal are (0) and R/M itself.

There is 1-1 correspondence between the set of ideals of R/M and set of ideals R which contain M.

The ideal M of R corresponds to the ideal 0 of R/M whereas the ideal R of R corresponds to the ideal R/M of R/M in the 1-1 mapping.

Thus there is no ideal between M and R other than those two, whence M is a maximal ideal.

(ii) Sufficient part:

If M is a maximal ideal of R by the correspondence mentioned above R/M has only (0) and itself as ideals.

Furthermore R/M is commutative and has unit element. Since R enjoy's both these properties.

By previous thm, All the conditions are fulfilled for R/M. So, we conclude by the result of that lemma, that R/M is a field.

4/10/19

Integral domain:

A commutative ring is an integral domain if it has no zero divisors.

Imbedded ring :

A ring R can be imbedded in a ring R'

if there is a homomorphism of R onto R'.

Over ring :

R' will be called an over ring or

extension of R if R can be imbedded in R'.

Thm:

Every integral domain can be imbedded in

a field.

Proof

Let D be an integral domain and the

field quotients be a/b, where $a, b \in D$ &

$b \neq 0$.

Now, $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$ and

$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$

Let M be the set of all ordered pairs (a,b)

where $a, b \in D$ and $b \neq 0$.

Now, we define

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

i) Reflexive :

If $(a,b) \in M$, then $(a,b) \sim (a,b)$

Since $ab = ba$

Hence $\sim$ is reflexive.

ii) Symmetric:

If $(a,b), (c,d) \in M$.

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

$\Rightarrow cb = da$

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

iii) Transitive:

If $(a,b), (c,d) (e,f) \in M$

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

$(c,d) \sim (e,f) = cf = de$

Case (i)

Let $c = 0$, Now $ad = bc$ & $cf = de$

$ad = 0$ and $de = 0$

But $d \neq 0$. Hence $a = 0$ & $e = 0$

$af - be = 0$

Case (ii)

Let $c \neq 0$

We have $ad = bc$ and $cf = de$

$adcf = bcde$

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

$\therefore \sim$ is transitive.

Let (a,b) be equivalence class in M of (a,b) and let f be the set of all equivalence class of $[a, b]$ where $a, b \in D$ and $b \neq 0$.

(4)

We define,

$$[a, b] + [c, d] = [ad + bc, bd]$$

Since D is integral domain and both $b \neq 0$ & $d \neq 0$, we have that $bd \neq 0$ and hence

$$[ad + bc, bd] \in F$$

Now, $[a, b] = [a', b']$

$[c, d] = [c', d']$

Addition is well-defined,

$$[a, b] + [c, d] = [a'b'] + [c'd']$$

From $[a, b] = [a', b']$, we have $ab' = ba'$

From $[c, d] = [c', d']$, we have $cd' = dc'$

By above definition,

$$[ad + bc, bd] = [a'd' + b'c', b'd']$$

In equivalent terms,

$$(ad + bc)\, b'd' = bd\, (a'd' + b'c')$$

Using $ab' = ba'$, $cd' = dc'$

$$(ad + bc)\, b'd' = adb'd' + bcd'b' = ab'dd' + bb'cd'$$

$$= ba'dd' + bb'dc'$$

~~Clearly~~, $(ad + bc)\, b'd' = bd(a'd' + b'c')$

Clearly $[a, b]$ acts as zero element for this addition and $[-a, b]$ be inverse of $[a, b]$

Scanned by TapScanner

F is an abelian group under addition

5

Now $[a,b][c,d] = [ac, bd] \in F$

Then $[a,b] = [a',b']$, $[c,d] = [c',d']$

$[a,b][c,d] = [a', b'][c', d']$

$= [c'd'][a',b']$

$[a,b][c,d] = [c,d][a,b]$

Now, $[d,d]$ as unit element and $[c,d]^{-1} = [d,c]$

where $c \neq 0$, $[d,c]$ in F

F is abelian group under multiplication.

Now, we see that the distributive law holds

F, then F is field.

This shows that D is imbedded in F.

Here, $x \neq 0$, $y \neq 0$ in D then

$[ax, x] = [ay, y]$ because $(ax)y = x(ay)$

Let us denote $[ar, x]$ by $[a, 1]$

define $\phi : D \to F$ by $\phi(a) = [a, 1]$ for every $a \in D$.

Now, verify that ϕ is an isomorphism of D into F and D has unit element 1, then $\phi(1)$ is unit element in F.

Hence every integral domain can be imbedded in field.

Definition:

An integral domain R with element in a principle ideal ring if every ideal A in R of form $A = (a)$ for some $a \in R$.

Corollary to theorem 3.71

A Euclidean ring possesses a unit element.

Proof

Let R be a Euclidean ring then R is certainly an ideal of R.

We may conclude that $R = (u_0)$

Therefore, in particular, $u_0 = u_0 c$ for some $c \in R$.

If $a \in R$, then $a = x u_0$ for some $x \in R$, Hence

$$ac = (x u_0) c = x u_0 = a$$

Thus c is seen to be the required unit element.

Definition:

If $a \neq 0$ and b are in a commutative ring R then a is said to divides b if there exists a $c \in R$ such that $b = ac$.

We shall use the symbol a/b mean that a does not divides b.

The proof of the next remark is so simple and straight forward we omit it. 7

Remark:

1) If a/b and b/c then a/c

2) If a/b and a/c then $a/(b \pm c)$

3) If a/b then a/bx for all $x \in R$.

Definition:

If $a, b \in R$, then $d \in R$ is said to be greatest common divisor of a and b if

i, d/a and d/b

2) whenever c/a & c/b then c/d.

We shall use the notain $d(a,b)$ to denote that d is a greater common divisor of a & b.

Lemma

Let R be a Euclidean ring and $a, b \in R$.

If $b \neq 0$ is not a unit in R:

Now, $ab \in A$

if $d(ab) = d(a)$

Every element of A is multiple of ab.

Since, $a \in A$, must be multiple of ab where $a = abx$ for some $x \in R$.

Taking place on integral domain, we obtain

$$bx = 1$$

In this way b is unit in R.

which is contradiction to fact. That it was not a unit.

Hence the result.

$$d(a) < d(ab)$$

Definition: [Prime element]

In the Euclidean ring R, a non-unit π. It is said to be a prime element of R if whenever $\pi = ab$ where a, b are in R.

Then one of a or b is a unit in R. A Prime element is thus an element in R which cannot be factored in R in a non-trivial way.

Lemma:

Let R be a Euclidean ring. Then every element in R is either a unit in R or can be written as the product of finite number of Prime elements of R.

proof

By induction method on $d(a)$

If $d(a) = d(1)$, then a is a unit in R

We assume that lemma is true for all elements x in R. such that $d(x) < d(a)$

So, suppose that $a = bc$ where neither b nor c is a unit in R.

$d(b) < d(bc) = d(a)$ and

$d(c) < d(bc) = d(a)$.

Thus by our induction hypothesis b & c. Can be written as a product as a product a finite number of prime elements of R.

$$b = \pi_1 \pi_2 \cdots \pi_n ,$$

$$c = \pi_1' \pi_2' \cdots \pi_n' .$$

Where the π's and π''s are prime elements of R.

Consequently,

$$a = bc = \pi_1 \pi_2 \cdots \pi_n \pi_1' \pi_2' \cdots \pi_n' \text{ and}$$

In this way a has been factored as a product of a finite number of prime elements.

Definition : Relatively prime

In the Euclidean Ring R, a & b in R are said to be relatively prime if their greatest common divisor is a unit of R.

Since any associate of greatest common divisor is a greatest common divisor and since 1 is an associate of any unit, if a & b are relatively prime, we may assume that

$$(a,b) = 1.$$

Euclidean Ring: 33

An integral domain R is said to be Euclidean ring if for every $a \neq 0$ in R there is defined a non-negative integer $d(a)$ such that

(i) for all $a, b \in R$, both non-zero, $d(a) \leq d(ab)$

(ii) For any $a, b \in R$, both non zero, there exist $t, r \in R$ where either $r = 0$ or $d(r) < d(b)$

Theorem

Let R be an Euclidean ring and let A be an ideal of R. Then there exists an element $a_0 \in A$ such that A consists exactly of all $a_0 x$ as x ranges over R.

Proof

If A just consists of the element 0, put $a_0 = 0$ and the conclusion of the theorem holds.

Thus we may assume that $A \neq (0)$, hence there is an $a \neq 0$ in A.

Pick an $a_0 \in A$ such that $d(a_0)$ is minimal.

Suppose that $a \in A$. By the properties of Euclidean rings there exists $t, r \in R$. Such that $a = \pm a_0 + r$ where $r = 0$ or $d(r) < d(a_0)$.

Since $a_0 \in A$ and A is an ideal of R, ta_0 is in A.

Combined with $a \in A$ this results in a not $\in A$ but $r = a - ta_0$ where $r \in A$.

If $r \neq 0$, then $d(r) < d(a_0)$, giving as an element r in A whose d-value is smaller than that of a_0, in contradiction to our choice of a_0 as the element in a of minimal d-value.

Consequently, $r = 0$ and

$$0 = a - ta_0 \Rightarrow a = \pm a_0$$

Which proves the theorem.

Lemma

Let R be a Euclidean ring. Then any two elements a and b in R have a greatest common divisor d. Moreover $d = \lambda a + \mu b$ for some $\lambda \mu \in R$.

Lemma:

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 the a or b.

Proof

Let π be a prime element in the Euclidean ring R.

When ever π / ab where $a, b \in R$, then one of a (or) b is unit in R.

Then either π / a (or) $(\pi, a) = 1$.

π does not divides a, so

$$(\pi, a) = 1$$

If $(\pi, a) = \pi$, we get (π, a) and π divides b.

So, $(\pi, a) / b = \pi / b$

Hence proved.

Corollary:

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 $a_1, a_2, \dots a_n$.

Proof:

π is a prime element in the Euclidean ring R.

Whenever $\pi / a_1, a_2 \dots a_n$.

We carry the analogy between prime element.

$\pi / a_1, a_2 \cdots a_n$ (or) $\pi (a_1, a_2 \cdots a_n) = 1$

$\pi (a_1, a_2 \cdots a_n) = 1$

π divide a_1,

$\therefore \pi (a_1, a_2 \cdots a_n) / a_1 = \pi / a_1$

$|||^{ly}$, $(\pi, a_1, a_2 \cdots a_n) / a_2 = \pi / a_2$

$\vdots$

$(\pi, a_1, a_2 \cdots a_n) / a_n = \pi / a_n$

Theorem : UNIQUE FACTORIZATION THEOREM

Let R be a Euclidean ring and $a \neq 0$ is a nonunit in R, suppose that $a = \pi_1 \pi_2 \cdots \pi_n = \pi_1' \pi_2' \cdots \pi_m'$ where the π and π_j' are prime elements of R. Then $n = m$ and each π_i, $1 \leq i \leq n$ an associate of some π_j', $1 \leq j \leq m$ and conversely each π'_k is an associate of some π_q.

Proof

The relation $a = \pi_1 \pi_2 \cdots \pi_n = \pi_1' \pi_2' \cdots \pi_m'$.

But $\pi_1 / \pi_1 \pi_2 \cdots \pi_n$, hence $\pi_1 / \pi_1' \pi_2' \cdots \pi_m'$.

π_1 must divide some π_i'. Since π_1 and π_i' are both prime elements of R and π_1 / π_i'.

Scanned by TapScanner

They must be associate and $\pi_i' = u_1 \pi_1$,

where u_1 is a unit in R.

Thus, $\pi_1 \pi_2 \cdots \pi_n = \pi_1' \pi_2' \cdots \pi_m' = u_1 \pi_1 \pi_2' \cdots \pi_{i-1}' \pi_{i+1}' \cdots \pi_m'$ cancel of π_1 and we are left

with $\pi_2 \cdots \pi_n$ and $u_1 \pi_2' \cdots \pi_{i-1}' \pi_{i+1}' \cdots \pi_m'$.

Repeat the argument on this relation with π_2.

After n steps, the left sides becomes 1.

The right side a product of a certain numbers of π'. This would force $n \le m$ since the π' are not units.

$|||^{ly}$, $m \le n$, so that $n = m$

$\therefore$ Every π_i has some π_i' as an associate and

Conversely.

Lemma

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

Proof ~~Sufficient part~~: Neccessary part:

If a_0 is not a prime element, then

$A = (a_0)$ is not a maximal ideal.

For suppose that $a_0 = bc$ where $b c \in R$ and

neither b nor c is a unit.

Let $B = (b)$, then certainly $a_0 \in B$, so that

$A \subset B$.

We claim that $A \neq B$ and $B \neq R$.

If $B = R$. Then $1 \in B$ so that $1 = xb$ for some $x \in R$ forcing b to be a unit in R. which it is not.

On the other hand, if $A = B$ and $b \in B = A$

Whence $b = xa_0$ for some $x \in R$.

Combined with $a_0 = bc$ this result in $a_0 = xca_0$ in consequence of which $xc = 1$.

But this forces c to be a unit in R, again contradicting our assumption.

Therefore, B is neither A nor R and since $A \subset B$, A cannot be maximal ideal of R.

Sufficient part:

Conversely,

Suppose that a_0 is a prime element of R and U is an ideal of R such that

$$A = (a_0) \subset U \subset R, \quad U = (u_0)$$

Since $a_0 \in A \subset U \doteq (u_0)$, $a_0 = xu_0$ for some $x \in R$. But a_0 is a prime element of R, from which it follows that either x (or) u is a unit in R.

If u_0 is a unit in R. Then $U = R$.

If on the other hand, x is a unit in R, then $x^{-1} \in R$ and the relation $a_0 = xu_0$ becomes

$u_0 = x^{-1} a_0 \in A$.

Since A is an ideal of R

This implies that $U \subset A$, together $A \subset U$, we include that $U = A$.

$\therefore$ There is no ideal of R which fits strictly b/w A and R.

$\therefore$ $A = (a_0)$ is a maximal ideal of R.

A particular Euclidean Ring

Defn: Gausian Integers:

Let $J[i]$ denote the set of all complex numbers of the form $a+bi$ whence a and b are integers;

Under the addition & multiplication of complex numbers $J[i]$ forms an integral domain called the domain of Gaussian integers.

Our first objectives is to exhibit $J[i]$ as a Euclidean ring. In order to do this we must first introduce a function $d(x)$ defined for every non-zero element in $J[i]$ which satisfies

(i) $d(x)$ is a non-negative integer for every

$x \neq 0 \in J[i]$

ii) $d(x) \leq d(x, y)$ for every $y \neq 0$ in $J[i]$

iii) Given $u, v \in J[i]$ there exist $t, r \in J[i]$

such that $v = tu + r$ where $r = 0$ (or) $d(r) < d(u)$.

Theorem

$J[i]$ is a Euclidean ring.

Proof

Gn, $x, y \in J[i]$, there exists $t, r \in J[i]$

such that $y = tx + r$, where $r = 0$ (or) $d(r) < dx$

where y is a arbitary in $J[i]$ but where

x is a positive integer n.

Suppose that $y = a + bi$ by the division

algorithm for the ring of integer. We can find

integers satisfies

$$|u_1| \leq \tfrac{1}{2} n \quad \text{and}$$

$$|v_1| \leq \tfrac{1}{2} n$$

Let $t = u + vi$ and $r = u_1 + v_1 i$,

Then $y = a + bi$

$\Rightarrow$ ~~[illegible]~~

$\Rightarrow u_n + u_1 + (v_n + v_1) i = (v + v_i) n + v_i + v_1 i = tn + r$

Scanned by TapScanner

Since, $d r = d(u_1 + v_i) = U_1^2 + V_1^2 \le \frac{n^2}{4} < n^2 = d(n)$

We have shown that $y = t_n + r$ with $r = 0$ (or)

$d(r) < d(n)$.

General case

Let $x \neq 0$ and y be arbitary element in $J[i]$.

Thus $x\bar{x}$ is a positive integer where $\bar{x}$ is the complex conjugate of x. Applying to the element $y\bar{x}$ and x we see that there elements $t, r \in J[i]$ such that $y\bar{x} = t_n + r$ with $r = 0$ (or) $d(r) < d(n)$..

Putting into relation $n = x \cdot \bar{x}$, we obtain

$d(y\bar{x} - tx \cdot \bar{x}) < d(n) = d(x \cdot \bar{x})$ applying to

$d(y\bar{x} - tx \cdot \bar{x}) = d(y \cdot tx)\, d(\bar{x})$ and $d(x \cdot \bar{x}) = d(x) d(\bar{x})$

We obtain that

$d(y - t(x))\, d(\bar{x}) < d(x)\, d(\bar{x})$

Since, $x \neq 0$, $d(\bar{x})$ is a positive integer, so this inequality simplifier to $d(y - t(x)) < d(x)$.

We represent $y = tx + r_0$, where $r_0 = y - tx$,

Thus t and r_0 are in $J[i]$ and $r_0 = 0$ (or)

$d(r_0) = d(y - tx) < dx$.

This proves the theorem.

Lemma

Let p be a prime integer and suppose that for some integer c relatively prime to p, we can find into x and y such that $x^2+y_p^2 = cp$.

Then p can be written as the sum of squares of two integers.

i.e) There exists integers a & b such that $p = a^2+b^2$.

Proof

The ring of integers is a subring of $J[i]$

Suppose that the integer p is also a prime element of $J[i]$. Since,

$$cp = x^2+y^2 = (x+yi)(x-yi)$$

$$\frac{p}{(x+yi)} \text{ (or) } \frac{p}{(x-yi)} \text{ in } J[i].$$

But if $\frac{p}{(x+yi)}$ then $(x+yi) = p(u+vi)$ which would say that $x = pu$ and $y = pv$.

So that p also would divide $x-yi$. But then $\frac{p^2}{(x+yi)(x-yi)} = cp$ from which we could

Conclude that p/c. Contrary to assumption,

$|||^{ly}$ if $\frac{p}{x-y}$. Thus p is not a prime element in $J[i]$!

In Consequence of this

$$p = (a+bi)(g+di)$$

where $(a+bi)$ and $(g+di)$ are in $J[i]$ and where neither $a+bi$ nor $g+di$ is unit in $J[i]$

But this means that neither $a^2+b^2=1$ nor $g^2+d^2=1$.

$p = (a+bi)(g+di)$, it follow easily that

$$p = (a-bi)(g-di)$$

$$p^2 = (a+bi)(g+di)(a-bi)(g-di)$$

$$= (a^2+b^2)(g^2+d^2)$$

$\therefore \frac{a^2+b^2}{p^2}$ so $a^2+b^2=1$, for p^2, $a^2+b^2 \neq 1$

$\because$ $a+bi$ is not a unit in $J[i]$.

$a^2+b^2 \neq p^2$ otherwise $g^2+d^2=1$. Contrary to the fact that $g+di$ is not a unit in $J[i]$.

This is the only feasibility left is that $a^2+b^2=p$ and the lemma is thee by established.

Lemma

Let R be a Euclidean ring. Then any two elements a and b in R have a greatest common divisor d. Moreover $d = \lambda a + \mu b$

Proof

Let A be a set of all elements $ra + sb$ where r, s ranges over R. We claim that A is an ideal of R.

For Suppose that $x, y \in A$ therefore

$x = r_1 a + s_1 b$, $y = r_2 a + s_2 b$ and so

$$x \pm y = (r_1 \pm r_2)a + (s_1 \pm s_2) b \in A.$$

$|||^{ly}$, for any $u \in R$, $ux = u(r_1 a + s_1 b)$

$$= (ur_1)a + (us_1)b \in A$$

Since A is an ideal of R by thm 3.7.1

There exists an element $d \in A$ such that every element in A is a multiple of d.

By of the fact that $d \in A$ and that every element of A is of the form $ra + sb$,

$d = \lambda a + \mu b$ for some $\lambda \mu \in R$.

Now by the corollary to thm 3.7.1, R has a unit element 1; thus $a = 1a + 0b \in A$,

$$b = 0a + 1b \in A$$

in A, they are both multiples of d, whence d/a and d/b.

Scanned by TapScanner

Suppose family that c/a and c/b then $c/\lambda a$ and $c/\mu b$ so that c certainly divides $\lambda a + \mu b = d$.

$\therefore$ d has all the requisite conditions for a greatest common divisor and the lemma is proved.

Definition:

Let R be a commutative ring with unit element. An element $a \in R$ is a unit in R if there exists an element $b \in R$ such that $ab = 1$.

Do not confuse a unit with a unit element 1. A unit in a ring is an element whose inverse is also in the ring.

Polynomial rings:

Let f be a field. By the ring of Polynomials in the indeterminant, x written as $F[x]$. We mean the set of all symbols $a_0 + a_1 x + a_2 x^2 + \dots + a_n x_n$, where n can be any non-negative integer and where the co-efficient $a_1 a_2 \dots a_n$ are all in F.

Scanned by TapScanner

Definition:

If $p(x) = a_0 + a_1 x + \cdots + a_m x^m$ and

$q(x) = b_0 + b_1 x + \cdots + b_n x$ are in $F[x]$, then

$p(x) = q(x)$. If and only if for every integer $i \geq 0$,

$a_i = b_i$. Thus two polynomials are declared to be

equal iff this corresponding co-efficients are equal.

Definition:

If $p(x) = a_0 + a_1 x + \cdots + a_m x^m$ and

$q(x) = b_0 + b_1 x + \cdots + b_n x^n$ are both in $F[x]$,

then $p(x) + q(x) = c_0 + c_1 x + \cdots + c_p x^i$ where

for each i, $c_i = a_i + b_i$

Definition:

If $p(x) = a_0 + a_1 x + \cdots + a_m x^m$ and

$q(x) = b_0 + b_1 x + \cdots + b_n x^n$, then $p(x)\, q(x) =$

$c_0 + c_1 x + \cdots + c_k x^k$ where $c_t = a_1 b_0 + a_{t-1} b_1 +$

$a_{t-2} b_2 + \cdots + a_0 b_t$

This defn:- says nthg more than; multiply the two polynomials by multiplying out the symbols, formally, use the relation $x^\alpha x^\beta = x^{\alpha+\beta}$ and collect terms.

Scanned by TapScanner