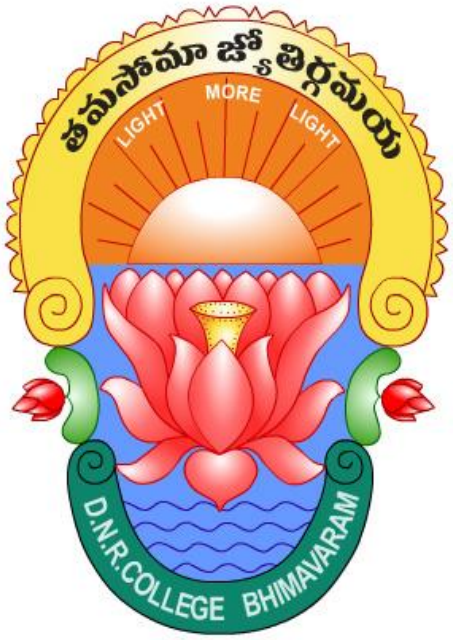
DNR COLLEGE P.G COURSES (AUTONOMOUS)

(AFFILIATED TO ADIKAVI NANNAYA UNIVERSITY)

P.G DEPARTMENT OF MATHEMATICS



I M.Sc MATHEMATICS

ALGEBRA - 1

UNIT – 1

PREPARED BY:

M.SURYA SIRISHA

Assistant Professor

D.N.R College(A),

Bhimavaram.

Definition:

Endomorphism:A homomorphism of a group G into itself is calledendomorphism

Automorphism:

An isomorphism from a group G onto itself is called an "Automorphism".

The set of all automorphisms of G is denoted by AUT(G).

Inner automorphism:

let G be a group and a€G the automorphism fa: G→G defined by $f_a(x)$ =axa-1 for all x€G is called an" inner automorphism of G" and It is denoted by In(G)

In (G) = {fa/a€G}

Outer automorphism:

An automorphism which is not inner is called an "outerautomorphism"

statement: The set AUT(G) of all Automorphism of a group G is a group under composition of mappings and IN(G)ΔAUT(G)Moreover G/Z(G) ≈IN (G)

proof:step (1): Given that G is a group

Consider AUT (G) = {f/f: G→G is an Automorphism}

claim:AUT (G) forms a group with respective toComposition of mappings.

Clearly, I€AUT (G)

AUT (G) ≠ϕ⊆S_G a symmetric group

∴gof€AUT (G)

ii) Let f € AUT(G)

⇒f:G→G is an automorphism

⇒f^{-1} : G→G is a bijective

f^{-1} :G→G is a homomorphism: Now $f[f^{-1}(x).f^{-1}(y)]=f[f^{-1}(x)].f[f^{-1}(y)]$

= I(x).I(y)

=xy

$\Rightarrow f[f^{-1}(x).f^{-1}(y)] = xy$

$f^{-1}(x).f^{-1}(y) = f^{-1}(xy)$

f^{-1} :G→G is an automorphism

$\therefore f^{-1} \in AUT(G)$

∴AUT(G) < SG

Hence AUT (G) forms a group with respective to Composition of mappings**.**

step (2):IN (G) ΔAUT (G): We know that f_a: G→G defined by$f_a(x) = axa^{-1}$, ∀ x€G is an automorphism of G.

Now IN (G) = $\{f_a / a \in G\}$

I)i)**IN(G)<AUT(G) :** let $f_a, f_b \in IN(G), x \in G$

i) Let f, g € AUT (G)

⇒f:G→G is an automorphism andg:G→G is also anautomorphism.

⇒gof:G→G is bijective

gof:G→G is homomorphism:

Let x,y€G

[gof (xy)] =g [f (xy)]

=g [f(x) f(y)]
=g [f(x)] g [f(y)]
= (gof)(x). (gof)(y)

∴gof:G→G is an automorphism

Now $(f_a.f_b)(x)=f_a(f_b(x))$

$= f_a(bxb^{-1})$

$=a(bxb\text{-}1)a^{-1}$

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

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

$=f_{ab}(x)$

$\therefore (fa.fb)(x)=fab(x)\ \forall x€G$

$\Rightarrow f_a.f_b= f_{ab}$ € IN (G)

$\Rightarrow f_a.f_b$€ IN(G)

ii) Let fa € IN(G)

$\Rightarrow$a € G

$\Rightarrow a^{-1}$ € G

$\Rightarrow f_{a-1}$ € IN(G)

Now $f_a.f_{a-1} =f_{aa-1}=f_e$

$\therefore (f_a)^{-1} = f_{a-1}$ € IN (G)

$\Rightarrow$ (fa)$^{-1}$ € IN (G)

$\therefore$IN (G) <AUT(G)

2) IN (G) is Normal in AUT (G): Let fa € IN (G) and f € AUT (G)

Aim: $f.f_a.f^{-1}$ € IN (G)

Let x € G

Now $[f.f_a.f^{-1}](x) = f\{f_a[f^{-1}(x)]\}$

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

$= f(a).f(f^{-1}(x)).f(a^{-1})$

$=c.x.c^{-1}$ where c = f(a) € G

$= f_c(x)$

$\therefore [f.f_a.f^{-1}](X) = f_c \forall\ x \in G$

$\Rightarrow f.f_a.f^{-1} = f_c \in IN(G)$

$\Rightarrow f.f_a.f^{-1} \in IN(G)$

$\therefore IN(G)\ \Delta\ AUT(G)$

step (3): G/Z (G) ≈ IN (G): We know that $Z(G)=\{a \in G/ax = xa\ \forall\ x \in G\}$

Define a mapping $\phi: G \rightarrow IN(G)$ by$\Phi(a) = f_a, \forall\ a \in G$

Clearly, ϕ is well defined

Φ is onto:Let $f_a \in IN(G)$

$\Rightarrow a \in GA$ also $\phi(a) = f_a$

∴every element in IN(G) has per-image in G

Φ is a homomorphism: Let $a, b \in G$

Now, $\phi(a\ b) = f_{ab}=f_a.f_b=\phi(a).\phi(b)$

$\therefore \phi: G \rightarrow IN(G)$ is an onto homomorphism

By fundamental theorem of homomorphism,

We have $G/ker\phi \approx IN(G)$

Finally, to prove that $ker\phi = Z(G)$:

Now$ker\phi = \{a \in G / \phi(a) =$ an identity element in G$\}$

$=\{a \in G / f_a = f_e\}$

$=\{a \in G / f_a(x) = f_e(x), \forall\ x \in G\}$

$=\{a \in G / axa^{-1} = exe^{-1}, \forall\ x \in G\}$

$= \{a \in G / axa^{-1} = x, \forall\ x \in G\}$

$=\{a \in G / ax = xa, \forall x \in G\}=Z(G)$

$\therefore G/Z(G) \approx IN(G)$

problem :Let G be a group and a€G.The mapping $f_a : G \to G$ is defined by

$f_a(x) = axa^{-1}$,$\forall x \in G$ is anautomorphism of G

solution: Given thatG is a group and a € G

Define a mapping $f_a : G \to G$ by $f_a(x) = axa^{-1} \forall x \in G$

claim:$f_a \in AUT(G)$

$f_a$is one-one: Let x,y € G

Let, $f_a(x) = f_a(y)$

$axa^{-1} = aya^{-1}$

$x = y$

f_a is onto : Let y € G

Then we get $a^{-1}ya \in G$

Now $f_a(a^{-1}ya) = a(a^{-1}ya)a^{-1}$

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

$=eye=y$

∴Every element in co domain has pre-image inDomain.

$f_a : G \to G$ is a homomorphism: Let x, y € G

Now $f_a(xy) = axa^{-1}$

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

$=(axa^{-1})(aya^{-1})$

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

$\therefore f_a(xy) = f_a(x).f_a(y)$

$\therefore f_a : G \to G$ is an automorphism

$\therefore f_a \in AUT(G)$

Conjugacy and G-sets:

Definition: Let G be a group and X is a set. Then G is said to "act on X". If ∃ a mapping $\varphi : GxX \to X$ with $\varphi(a,x)=a*x$ such that I) $a*(b*x) = ab*x$

II) $e*x = x$,∀a ,b ∈ G , x ∈ X.

The mapping φ is called "the action of G on X".X is said to be a "G - set"

Example (1): Let G be a group and a ∈G we defined $a*x = axa^{-1}$ for a ∈ G, x ∈ GThen show that G is a G-set.

solution: Let G be a group and G be a set.

claim: G is a G – set.

Define $\varphi: GxG \to G$ by $\varphi(a, x) = a*x = axa^{-1}$

Let a, b ∈ G

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

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

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

$= ab*x$

$\therefore a*(b*x) = ab*x$

ii) $e*x = exe^{-1} = exe = x$

$\therefore e*x = x$

∴ G is a G – set.

Examle(2) : Let G be a group and H<G then the set G/H of all left cosets in a G is a G – set by defining a*xH = axH ,∀a € G, xH € G/H.

solution: Let G be a group and H<G

We know that G/H = {xH/x€G}

claim: G/H is a G – set.

Define φ: G x G/H → G/H by φ(a,xH)=a*xH = axH∀a € G, xH € G/H

Let a, b € G, xH € G/H

i) a*(b*xH) = a*(bxH)

= abxH
=ab*xH

∴a*(b*xH) = ab*xH

ii) e*xH = exH=xH

∴e*xH = xH

∴G/H is a G – set.

Theorem : Let g be a group and let x be a set.if x is a g – set, then the action of g on x induces a homomorphism φ : g →$s_x$any homomorphism φ : g → sx induces an action of g onto x

proof: Let G be a group and let X be a set

I. Suppose that X is a G – set

For any a € G ,

Define a mapping f_a : X→X by $f_a(x)$ = ax ,∀x€X

Clearly, fa is one – one and onto

∴fa is bijective

∴fa € Sx

Define a mapping $\varphi: G \to Sx$ by $\varphi(a) = f_a, \forall a \in G$

Let , $x \in X$

Now $(f_a.f_b)(x) = f_a(f_b(x))$

$= f_a(bx)$

$=a(bx)$

$=(ab)x$

$=f_{ab}(x)$

$\therefore f_a.f_b = f_{ab}$

φ is homomorphism: Let a ,b ∈ G

Now $\varphi(ab) = f_{ab} = f_a.f_b = \varphi(a).\varphi(b)$

$\therefore \varphi(ab) = \varphi(a).\varphi(b)$

II)Let $\varphi: G \to Sx$ be a homomorphism

claim: X is a G – set

Define $a * x = [\varphi(a)](x) \ \forall \ a \in G , x \in X$

Let a, b ∈ G , x ∈ X

I) $a*(b*x) = a*(\varphi(b)(x)) = [\varphi(a)](\varphi(b)(x))$

$= [\varphi(a).\ \varphi(b)](x)$

$= [\varphi(ab)](x)$

$= ab *x$

$\therefore a*(b *x)=ab *x$

II) $e*x = [\varphi(e)(x)] = fe(x) = ex = x$

$\therefore e*x = x$

$\therefore$ X is a G – set

State and Prove Cayley's theorem

statement:let g be a group then g is an isomorphic into the symmetric group S_G

proof :let G be a group and G be a set .

by known theorem , G is a G – set .

by known result,∃ a homomorphism $\varphi : G \rightarrow S_G$ defined by$[\varphi(a)](x) = ax, \forall x \in G$**claim :**$G \approx S_G$

φ is one – one :i.e., it is enough to show that Ker φ = {e}

Now Ker $\varphi = \{a \in G / \varphi(a) = I\}$

$= \{a \in G / \varphi [(a)](x) = I(x) , x \in G\}$

$= \{a \in G / ax = x\}$

$= \{a \in G / ax = ex\}$

$= \{a \in G / a = e\}$

$= \{e\}$

∴ Ker φ = {e}

∴φ is one- one

∴φ: G → SG is an into isomorphism

∴ G ≈ SG

Hence proved.

Theorem :let "G"be a group and H<G of finite index "n" then there is a homomorhism $\varphi:G \rightarrow S_n$ such that Ker $\varphi = \cap x \in G\ xHx^{-1}$

proof: Let H<G of finite index n .

∴ |G/H| = n also $S_{G/H} \approx S_n$

by known theorem , G/H is a G – set .

$\Rightarrow \exists$a homomorphism $\varphi: G \to S_{G/H}$ defined by $[\varphi(a)](xH) = axH \forall x \in G$

we get , $\exists$ a homomorphism $\varphi : G \to S_n$ defined by $[\varphi(a)](xH) = axH \forall\ x \in G$

claim:Now Ker = $\{a \in G / \varphi(a) = I\}$

$= \{a \in G / [\varphi(a)](xH)$

$= I(xH), \forall \in G/H\}$

$= \{a \in G / axH = xH, \forall\ x \in G\}$

$= \{a \in G / a(xHx^{-1}) = (xHx^{-1}), \forall\ x \in G\}$

$= \{a \in G / a \in xHx^{-1}, \forall\ x \in G\}$

$= \cap_{x \in G}\ xHx^{-1}$

Ker $\varphi = \cap_{x \in G} xH\ x^{-1}$

Hence $\exists$ a homomorphism $\varphi : G \to S_n$ such thatKer $\varphi = \cap_{x \in G} xH\ x^{-1}$.

Note (1): $|G| = \Sigma_{a \in G} O(G)/O(N(a))$ is called the "class equation of G".

Note (2): $|G| = \Sigma_{a \in G} O(G)/O(N(a))$

$= \Sigma_{a \in Z} O(G)/O(N(a)) + \Sigma_{a \notin Z} O(G)/O(N(a))$

$= \Sigma_{a \in Z} O(G)/O(G) + \Sigma_{a \notin Z} O(G)/O(N(a))$

$\therefore |G| = |Z| + \Sigma_{a \notin Z}\ O(G)/O(N(a))$.

Note (3): If $|G| = p^n$, where p is prime then $Z \neq \{e\}$ (or) G hasNon-trivial center.

Note (4): G is abelian $\Leftrightarrow Z = G$

Result : show that every group of order p^2 isabelian.

Proof: let g be a group $\ni$ $o(g) = p^2$

claim: G is abelian

i.e., it is enough to show that Z = G

We know that $Z = \{a \in G / ax = xa\ \forall x \in G\}$

By know result, $Z \leq G$, G is finite.

By Lagrange's theorem O(Z) /O(G)

$\Rightarrow O(Z)/P^2$

$\Rightarrow O(Z) = 1$ (or) $O(Z) = P$ (or) $O(Z) = P^2$

i) Since O (G) = P2

By known result, $Z \neq \{e\}$

$\Rightarrow O(Z) > 1$

$\therefore O(Z) \neq 1$

ii) Let O(Z) = P

Let $a \in G \ni a \notin Z$

We know that $N(a) \leq G$ also $Z \subseteq N(a)$

$\Rightarrow O(N(a))/O(G)$

$\Rightarrow O(N(a))/p2$

$\Rightarrow O(N(a)) = p2$

$\Rightarrow O(N(a)) = O(G)$

$\Rightarrow N(a) = G$

$\Rightarrow a \in Z$

Which is contradiction to $a \notin Z$

$\therefore O(Z) \neq p$

$\therefore O(Z) = p2 = O(G)$

$Z = G$

G is abelian.

STATE AND PROVE BURNSIDE THEOREM:

statement:let G be a finite group acting on a finite set xthen the number k of orbit in x under G is $K = 1/|G| \Sigma_{g \in G} |x_g|$

proof: Define, $S = \{(g, x) \in GxX / gx = x\}$

$\therefore |S| = |X_g| = |G_x|$

$|S| = \Sigma_{g \in G} |x_g| = \Sigma_{x \in X} |G_x|$ ------- (1)

We know that, $|Gx| = |G| / |G_x|$

$\Rightarrow |G_x| = |G| / |Gx|$

$\Rightarrow \Sigma_{x \in X} |G_x| = \Sigma_{x \in X} |G| / |Gx|$

$= |G| \Sigma_{x \in X} 1 / |Gx|$

$= |G| \Sigma_{a \in C} \Sigma_{x \in Ga} 1 / |Ga|$

Where C contains exactly one element from each orbit.

$= |G| \Sigma_{a \in C} [1/|Ga| + 1/|Ga| + \text{--- (|Ga| times)}]$

$= |G| \Sigma_{a \in C} |Ga| / |Ga|$

$= |G| \Sigma_{a \in C} (1)$

$= |G|. K$

$\Sigma_{x \in X} |G_x| = |G|. K$

$K = 1/|G| \Sigma_{x \in X} |G_x|$

$\therefore K = 1/|G| \Sigma_{g \in G} |x_g|$

Hence proved.

SOLVABLE GROUP:

Definition :solvable group:

A group G is said to be "solvable" if $G^{(k)} = \{e\}$ for some integer k.

Theorem: Every homomorphic image of a solvable group is solvable.

proof: let G be a solvable group

i.e., $G^{(k)} = \{e\}$ for some integer k

Let $\varphi: G \to G^*$ be a homomorphism

Let G^* be the homomorphic image of G under φ

claim: G^* is solvable

Now, $(G^*)^{(k)} = \varphi(G^{(k)})$

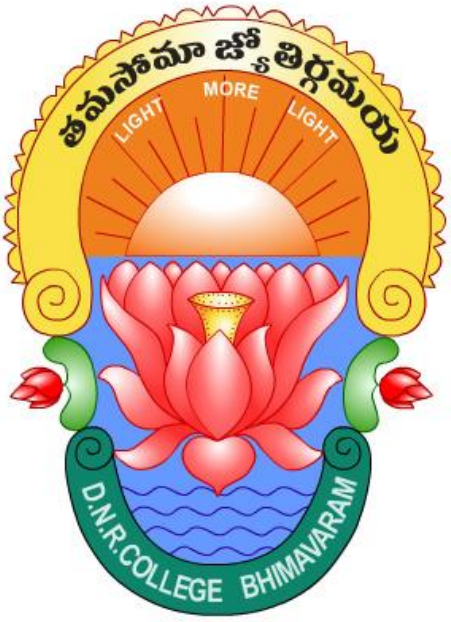
$= \varphi(e)$
$= \{e^*\}$

$\therefore G^*$ is solvable.

DNR COLLEGE P.G COURSES (AUTONOMOUS)

(AFFILIATED TO ADIKAVI NANNAYA UNIVERSITY)

P.G DEPARTMENT OF MATHEMATICS



I M.Sc MATHEMATICS

ALGEBRA - 1

UNIT – 2

PREPARED BY:

M.SURYA SIRISHA

Assistant Professor

D.N.R College(A),

Bhimavaram.

Theorem: let $H_1, H_2, ---H_n$ be a family of subgroups of a group G&

let $H = H_1, H_2, ---H_n$ if $H_i \Delta H$ & $H_i \cap (H_1 ---H_{i-1}H_{i-+1}---H_n) = (e)$ for $1 \leq i \leq n$ then show that $H_1 x H_2 x ---x H_n \approx H$.

Proof: Suppose that $H_1, H_2, ---H_n$ be a family of subgroups ofa group G &

$H = H_1.H_2.---H_n$ $H_i \Delta H$ & $H_i \cap (H_1 ---H_{i-1}\ H_{i-+1}---H_n) = (e) \rightarrow (1)$

Claim: $H_1 x H_2 x ---x\ H_n \approx H$.

Let $x \in H_i$, $y \in H_j$

By (1), $H_i \cap H_j = \{e\}$

$\Rightarrow xy = yx \longrightarrow (2)$

Define a mapping $\varphi: H_1 x H_2 x ---x\ H_n \rightarrow H$ by

$\varphi(x_1, x_2, ---, x_n) = x_1.x_2.---.x_n \forall\ x_i \in H_i \rightarrow (3)$

i) φ is homomorphism:

Now, $\varphi[(x_1, x_2, ---, x_n).(y_1, y_2, ---, y_n)] = \varphi[(x_1y_1, x_2y_2, ---, x_ny_n)]$

$= x_1y_1.x_2y_2.---.x_ny_n$

By using equation(2),we get

$= [x_1.x_2.---.x_n][y_1.y_2.---.y_n]$

$= \varphi(x_1, x_2, ---, x_n)\varphi(y_1, y_2, ---, y_n)$

$\therefore \varphi$ is homomorphism

ii) φ is one – one:

To prove that ker $\varphi = \{e\}$

Let $(x_1, x_2, ---, x_n) \in \ker \varphi$

$\varphi(x_1, x_2, ---, x_n) = e$

$x_1.x_2.---.x_n = e$

$x_1x_1^{-1}.x_2.---.x_n = x_1^{-1}e$

$x_2.---.x_n = x_1^{-1}$

Since $x_1^{-1} \in H_1$ also $x_1^{-1} \in H_2 --- H_n$

$\Rightarrow x_1^{-1} \in H_1 \cap (H_2 \text{---} H_n)$

$\Rightarrow x_1^{-1} = e$

$\Rightarrow x_1 = e$

Similarly, we get $x_2 = e, \text{---}, x_n = e$

$\Rightarrow (x_1, x_2, \text{---}, x_n) = (e, e, \text{---}, e)$

$\therefore \ker \varphi = \{e\}$

$\therefore \varphi$ is one – one

Clearly, φ is onto

$\varphi: H_1 x H_2 x \text{---} x H_n \rightarrow H$ is isomorphism $H_1 x H_2 x \text{---} x H_n \approx H$.

FIRST SYLOW THEOREM:

Statement: Let G be a finite group and let p be prime. If $p^m / O(G)$ but $p^{m+1} \nmid O(G)$ then G has a subgroup of order p^m

Proof: Given that G be a finite group and let p be prime.

If $p^m / O(G)$ but $p^{m+1} \nmid O(G)$

Claim: G has a subgroup of order p^m

To prove this result by induction on O(G) .

Case(i): If O(G) = 1 then the result is true

Case(ii): Assume that the result is true for all finite abelian groups whose

orders< O(G)

Case(I): suppose that G has a proper subgroup $H \ni p^m / O(H)$

Clearly, $H \subset G$

$\Rightarrow O(H) < O(G)$

By induction hypothesis, H has a subgroup T of order pm

i.e., T<H and $O(T) = p^m$

$\because T < H < G$

$T < G, O(T) = p^m$

∴ G has a subgroup T of order p^m

CASE(II):suppose that G cannot have a proper subgroup H ∋ $p^m/O(G)$

i.e., ∋ $p^m \nmid O(H)$

Claim:G has a subgroup of order pm

By class equation in G,

we have $|G| = |Z| + \Sigma_{a \notin Z} O(G)/O(N(a))$

$\Rightarrow |Z| = |G| - \Sigma_{a \notin Z} O(G)/O(N(a)) \rightarrow (1)$

Here p/p^m and $p^m/O(G)$

$\Rightarrow p/O(G)$ ----(2)

Clearly, N(a) < G

$\Rightarrow p^m \nmid O(N(a))$

$\Rightarrow p^m/[O(G)/O(N(a))]$

$\Rightarrow P^m/ \Sigma_{a \notin Z} O(G)/O(N(a))$

$\Rightarrow p/ \Sigma_{a \notin Z} O(G)/O(N(a))$ ---(3)

From (2) & (3)

$p/ [|G| - \Sigma_{a \notin Z} O(G)/O(N(a))]$

$\Rightarrow p/ |Z|$ by (1)

By Cauchy's theorem for abelian groups ∃ an element $b€Z \ni b^p=e$

i.e., O(b) = p

Let B =<b>be a cyclic subgroup Of G

Clearly, O(B) = O(b) = p

Since b € Z

$\Rightarrow <b> \Delta G$

$\Rightarrow B \Delta G$

G/B ={xB/x € G}

Let $\bar{G}= G/B$

$\Rightarrow O(\bar{G}) = O(G/B) = O(G)/O(B)$

$= p^m.n/p$

$= p^{m-1}.n$

$O(\bar{G}) = p^{m-1}.n$

$p^{m-1}/O(\bar{G})$,also $p^m \nmid O(\bar{G})$

Since $O(\bar{G}) = O(G)/O(B) < O(G)$

By induction hypothesis,

$\bar{G}$ has a subgroup $\bar{p}$ of order p^{m-1}

i.e., $p < G$, $O(P) = P^{m-1}$

Consider the set $p=\{x \in G/xB \in p\}$

$P < G$ also, we have $\bar{p} \approx P/B$

$\Rightarrow O(\bar{P}) = O(P/B)$

$\Rightarrow O(\bar{p}) = O(P)/O(B)$

$\Rightarrow O(p) = O(\bar{p}).O(B)$

$= p^{m-1}.p$

$O(p) = p^m$

$\therefore \exists\ P < G \ni O(p) = p^m$

Hence , G has a subgroup of order p^m

Hence , the result is holds for G by using induction .

Definition: let A,B be two subgroups of a group G. A&B are said to be conjugate if $A = xBx^{-1}$ for some $x \in G$

STATE AND PROVE SECOND SYLOW THEOREM:

Statement: Let G be a finite group and p be prime, $p^n/O(G)$ but $p^{n+1} \nmid O(G)$ then any two subgroups of order p^n are conjugate.

Proof: Assume that,$A<G,B<G \ni O(A)=p^n, O(B)=p^n$

Claim: A & B are conjugate

i.e., it is enough to show that $A = xBx^{-1}$ for some $x \in G$

If possible suppose that $A = xBx^{-1} \forall x \in G$

$\Rightarrow A \cap xBx^{-1} = \varphi \subseteq A$

$\Rightarrow A \cap xBx^{-1} \subseteq A$

$\Rightarrow O(A \cap xBx^{-1}) < O(A)$

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

We know that, $O(AXB) = O(A)O(B)/O(A \cap xBx^{-1})$

$= p^n.p^n/p^m$

$= p^{2n-m} \rightarrow (1)$

Since $m<n$

$\Rightarrow n>m$

$\Rightarrow n-m>0$

$\Rightarrow n-m \geq 1$

$\Rightarrow n+(n-m) \geq n+1$

$\Rightarrow 2n-m \geq n+1$

$\Rightarrow p^{2n-m} \geq p^{n+1}$

$\Rightarrow p^{n+1} \leq p^{2n-m}$

$\Rightarrow p^{n+1}/p^{2n-m}$

$\Rightarrow p^{n+1}/\Sigma O(AXB)$

$\Rightarrow P^{n+1}/O(G)$

Which is a contraction to $p^{n+1} \nmid O(G)$

Our assumption is wrong

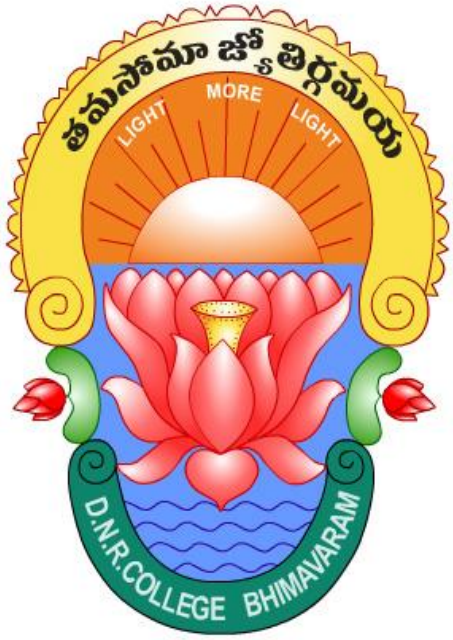
$A = xBx^{-1}$ for some $x \in G$

Hence, A & B are conjugate.

DNR COLLEGE P.G COURSES (AUTONOMOUS)

(AFFILIATED TO ADIKAVI NANNAYA UNIVERSITY)

P.G DEPARTMENT OF MATHEMATICS



I M.Sc MATHEMATICS

ALGEBRA - 1

UNIT – 3

PREPARED BY:

M.SURYA SIRISHA

Assistant Professor

D.N.R College(A),

Bhimavaram.

DEFINITIONS:

Ring: Let R be a non-empty set and +, .be two binary operations in R then the algebraic structure (R,+, .) is said to be RING if (R,+) is a commutative group

(R, .)is a semi-group Distributive laws.

Commutative Ring: In a ring (R,+, .) if a.b = b.a for a,b € R then we say that R is commutative ring.

Field: let R be a commutative ring with unity elements if every non-zero element of R is invertible under multiplication then R is a field.

Right Ideal:let R be a ring and $U \neq \varphi \subseteq R$ we say that U is a right ideal in R. If

i) a,b € U ⇒ a-b € U

ii) a € U,r € R ⇒ar € U.

Left Ideal:let R be a ring and $U \neq \varphi \subseteq R$ we say that U is a left ideal in R. If

i) a,b € U ⇒ a-b € U

ii) a € U ,r € R ⇒ra € U

Ideal:let R be a ring and $U \neq \varphi \subseteq R$ we say that U is an ideal in R. If

i) a,b € U ⇒ a-b € U

ii) a € U ,r € R ⇒ar,ra € U.

Trivial&Non-Trivial Ideals: In a ring R , the ideals {0} and R are called trivial(or)improperideals in R and all other ideals of R are called non-trivial(or)proper ideals of R.

Problem: Let R be a ring and a € R then show that aR={ax/x€R}is a right ideal

of R

Solution: Given that R is a ring and a € R also aR={ax/x€R}

Claim:aR is a right ideal of R.

Clearly, 0 € R

∴0 = a.0 € R

⇒0 € aR

⇒aR ≠ φ⊂R

i) Let x,y € R

⇒x=ap, y=aq for some p,q € R

Now, x-y = ap-aq

=a(p-q)

x-y=a.t where t=p-q €R

Here at€aR

⇒X-y € aR

ii) Let x € aR, k € R

Now xk = (ap)k

=a(pk)

xk = az where z=pk € R

Here az € R

⇒xk € R

∴aR is a right ideal of R.

Theorem: Let R be a commutative ring with unity. Suppose R has no non-trivial ideals then show that R is a field.

Proof: Given that R is a commutative ring with unity

Suppose that R has no non-trivial ideals.

⇒The any ideals of R are {0} and R itself.

Claim:R is a field

Let 0≠a€R

Then by known result,The set aR={ax/x€R} is an ideal in R.

Here a≠0€R ⇒aR ≠ {0}

By the hyothesis,we get aR=R.

Since 1€R

⇒1€aR

⇒ 1=ax for some x€R

⇒ax=1 for some x€R

⇒x€R is the multiplicative inverse of a in R.

∴every non-zero element in R has multiplicative inverse in R.

Hence R is a field.

Definitions:

i) Homomorphism: Let (R,R')be groups.Amappingφ: R→R'is calleda homomorphism. Ifφ(a).φ(b)=φ(ab),∀a,b€R.

ii) Monomorphism: Ifφ is one-one then φ is calledMonomorphism of R.

iii) Epimorphism: Ifφ is onto then φ is calledepimorphism of R.

Iv) Isomorphism: Ifφ is homomorphism andbijection then φ is calledisomorphism of R onto R'.

V)Endomorphism:A homomorphism of R intoitself is called anendomorphism of R.

Vi)Automorphism: An endomorphism of R which is both one-one&onto is calledan automorphism.

Vii)Kernelof Homomorphism: If f:R→S is a ring homomorphism then the kernel of f isdenoted by "kerf"(or)I(f)(or)f-1(0) and is defined askerf={x€R/f(x)=0'}

where 0'€S is the zeroelement.

State And Prove Fundamental Theorem Of Homomorphism:

Statement: let f be a homomorphism of a ring R into a ring Swith kernel then

R/N ≈Im(f).

Proof: let f:R→S is a ringhomomorphism

Let N=kerf

By known result,kerf is an ideal of R

⇒N is an ideal of R

⇒R/N={x+N/x€R} isa quotient ring

We know that,Im(f)={f(x)/x€R}

Claim: R/N ≈Im(f)

Define φ:R/N→Im(f) by φ(x+N)=f(x),∀x€R

φis well-defined&one-one:

Let x,y€R

⇒x+N,y+N€R/N

Let x+N=y+N

⇔x-y€N⇔X-y€kerf

⇔f(x-y)=0

⇔f(x)-f(y)=0

⇔f(x)=f(y)

⇔φ(x+N)=φ(y+N)

φ is onto: let T€Imf

⇒T=f(x) for some x€R

Since x€R

x+N € R/N

By def φ,φ(x+N)=f(x)=T

∴Every element in Imf haspre-element in R/N.

φ is a homomorphism: Let x,y€R

⇒x+N,y+N€R/N

i) φ[(x+N)+(y+N)]=φ[(x+y)+N]

=f(x+y)

= f(x)+f(y)

=φ(x+N)+φ(y+N)

ii)φ[(x+N).(y+N)]=φ[(xy)+N]

=f(xy)= f(x).f(y)

=φ(x+N).φ(y+N)

∴φ:R/N→Im(f) is anisomorphism.

∴∃an isomorphism φ fromR/N into Im(f).

∴R/N≈Imf.

Definitons:

Maximal Ideal: An ideal M≠R is said to be maximal in R if ∃an ideal U of R ∋M⊂U⊂R theneither U=M(or)U=R.

Co-Maximal: Two ideals A,B in any ring R are called co-maximal if A+B=R

Prime Ideal: An ideal P in a ring R is called a prime ideal if A,B are ideals in R such that $AB \subseteq P$ then $A \subseteq P$ (or) $B \subseteq P$.

Theorem: If R is a non-zero ring with unity 1 and I is an ideal in R $\ni I \neq R$, then $\exists$ a maximal ideal M of R $\ni I \subseteq M$.

Proof: Given that R is a non-zero ring with unity 1 & $I \neq R$ is an ideal of R.

Claim: $\exists$ a maximal ideal M of R $\ni I \subseteq M$.

Let $S=\{J/J$ is an ideal of R& $I \subseteq J$, $J \neq R\}$

Clearly, $(S, \subseteq)$ is a poset

Let C be a chain in S

Put $T=\cup_{k_i \in C} k_i$

First to prove that T is an ideal of R

Let $x,y \in T$ and $r \in R$

$x,y \in \cup_{k_i \in C} k_i$

$x \in k_i$, $y \in k_j$ for some $k_i,k_j \in C$

Since $k_i,k_j \in C$ and C is a chain in S.

$k_i \subseteq k_j$ (or) $k_j \subseteq k_i$

Assume that $k_i \subseteq k_j$

$\therefore x,y \in k_j$ and also $r \in R$, k_j is an ideal of R

$\Rightarrow x-y \in k_j$ and $xr,rx \in k_j$

$\Rightarrow x-y \in \cup_{k_i \in C} k_i$ and $xr,rx \cup_{k_i \in C} k_i$

$\Rightarrow x-y \in T$ and $xr,rx \in T$

$\Rightarrow$ T is an ideal of R also $k_i \subseteq \cup_{k_i \in C} k_i = T$

$\Rightarrow$ T is an ideal of R and $k_i \subseteq T$ for $k_i \in C$

$\Rightarrow$T is an upper bound of C

Next to prove that T€S:

i.e., to prove that T is an ideal of R and I$\subseteq$T, T$\neq$R.

Since k_i€C$\subset$S

$\Rightarrow k_i$€S

$\Rightarrow k_i$ is an ideal of R and I$\subseteq k_i, k_i \neq$R.

Since I$\subseteq k_i$

$\Rightarrow$I$\subseteq \cup_{ki \in C} k_i$

$\Rightarrow$ I$\subseteq$T

if T=R then 1€T

$\Rightarrow 1 \subseteq \cup_{ki \in C} k_i$

$\Rightarrow$1€ k_j for some k_i€C

$\Rightarrow k_j$=R

which is a contradiction to $k_j \neq$R

$\therefore$ T$\neq$R

$\therefore$ T€S

Every chain in S has an upper bound in S.

By Zorn's lemma S has a maximal element say M

i.e., M€S

i.e., M is an ideal of R and I$\subseteq$M, M$\neq$R

Finally, to prove that M is maximal in R.

Let N be an ideal of R $\ni$M$\subseteq$U$\subseteq$R.

To prove that N=M(or)N=R

Suppose that N≠M

Claim: N=R

Let N≠RN€S

N is a maximal in S

Which is a contradiction to M ismaximal in S

∴Our assumption N≠R is wrong

∴N=R

∴M is a maximal ideal of R such thatI⊆M

Hence, ∃ a maximal ideal M of R∋ I⊆M

Definition: An ideal A in a ring R is called Nilpotent if $A^n=(0)$ for some n € Z^+

Example:i)In the ring R=Z/(4), A={0,2} is Nilpotent ideal because $A^2=2.2=4=(0)$.

ii) Every zero ideal is a Nilpotent ideal.

Note: Every element in a Nilpotent ideal is a Nilpotent ideal.

Example: we know that A={0,2} is an Nilpotent ideal in a ring R=Z/(4).

Since 0,2 € A

0.1=0,2.2=4=0 in R

∴0,2 are Nilpotent elements.

Definition: An ideal A in a ring R is called a Nill ideal if each element of A is Nilpotent

Example:A={0,2} is a Nill ideal in a ring R=Z/(4).

Problem: Show that A & B are Nilpotent ideals there sum A+B is Nilpotent ideal.

Solution: Given that

Claim: A+B is Nilpotent ideal.

i.e., it is enough to show that $(A+B)^n=0$

$(A+B)^n=n_{c0}A^nB^0+n_{c1}A^{n-1}B^1+\text{---}+n_{cn}A^0B^n$

$=0+n_{c1}A^{n-1}B^1+\text{---}+n_{cn}A^0B^n$

$=nA^nA^{-1}B+\text{---}+n_{cn}A^0B^n$

$=0+0+\text{---}+0$

$=(0)$

$\therefore(A+B)^n=(0)$

$\therefore$ A+B is Nilpotent ideal.

Zorn's Lemma: A partially ordered set is a system of a non-empty set S & a relation Usually denoted by $\leq$ such that the following conditions are satisfied $\forall a,b,c \in S$

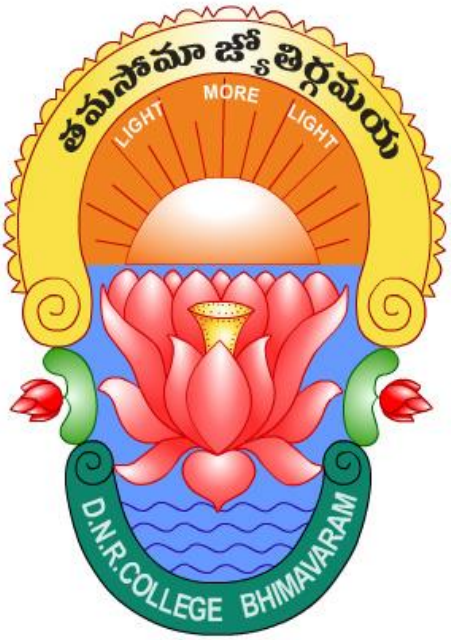
i) $a \leq b$ and $b \leq a \Rightarrow a=b$
ii) $a \leq a$
iii) $a \leq b$ and $b \leq c \Rightarrow a \leq c$

A chain C in a poset $(S,\leq)$is a subset of S for every $a,b \in C$ either $a \leq b$(or)$b \leq a$. An element $u \in S$ is an upper bound of C if $a \leq u$ for every $a \in C$,an element $m \in S$ is a maximal element of a poset $(S,\leq)$if $m \leq a$, $a \in S$ implies m=a.

DNR COLLEGE P.G COURSES (AUTONOMOUS)

(AFFILIATED TO ADIKAVI NANNAYA UNIVERSITY)

P.G DEPARTMENT OF MATHEMATICS



I M.Sc MATHEMATICS

ALGEBRA - 1

UNIT – 4

PREPARED BY:

M.SURYA SIRISHA

Assistant Professor

D.N.R College(A),

Bhimavaram.

Definition: A commutative integral domain R with unity is called UNIQUE FACTORIZATION DOMAIN if it satisfies the following conditions.

i) Every non-unit of R is a finite product of irreducible factors.
ii) Every irreducible element is prime.

Definition: A non zero element "a" of an integral domain R with unity is called an IRREDUCIBLE ELEMENT. If

i) a is not a unit,
ii) a=bc for b,c €R. ⇒ either b is a unit(or)c is a unit.

Definition: A non zero element P of an integral domain R with unity is called a "PRIME ELEMENT" if

i) P is not a unit
ii) if P/ab then P/a(or)P/b for a,b€R.

Principal Ideal Domain: A commutative integral domain R with unity is a principal ideal domain if each ideal in R is of the form (a)=aR, a€R.

Theorem: Every PID is a UFD.

Proof: let R be a PID

Every ideal in R is a P.I

Claim:R is a UFD

i.e., it is enough to show that

i) Every non-unit of R is a finite product of irreducible factors.

ii) Every irreducible element is prime.

Step:1) In this step to show that Every ascending chain of ideals of R is finite

In this step to show that Every ascending chain of ideals of R is finite.

Suppose that $I_1 \subset I_2 \subset I_3 \subset I_4 \subset$ --→ (1) be an ascending chain of ideals of R.

Let $I = U_{i=1} I_i$

I is an ideal of R: clearly, $I \neq \phi \subseteq R$

Let a,b€ I

$\Rightarrow a,b \in \cup I_i$

$\Rightarrow a,b \in I_i$

$\Rightarrow a-b \in I_i$ for some i

$\Rightarrow a-b \in \cup I_i$

$\Rightarrow a-b \in I$

Let $a \in I_i, b \in I_j$ for $i \neq j$

By (1), $I_i \subseteq I_j$(or) $Ij \subseteq Ii$

$\Rightarrow a,b \in I_i$

$\Rightarrow a-b \in I_i$

$\Rightarrow a-b \in \cup I_i = I$

ii) Let $a \in I$, $x \in R$

$\Rightarrow a \in I_i$ for some i, $x \in R$

$\Rightarrow ax, xa \in I_i$

$\Rightarrow ax, xa \in \cup I_i = I$

Clearly, $a \in <a> = I = \cup I_i$

$\therefore$I is an ideal of R

Since R is PID

Then $I = <a>$ for some $a \in R$

$\Rightarrow a \in I_i$ for some I

$\Rightarrow <a> \subseteq I_i$

$\therefore I = <a> \subset I_i \subset I_{i+1} \subset \cup I_n = I$

$\therefore I = I_i = I_{i+1}$ -----

$\therefore$chain (1) is finite.

STEP:2) To prove that each element $a \in R$ is a product of finite number of irreducible elements

If a is irreducible then it is clear

Let a=bc,

Where neither b nor c is not a unit. If both b &c are product of irreducible elements then the result is true

Suppose that b cannot be written as product of irreducible elements

Let b=xy where neither x nor y is not a unit.

If both x & y are product of irreducible elements then the result is true.

If not,continuing the above process finally we get an ascending chain of ideals of R

i.e., <a>⊂<b>------

This chain is not stationary

Which is contradiction to step(1)

If both b &c are product of irreducible elements. Each element a€R is a product of finite number of irreducible elements.

Step:3) Finally to prove that every irreducible element is prime.

Let a€R be an irreducible element

Since R is a PID then by known result a is prime.

By step(1),step(2) & step(3)

we conclude that R is a UFD.

Definitions:

Principal Ideal Domain: A commutative integral domain R with unity is a principal ideal domain if each ideal in R is of the form (a)=aR, a€R.

Eucliden Domain: A commutative integral domain R with unity is A Euclidean domain if∃ a function φ: R→Z is satisfying the following conditions:

i) If a,b € R*=R-{0} and b/a, then φ(b)≤φ(a)
ii) For all a,b€R,b≠0,∃q,r€E ∋a=bq+r with φ(r)≤φ(b)

Example: i) Every field is a Euclidean domain

ii) The ring of integers Z is a Euclidean domain if $\varphi(n)=|n|$, $n \in Z$.

Theorem: Every Euclidean domain is a PID.

Proof: let R be Euclidean domain $\exists$ a function $\varphi: R \to Z$ is Satisfying the following conditions:

i) If $a, b \in R^*=R-\{0\}$ and b/a, then $\varphi(b) \leq \varphi(a)$
ii) For all $a,b \in R, b \neq 0, \exists q,r \in E \ni a=bq+r$ with $\varphi(r)<\varphi(b)$

Claim: R is a PID.

Let $I \neq (0)$ be an ideal in R

$\Rightarrow \exists x \in I \ni x \neq 0$

Now we have $1/x \ \forall x \neq 0 \in I$

$\Rightarrow \varphi(1) \leq \varphi(x) \ \forall x \neq 0 \in I$

Define $\varphi(I)=\{\varphi(x)/x \neq 0 \in I\}$

Clearly, $\varphi(1)$ is a lower bound of $\varphi(I)$

Clearly, $\varphi(I) \neq \varphi \subseteq Z+$

$\varphi(I)$ has a least element

$\Rightarrow \exists \ d \in I \ni \varphi(d)$ is least element in $\varphi(I)$

Claim: $I=<d>$

Clearly, $<d> \subset I$

To prove that $I \subset <d>$

Let $a \in I \subset R$, also $d0I \subset R$

By division algorithm in R,

$q, r \in R \ni a=dq+r$ ----(1) with $\varphi(r)<\varphi(d)$

If $r \neq 0 \in R$ Then $r=a-dq \in I$

$\Rightarrow r \in I$

$\Rightarrow \varphi(r) \in \varphi(I)$ also $\varphi(r)<\varphi(d)$

$\Rightarrow \varphi(r)$ is the least element in $\varphi(I)$

Which is contradiction to φ(d) is the least element in φ(I)

∴ r=0

From (1) a=dq €<d>

⇒I⊂<d>

∴I=<d> is a PI in R

∴Every ideal in R is a PI

∴R is a PID

Hence every Euclidean domain has a PID.

Definitions:

Eucliden Domain: A commutative integral domain R with unity is A Euclidean domain if ∃a function φ:R→Z is Satisfying the following conditions:

i) If a, b € R*=R-{0} and b/a, then φ(b)≤φ(a)
ii) For all a,b€R,b≠0,∃q,r€E ∋ a=bq+r with φ(r)≤φ(b)

Example: i) Every field is a Euclidean domain

ii) The ring of integers Z is a Euclidean domain if φ(n)=|n|, n€Z.

Principal Ideal Domain: A commutative integral domain R with unity is a principal ideal domain if each ideal in R is of the form (a)=aR, a€R.

Definition: A commutative integral domain R with unity is called "Unique Factorization Domain" if it satisfies the following conditions.

i) Every non-unit of R is a finite product of irreducible factors.
ii) Every irreducible element is prime.

Theorem: Every Euclidean domain is a UFD.

Proof: PART:1) Let R be Euclidean domain∃ a function ϕ:R→Z is Satisfying the following conditions:

i) If a, b € R*=R-{0} and b/a, then ϕ(b)≤ϕ(a)
ii) For all a,b€R,b≠0,∃q,r€E ∋ a=bq+r with ϕ(r)<ϕ(b)

Claim: R is a PID.

Let I≠(0) be an ideal in R

⇒∃x€I∋x≠0

Now we have 1/x ∀x≠0€I ϕ(1)≤ϕ(x) ∀x≠0€I

Define ϕ(I)={ϕ(x)/x≠0€I}

Clearly, ϕ(1) is a lower bound of ϕ(I)

Clearly, ϕ(I)≠ϕ ⊆ Z^+

ϕ(I) has a least element

⇒∃ d€I ∋ϕ(d) is least element in ϕ(I)

Claim: I=<d>

Clearly, <d>⊂I

To prove that I⊂<d>

Let a€I ⊂R, also d≠0€I⊂R

By division algorithm in R,

q, r €R ∋ a=dq+r ----(1) with ϕ(r)<ϕ(d)

If r≠0€R then r=a-dq€I

⇒r€I

⇒ϕ(r) €ϕ(I) also ϕ(r)<ϕ(d)

⇒ϕ(r) is the least element in ϕ(I)

Which is contradiction to ϕ(d) is the least element in ϕ(I)

∴ r=0

From (1) a=dq€<d>

⇒I⊂<d>

∴I=<d> is a PI in R

∴Every ideal in R is a PI

∴R is a PID

Hence every Euclidean domain has a PID.

Part:2) Let R be a PID

Every ideal in R is a P.I

Claim: R is a UFD

i.e., it is enough to show that every non-unit of R is a finite product of irreducible factors.

Every irreducible element is prime.

STEP:1) In this step to show that Every ascending chain of ideals of R is finite.

Suppose that $I_1 \subset I_2 \subset I_3 \subset I_4 \subset$ --→ (1) be an ascending chain of ideals of R.

Let $I=\cup_{i=1} I_i$

I is an ideal of R: clearly, $I \neq \phi \subseteq R$

Let a,b€ I

⇒a,b€$\cup I_i$

⇒a,b€I_i

⇒a-b€I_i for some i

⇒a-b€$\cup I_i$

⇒a-b€I

Let a€I_i,b€I_j for i≠j

By (1), $I_i \subseteq I_j$(or) Ij⊆Ii

⇒a,b€I_i

⇒a-b€ I_i

⇒a-b€$\cup$ I_i =I

ii) Let a€I, x€R

⇒a€ I_i for some i, x €R

$\Rightarrow ax, xa \in I_i$

$\Rightarrow ax, xa \in \cup I_i = I$

Clearly, $a \in \langle a \rangle = I = \cup I_i$

$\therefore$I is an ideal of R

Since R is PID

Then $I = \langle a \rangle$ for some $a \in R$

$\Rightarrow a \in I_i$ for some I

$\Rightarrow \langle a \rangle \subseteq I_i$

$\therefore I = \langle a \rangle \subset I_i \subset_{I_{i+1}} \subset \cup_{I_n} = I$

$\therefore I = I_i = I_{i+1}$ -----

$\therefore$chain (1) is finite.

STEP:2) To prove that each element a€R is a product of finite number of irreducible elements

If a is irreducible then it is clear

Let a=bc,

Where neither b nor c is not a unit. If both b &c are product of irreducible elements then the result is true

Suppose that b cannot be written as product of irreducible elements

Let b=xy where neither x nor y is not a unit.

If both x & y are product of irreducible elements then the result is true.

If not,continuing the above process finally we get an ascending chain of ideals of R

i.e., $\langle a \rangle \subset \langle b \rangle$------

This chain is not stationary

Which is contradiction to step(1)

If both b &c are product of irreducible elements. Each element a€R is a product of finite number of irreducible elements.

Step:3) Finally to prove that every irreducible element is prime.

Let a€R be an irreducible element

Since R is a PID then by known result a is prime.

By step(1),step(2) & step(3)

we conclude that R is a UFD.

By part(1) & part(2) ,

Every Euclidean domain is a UFD.

Definitions: Content Of A Polynomial:

Let $f(x)=a_0+a_1x+a_2x^2+---+a_nx^n$ be a polynomial over a UFD in R.

Then the content of f(x) is denoted by c(f) and is defined as $c(f)=(a_0,a_1,---,a_n)$.

Example: $f(x)=2x^2-4x+8=0$

$\therefore C(f)=(2,-4,8)=2$.

Primitive Polynomial:

Let $f(x)= a_0+a_1x+a_2x^2+---+a_nx^n$ be a polynomial over a UFD in R.

f(x) is said to be primitive if c(f)=1 (or) a unit.

i.e., $(a_0,a_1,---,a_n)=1$.

Example: $f(x)=3x^2-5x+7$

Here,(3,-5,7)=1

$\therefore$f(x) is primitive.

Note: let R be a UFD. Every non-zero f(x) of R[x] can be written as $f(x)=g.f_1(x)$ where g=c(f) and $f_1(x)$ is primitive.

Example: $f(x)=x^2+1$€R[x]

c(f)=1=g

$\therefore f(x)=g.f(x)$

Theorem: If R is a UFD then the product of two primitive Polynomials in R[x] is again a primitive polynomial in R[x].

Proof: let $f(x)= a_0+a_1x+a_2x^2+---+a_mx^m$

$g(x)= b_0+b_1x+b_2x^2+---+ab_nx^n$ be two primitive polynomials in R[x]

Let $h(x)=f(x)g(x)$

$=c_o+c_1x+---+c_{m+n}x^{m+n}$

Claim: h(x) is primitive.

If possible suppose that h(x) is not primitive in R[x].

$\Rightarrow \exists$a prime element of R $\ni p/c_i \ \forall i$

Since f(x) is primitive then $p\nmid a_i$ where a_i is the first coefficient of f(x).

Since g(x) is primitive then $p\nmid b_j$ where b_j is the first coefficient of g(x).

Let c_{i+j} = the coefficient of x_{i+j} of h(x).

$=a_ib_j+(a_{i-1}b_{j+1}+a_{i-2}b_{j+2}+---a_0b_{j+i}) +(a_{i+1}b_{j-1}+a_{i+2}b_{j-2}+---+a_{i+j}b_0)$

$\Rightarrow a_ib_j =c_{i+j}-\{(a_{i-1}b_{j+1}+a_{i-2}b_{j+2}+---a_0b_{j+i})+(a_{i+1}b_{j-1}+a_{i+2}b_{j-2}+---+a_{i+j}b_0)\}\rightarrow(1)$

Since $p/a_0,p/a_1,p/a_2,---p/a_{n-1}$

Then $p/ a_{i-1}b_{j+1}+a_{i-2}b_{j+2}+---a_0b_{j+i}$

Since $p/b_{j-1},p/b_{j-2},---p/b_0$

Then $p/ a_{i+1}b_{j-1}+a_{i+2}b_{j-2}+---+a_{i+j}b_0$also p/c_{i+j}

from (1), we get

P/RHS of (1)

$\Rightarrow p/a_ib_j$

$\Rightarrow p/a_i$ (or) p/bj

Which is contradiction to $p\nmid a_i$ and $p\nmid b_j$

$\therefore$Our assumption h(x) is not primitive is wrongh(x) is primitive.

Hence the product of two primitive polynomials in R[x] is primitive.