Dr. A.S.A

ALGEBRAIC STRUCTURE

PART - A

1. Find Inverse is unique in G.

Let a' and a'' be the inverse of a

ie, $aa' = a'a = e$ ——— (1)

$aa'' = a''a = e$ ——— (2)

$a' = a'e$

$= a'(aa'')$

$= (a'a)a''$

$= ea''$

$= a''$

∴ Hence inverse element is unique.

2. Define Cyclic group with example.

In a group $(G, \cdot)$ iff every element is of the form $a^n (n \in Z)$, then $(G, \cdot)$ is called cyclic group generator by "a" and is denoted by $<a>$ is defined as $<a> = \{a^n / n \in z\}$. eg:- $g = \{1, -1, i, -i\}$

3. Define normal subgroup.

A sub group N of G is a normal subgroup of G iff $gNg^{-1} = N$ for all $g \in G$.

4. Define Automorphism.

Let $f : G \rightarrow G$ be a automorphism

if $f(ab) = f(a) f(b)$

5. Define permutation group.

Let S is a finite set having n elements $x_1, x_2, \dots x_n$. If $\phi \in A(S) = S_n$, then ϕ is a one-to-one mapping of S onto itself, and we could write ϕ out by showing what it does to every element eg.: $\phi : x_1 \rightarrow x_2$, $x_2 \rightarrow x_4$, $x_4 \rightarrow x_3$, $x_3 \rightarrow x_1$.

6. Write a example for permutation groups.

Let $S = \{1, 2, 3\}$.

Define $\sigma : S \rightarrow S$ by $\sigma(1) = 2$, $\sigma(2) = 1$, $\sigma(3) = 3$

$$\therefore \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

7. Define ring.

A non-empty sets R together with two binary operations denoted by "+" and "." which the following axioms are satisfied

* $(R, +)$ is abelian group
* $(R, \cdot)$ is an associative binary operation with R.
* $a \cdot (b+c) = a \cdot b + a \cdot c$
  $(a+b) \cdot c = a \cdot c + b \cdot c$ for $a, b, c \in R$

8. Define maximal ideal.

Let R be ring an ideal $M \neq R$ is said to be a maximal ideal of R. if where even u is ideal of R. Show that $M \subseteq U \subseteq R$ then either $u = m$ or $u = R$

9. Define ~~Commutative~~. Divisibility.

if $a \neq 0$ and b are in commutative ring R. Then a is divide b if $\exists$ an element $c \in R$. Such that $b = ac$.

10. Define greatest common divisor.

if $a, b \in R$ then $d \in R$ is said to be greatest common divisor of a, and b is

* d/a and d/b
* Whenever c/a and c/b then c/d

Part - B.

1). State and Prove lagrange's Theorem:

Statement:

If H is a Subgroup of finite group G then $o(H)$ divides $o(G)$.

Proof:

Let G has finite group with order m.

(ie) G has m elements → (1)

let H has a Subgroup of G with order n.

(ie) H has n elements → (2)

We know that,

Each left coset of H or each right coset of H has "n" elements → (3)

we know that,

Union of K disjoint left cosed of H or Union of K disjoint right cosed of H.

∴ G has nk elements → (4)

∵ Each has n element and K cosets has nk elements.

From (1) = (4)

$$n = mK$$

$$\boxed{n/m = K}$$

$o(H)$ divides $o(G)$

Hence it's Proved.

2). If H and K are finite subgroup of G of orders $o(H)$ and $o(K)$ then,

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

Proof:

let $L = H \cap K$

Since H and K are subgroup of G let L be a subgroup of G and $L \subseteq H$ and K.

let $Lx_1, Lx_2, Lx_3 \ldots Lx_m$ be the distinct right cosets of link.

So that

$$K = Lx_1 \cup Lx_2 \cup \ldots \cup Lx_m \rightarrow (1)$$

and
$$m = [K : L]$$
$$= \frac{o(K)}{o(L)}$$
$$= \frac{o(K)}{o(H \cap K)} \rightarrow (2)$$

$(1) \Rightarrow HK = HLx_1 \cup HLx_2 \ldots \cup HLx_m$

$= Hx_1 \cup Hx_2 \ldots Hx_m$ Since $L \subseteq H$

we claim $Hx_1, Hx_2 \ldots Hx_m$ are distinct.

Suppose $Hx_i = Hx_j$

$\therefore x_i x_j^{-1} \in H$

Also $x_i x_j \leftarrow K$

Hence $x_i x_j^{-1} \in K$

$\therefore x_i x_j^{-1} \in H \cap K = L$

Hence $Lx_i = Lx_j$

$\Rightarrow \Leftarrow$

Since the co.sets $Lx_1, Lx_2 \ldots Lx_n$ are distinct.

(3) we have

$$O(HK) = o(Hx_1) + o(Hx_2) + \ldots o(Hx_m)$$
$$= m\,o(H)$$

by (2)

$$o(HK) = \frac{o(H)\,o(K)}{o(H \cap K)} \quad //$$

---

3). A subgroup N of G is normal of G if and only if the product of two left cosets of N in G is again a left coset of N in G.

Proof:

let N is normal of G

for $a, b \in G$

$$(aN)(bN) = a(Nb)N$$
$$= a(bN)N$$
$$= abN \quad (\text{since } N \text{ is normal})$$
$$(\because NN = N)$$

The product of two left cosets of N is again a left coset of N.

Conversly:

Suppose product of two left cosets of N again a left coset of N for $g \in G$ gN and gN^{-1} cosets.

Their product $(gN)(gN^{-1})$ must left cosets.

Since $e = (ge)(g^{-1}e) \in (g \in N)(gN^{-1})$

but $N = eN$

Thus, $(gN)(g^{-1}N) = eN$

$= N$

$(gn)(g^{-1}n_1) \in N \quad , \forall n, n_1 \in N$

$(gng^{-1})n_1 \in N$

$(gng^{-1})n_1 n_1^{-1} \in N n_1^{-1}$

$(gng^{-1}) \in N$

Hence N is normal subgroup of G.

4). State and prove fundamental of homomorphism (or) Basic theorem of homomorphism.

<u>Statement:</u>

let f be a homomorphism of G onto G' with Kernel K. Then $G/K \cong G'$

(or)

let f be a epimorphism with kernel K then G/K isomorphism to G'

Proof:

Define $\phi = G/K \to G'$ by $\phi(Ka) \neq a$

Step 1:

ϕ is well defined

let $Kb = Ka$

Then $b \in Ka$

Hence $b = ka$, $k \in K$

Now, $f(b) = f(ka)$

$= f(k) + a$

$= e' f(a)$

$= f(a)$

$\phi(Kb) = f(b) \Rightarrow f(a)$

$= \phi(K(a))$

Hence $\phi(Ka) = \phi(Kb)$

Step 2:

ϕ is 1-1

for $\phi(Ka) = \phi(Kb)$

$f(a) = f(b)$

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

$ab^{-1} \in K$

$a \in Kb$

$Ka \in Kb$

Step 3:

ϕ is onto

let $a' \in G'$

Since f is onto

there exist $a \in G$

Such that $f(a) = a'$

Hence $\phi(Ka) = f(a)$
$= a'$.

Step 4:

ϕ is homomorphism

$$\phi(Ka\,Kb) = \phi(Kab)$$
$$= f(ab)$$
$$= f(a)f(b)$$
$$= \phi(Ka)\,\phi(Kb)$$

Thus ϕ is an homomorphism.
from G/K onto G'

$\therefore G/K \cong G'$.

---

5) For $n > 1$, the set A_n of all even permutation in S_n is a subgroup of S_n. Also the order of A_n is $\lfloor n/2$.

Proof:

let A_n = Set of all even permutation in S_n.

The identity permutation I is even and so $I \in A_n$ $\therefore A_n \neq \phi$.

let $\sigma, \tau \in A_n \Rightarrow \sigma$ and τ are even permutations.

$\Rightarrow \sigma$ and τ^{-1} are even permutations.

$\Rightarrow \sigma\tau^{-1}$ is an permutation.

$\therefore \sigma\tau^{-1} \in A_n$

$\therefore A_n$ is subgroup of S_n.

let $S = \{1, 2 \ldots n\}$ and let B_n = set of all odd permutation in S_n.

$\tau : A_n \to B_n$ by $\tau(\sigma) = (1,2)\sigma \ \forall \sigma \in A_n$.

(* We observe that σ is even, $(1,2)$ is odd $\therefore (1,2)\sigma$ is odd)

we prove τ is bijective.

Now, $\tau(\sigma_1) = \tau(\sigma_2)$

$$= (1\ 2)\sigma_1 = (1\ 2)\sigma_2$$

$\sigma_1 = \sigma_2$ by cancellation law in group S_n. $\therefore \tau$ is one to one.

If $\psi \in B_n$ then $(1\ 2)\psi$ being an even permutation belongs to A_n and

$$\tau((1,2)\psi) = (1\ 2)(1\ 2)\psi = \psi$$

$\therefore \tau$ is onto. Thus τ is bijection

$\therefore A_n$ and B_n have the same number of elements. But S_n has $\lfloor n$ elements.

$\therefore A_n$ has $\frac{n!}{2}$ elements $(n > 1)$

Remark :

Since A_n is a subgroup of S_n of order $\lfloor n/2$ the index of A_n in

$$S_n = [S_n : A_n] = \frac{O(S_n)}{O(A_n)} \Rightarrow \frac{\lfloor n}{\lfloor n} = 2$$

But any subgroup of index 2 in a group G is normal in G. $\therefore A_n$ is normal in S_n.

6). Let G be a group $\{1,-1\}$ under multiplication show that for $n>1$, then map $\sigma : S_n \to G$ defined by,

$$\sigma(\theta) = \begin{cases} 1 & \text{if } \theta \text{ is an even permutation} \\ -1 & \text{if } \theta \text{ is an odd permutation} \end{cases}$$

is a homomorphism of S_n onto G. What is the kernel of σ?

Proof:

let $p, q \in S_n$

(i) when p, q are both even permutations pq is an even permutation.

$\therefore \sigma(pq) = 1$. Also $\sigma(p) = 1$, $\sigma(q) = 1$

$\therefore \sigma(pq) = \sigma(p)\sigma(q)$

(ii) when p, q are both odd pq is even.

$\therefore \sigma(pq) = 1$. Also $\sigma(p) = -1$, $\sigma(q) = -1$

$\therefore \sigma(pq) = \sigma(p)\sigma(q)$

(iii) Suppose only one of p, q is even; say p is even and q is odd. Then pq is odd.

$\therefore \sigma(pq) = -1$,

Also, $\sigma(p) = 1$, $\sigma(q) = -1$

$\therefore \sigma(pq) = \sigma(p)\sigma(q)$

Thus, $\sigma(pq) = \sigma(p)\sigma(q)$ $\forall p, q \in S_n$ and σ is a homomorphism.

To prove σ is onto we note that for $n>1$, S contains more than one element and S_n has an odd permutation, for e.g $(1,2)$;

S_n also contains an even permutation, namely the identity permutation I;
Also $\sigma(I)=1$, $\sigma(1,2)=-1$.

$\therefore$ σ is onto.

$$\ker \sigma = \{\theta \in S_n \mid \sigma(\theta) = \text{identity of } G\}$$
$$= \{\theta \in S_n \mid \sigma(\theta) = 1\}$$
$$= \{\theta \in S_n \mid \theta \text{ is even}\}$$
$$= A_n.$$

7). Any finite integral domain is a field.

Proof:

let R be a finite integral domain.
To prove that every non zero element in R has multiplicative inverse.

let $a \in R$ and $a \neq 0$
let $R = \{0, 1, a_1, a_2, \ldots a_n\}$

Consider $\{a1, aa_1, aa_2, \ldots aa_n\}$

By theorem,

All these elements are non-zero and all use elements are distinct.

Hence $aa_1 = 1$ for $a \in R$

Since R is commutative

$$aa_1 = a_1 a = 1$$

So that $a_1 = a^{-1}$ hence R is field.

8). let R be a commutative ring with identity. An ideal m of R is maximal if and only if R/m is ideal.

Proof:

Since R is commutative ring with identity and $m \neq R$. Then R/m is also commutative ring with identity.

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

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

$\therefore$ U is an ideal of R.

let $m \in M$ then $m = 0a + m \in U$

$\therefore$ $M \subseteq U$

$\therefore$ U is an ideal of R.

But m is maximal ideal

$U = R$

Hence $I \in U$

$\therefore$ $I = ba + M$, for $b \in M$

Now, $M + I = M + ba + M$

$$= M + ba$$

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

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

Thus, every non-zero element R/m has inverse.

Hence R/m is a field.

---

9). let R be an Euclidean ring. let a and ~~be~~ ~~to~~ b be two non empty element of R.

Then,

(1). b is not a unit R $(b \neq 0) \Rightarrow d(a) < d(ab)$

(2). b is a unit R $\Rightarrow d(a) = d(ab)$

Proof:

Suppose b is not a unit R.

by definition,

Euclidean domain $\exists$ an element q, $r \in R$. Show that $a = q(ab) + r \rightarrow (1)$

either $r = 0$ (or) $d(r) < d(ab)$

Suppose $r = 0$ then $a = q(ab)$ by (1)

$\therefore \quad a - q(ab) = 0$

$a(1 - qb) = 0$

Now R has no zero division and $a \neq 0$

$\therefore \quad 1 - qb = 0$

$qb = 1$

$\therefore$ b is unit in R

which is $\Rightarrow \Leftarrow$

$\therefore r \neq 0$. Hence $d(r) < d(ab) \rightarrow (1)$

Now (1) $\Rightarrow$ $r = a(1 - qb)$

$\therefore d(r) = d(a - qb) \geq d(a) \rightarrow (3)$

$d(a) \leq d(r) < d(ab)$ by (2) & (3)

$\therefore \quad d(a) < d(ab)$ //.

---

10). Let R be a Euclidean domain. Let $a, b, c \in R$. Then a / bc and $(a, b) = 1 \Rightarrow a / c$

Proof:

Since $(a,b)=1$

$\exists\ x, y \in R$

Show that $ax+by=1$

$\therefore acx+bcy=K$

Now a/acx.

Also $a/bc \Rightarrow a/bcy$

$\therefore a\,(acx+bcy)$

Hence a/c.

Part - C

D. let A and B be two subgroup of G. Then AB is subgroup of G. if and only if $AB=BA$.

Proof :

let AB is a subgroup of G

To prove,

$$AB=BA$$

let $x \in AB$

(ie) $x^{-1} \in AB$

let $x^{-1}=ab$ where $a\in A$, $b \in B$

(ie) $x=(ab)^{-1}$

$\quad = b^{-1}a^{-1}$

Since A and B subgroup of G

(ie) $b^{-1}\in B$, $a^{-1}\in A$

$\therefore x \in BA$

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

let $x \in BA$

(ie) $x = ba$

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

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

Since A and B are subgroup of G.

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

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

we write $x \in AB$

Hence $BA \subseteq AB$ $\rightarrow$ (2)

From (1) & (2)

$AB = BA$.

Converse:

let $AB = BA$

we claim AB is subgroup of G

Now $e \in AB$ and $AB \neq 0$

let $x, y \in AB$

let $x = a_1 b_1$ and $y = a_2 b_2$

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

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

Now $b_2^{-1} a_2^{-1} \in BA$

Since $AB = BA$

(ie) $b_2^{-1} a_2^{-1} \in AB$

(ie) $b_2^{-1} a_2^{-1} = a_3 b_3$

where $a_3 \in A$, $b_3 \in B$

Since $b_1 a_3 \in BA$

Since $BA = AB$

(ie) $b_1 a_3 \in AB$

$b_1 a_3 = a_4 b_4$ where $a_4 \in A$, $b \in B$

(ie) $xy^{-1} = a_1 b_1 a_4 b_4 \leftarrow AB$

(ie) AB is a subgroup of G.

2). let G be a group A(G) be an automorphi-sm of G is also a group.

Proof:

let $T_1 T_2 \in A(G)$

we define,

$(T_1 T_2) = (aT_1) T_2 \rightarrow (1)$

So that $a(T_1 T_2) \in G$

we shall show that $T_1 T_2$ injective

Suppose $a(T_1 T_2) = b(T_1 T_2)$

$a(T_1) T_2 = b(T_1) T_2$

$aT_1 = bT_1$, $b \in z$, T_2 injective

$a = b$, $b \in z$, T_1 injective

$T_1 T_2$ is injective $\rightarrow (2)$

let $c \in G$

Since T_n injective.

$\exists$ $b \in G$ show that $bT_2 = E$

But T_2 is a surjective.

Hence $\exists$ an element $a \in G$

show that $aT_1 = b$

Similarly $TT^{-1} = I$

Thus inverses $T = T^{-1}$

Hence $A(G)$ is group.

let $c \in G$

Since T_2 injective

$\exists$ $b \in G$ show that $bT_2 = c$

But T_2 also surjective

Hence $\exists$ an element $a \in G$

Show that $aT_1 = b$

Thus $a(T_1 T_2) = c$

This show that $T_1 T_2$ surjective.

---

3). **Cauchy's Theorem**

Statement:

Any finite group is isomorphic to a group permutation.

(or)

Every group is isomorphism to a subgroup of $A(S)$ for some S.

Proof:

To find three steps.

First to find a set G' of permutation.

Then we find G' is a group of permutation, and finally an isomorphism.

$\phi \to G - G'$

Step 1:

let G be a finite group of order n.

Thus $a(T_1T_2) = c$

This shows that T_1T_2 surjective $\rightarrow$ (3)

From (1) & (2)

T_1T_2 is bijective form

Hence $T_1T_2 \in G$

Thus $A(G)$ possesses closure.

let $T_1T_2T_3 \in A(G)$ for $a \in G$

we have $a[(T_1T_2), T_3] = [a(T_1T_2)]T_3$

$= ((a_{ij})T_2)T_3$

$= a(T_1(T_2T_3))$

(ie) $(T_1T_3)T_2 = T_1(T_2T_3)$

The associative of $A(G)$

let I be identity

(ie) $aI = a \quad \forall a \in G$

$a(IT) = (aI)T$

$a = T \quad \forall a \in G$

$\Rightarrow IT = T$

Similarly $TI = T$

Hence I is an identity of $A(G)$

Define $bT^{-1} = a$

$\Leftrightarrow aT = b$

But $b(T^{-1}T) = (bT^{-1})T$

$= aT$

$= b \quad \forall b \in G$

Hence $T^{-1}T = I$

let $a \in G$

Define $f_a : G \to G$ by

$f_a(x) = ax$

Now, f_a is 1-1

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

$ax = ay$

$x = y$

f_a is on to

If $y \in G$ then,

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

$= aa^{-1}y$

$= y$

Thus f_a is bijection

Since G has n element.

f_a just a permutation on A

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

Step 2:

G' be group

let $f_a f_b \in G'$

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

$= f_a(bx)$

$= a(bx)$

$= (ab)x$

$= f_{ab} x.$

Hence $f_a \circ f_b = f_{ab}$

Hence G' closed under composition.

$f_e \in G'$ is identity

Inverse of f_a in G' is f_a^{-1}

Thus G' is group.

Step 3:

To prove $G \cong G'$

Define $\phi : G \to G'$

by $\phi(a) = f_a$

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

$$f_a = f_b$$

$$f_a(x) = f_b(x)$$

$$ax = bx$$

$$a = b$$

Hence ϕ is 1-1

Clearly onto

Also,

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

Hence ϕ is an isomorphism.

---

4). Every integral domain can be embedded in a field.

Proof:

stage 1:

let D be an integral domain. let $S = \{(a,b) / a,b \in D$ and $b \neq 0\}$ the ordered pair (a,b) and (c,d) as are representing a fractional quotient.

lemma 1:

$\sim$ equivalent relation in S

Proof:

let $(a,b) \in S$

$(a,b) \sim (a,b)$ since $ab = ba = ab$

Hence $\sim$ is reflexive

Now,

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

$cd = da \Rightarrow (c,d) \sim (a,b)$

Hence $\sim$ is symmetric.

Now, let $(a,b) \sim (c,d)$ and $(c,d) \sim (e,f)$

To prove $(a,b) \sim (e,f)$. must prove that $af = be$.

case i:

let $c = 0$

Now, $ab = bc$ and $cf = de$ $\therefore ad = 0$ and $de = 0$

But $d \neq 0$. Hence $a = 0$, $de = 0$.

$\therefore af = be = 0$

case ii:

let $c \neq 0$

we have $ad = be$ & $cf = de$

$\therefore adcf = bcde$

$\therefore af = be$

$\therefore \sim$ transitive

consider the equivalance class containing (a,b)

stage ii:

let $a/b, c/d \in F$

we define $a/b + c/d = \frac{ad+bc}{bd}$ and

$a/b \cdot c/d = ac/bd$

Since D is an integral domain and $b,d \neq 0$ we have $bd \neq 0$.

$\therefore$ $ad+bc/bd$ and $ac/bd \in F$

lemma 2:

Addition and multiplication defined as ae well defined.

Proof:

let $(a_1 b_1) \in a/b$ and $(c_1, d_1) \in c/d$.

$\therefore$ $a_1 b = b_1 a$ and $c_1 b = d_1 c$ $\rightarrow$ (1)

$\therefore$ $a_1 b d d_1 = b_1 a d d_1$ and $c d b b_1 = d_1 c b b_1$

$\therefore$ $(a_1 d_1 + b_1 c_1) bd = (ad+bc) b_1 d_1$

$$\therefore \quad \frac{ad+bc}{bd} = \frac{a_1 d_1 + b_1 c_1}{b_1 d_1}$$

$$\therefore \quad \frac{a_1 d_1}{b_1 d_1} + \frac{b_1 c_1}{b_1 d_1} = \frac{ad}{bd} + \frac{bc}{bd}$$

$\therefore$ $a/b + c/d = a_1/b_1 + c_1/d_1$

$\therefore$ Addition is well defined.

lemma 3:

Stage 3:

F is a field with addition and multiplication defined.

Proof:

Now $0/I$ is zero of F and $-a/b$ is the addition inverse of a/b $\therefore (F, +)$

Then $1/I$ is the identity of F

If a/b is non-zero of F then $a \neq 0$.

$\therefore$ $b/a \in F$ and inverse of a/b

Now $a/b\,(c/d + e/f) = a/b\,(cf + de/df)$

$= acf + ade / bdf$

$$= \frac{acfb + adeb}{bdfb}$$

$$= \frac{a}{b} \cdot \frac{c}{d} + \frac{a}{b} \cdot \frac{e}{f} \Rightarrow ac/bd + ac/bf$$

$\therefore$ F is a field.

Stage 4:

The field F contains a subring R which is isomorphic D.

lemma 4:

The map $f : D \to F$ given by $f(a) = a/I$ is an isomorphism of D onto $f(D)$.

Proof:

let $a, b \in D$

Then $f(a+b) = a+b/I$

$= a/I + b/I$

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

and $f(ab) = \frac{ab}{I} = \frac{a}{I} \cdot b/I \Rightarrow f(a) f(b)$.

Also f is 1-1

for $f(a) = f(b)$

$a/I = b/I$

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

$\Rightarrow (aI) = bI$

$a = b$

f is an isomorphism.

5). Unique Factorization Theorem.

Statement:

let R be a Euclidean ring and $a \neq 0$ a unit in R suppose that $a = \pi_1 \pi_2 \cdots \pi_n = \pi_1' \pi_2' \cdots \pi_m'$ where π_i, π_i' are prime. Then $n = m$ and conversely each π_1' is an associate of π.

Proof:

The relation $a = \pi_1 \pi_2 \cdots \pi_n = \pi_1' \pi_2' \cdots \pi_n'$

But $\pi_1 / \pi_1, \pi_2 \cdots \pi_n$

hence $\pi_1 / \pi_1', \pi_2' \cdots \pi_m'$

By lemma,

π_1 / π_1' Since π_1 and π_1' ~~are~~ both prime and they must be associate and

$\pi_1' = u\pi_1$ where u, unit in R

Thus $\pi_1, \pi_2 \cdots \pi_n = \pi_1', \pi_2' \cdots \pi_m'$

$= u\pi_1 \pi_2' \cdots \pi_m'$

Then cancel of π_1 and $\pi_2, \pi_3 \cdots \pi_n = u\pi_2' \cdots \pi_m'$

Repeat the argument with n step.

(ie) $n \leq m$

Similarly $m \leq n$

Hence $n = m$

(ie) Every π_i has some π_i' are associate.

Conversely:

By theorem, Every non zero element of Euclidean ring can be uniqely as a product at prime or unit element in R.