

1000



R279

Directorate of Distance Education

**M
A
T
H
E
M
A
T
I
C
S**

M.Sc. - I Year

Paper - I

ALGEBRA

**MADURAI KAMARAJ UNIVERSITY
MADURAI - 625 021.**

All copyright privileges are reserved

1000

R279



Directorate of Distance Education

Year

Paper - I

ALGEBRA

M
A
T
H
E
M
A
T
I
C
S

Printed by : M.M. 3114, Madurai Kamaraj University Co-operative Printing Press Ltd.,
Madurai - 625 021. Phone : 2458679 Copies : 1000 Year : 6/2007

MADURAI KAMARAJ UNIVERSITY
MADURAI - 625 021

All rights reserved

SYLLABUS

M.Sc. - I Year

Paper – I : ALGEBRA

- Unit I : Normal subgroups, Quotient groups, Direct products, Permutation groups
- Unit II : Conjugate Classes, Class equation, Cauchy's Theorem, Sylow Theorems
- Unit III : Solvable and Nilpotent groups, Jordan Holder Theorem
- Unit IV : Basic properties of rings, Integral domain Fields, Homomorphism, Isomorphism Ideals, Quotient rings, Prime and Maximal ideals
- Unit V : Euclidian Domain, Principal Ideal Domain, Unique Factorization Domain
- Unit VI : Polynomial rings, Roots of polynomials, Factorization of polynomials, Eisensteins criterion, Gauss Theorem
- Unit VII : Field extensions, Normal extension, Separable extension
- Unit VIII : Galois extensions, Fundamental Theorem of Galois Theory
- Unit IX : Galois group over rations, Construction with straight edge and compass
- Unit X : Finite Fields

Text Books

1. Lecture Material prepared by DDE, Madurai Kamaraj University
2. University Algebra by N.S. Gopalakrishnan
3. Topics in Algebra by I.N. Herstein

SCHEME OF LESSONS

M.Sc. - I Year

Paper – I : ALGEBRA

UNIT – I :

- 1) Groups and Subgroups
- 2) Lagrange's Theorem
- 3) Normal subgroups and Quotient groups.
- 4) Homomorphisms
- 5) Direct products
- 6) Permutation groups

UNIT – II :

- 1) Conjugate classes and Class equation
- 2) Cauchy's Theorem
- 3) Sylow's Theorems

UNIT – III :

- 1) Solvable groups
- 2) Nilpotent groups
- 3) Jordan - Holder Theorem

UNIT – IV : Ring Theory

- 1) Rings and Fields
- 2) Homomorphism and Isomorphism
- 3) Quotient rings
- 4) Prime and Maximal ideals

UNIT – V :

- 1) Euclidian domain
- 2) Principal ideal domain
- 3) Unique factorization domain

UNIT – VI :

- 1) Polynomial rings
- 2) Roots of polynomials
- 3) Eisensteins criteria
- 4) Gauss Theorem

UNIT – VII :

- 1) Field extension
- 2) Normal extensions
- 3) Separable extension

UNIT – VIII :

- 1) Galois extension
- 2) Artin's Theorem
- 3) Fundamental theorem of Galois theory

UNIT – IX :

- 1) Cyclic extension
- 2) Solvability by radicals
- 3) Construction with straight edge and compass

UNIT – X :

- 1) Finite fields

- 1) Euclidean domain
- 2) Principal ideal domain
- 3) Unique factorization domain

- 1) Polynomial rings
- 2) Roots of polynomials
- 3) Eisenstein's criteria
- 4) Gauss Theorem

- 1) Field extension
- 2) Normal extensions
- 3) Separable extension

- 1) Galois extension
- 2) Artin's Theorem
- 3) Fundamental theorem of Galois theory

- 1) Cyclic extension
- 2) Solvability by radicals
- 3) Construction with straight edge and compass

- 1) Finite fields

GROUP THEORY

Definition of a Group :

A non-empty set G , together with a binary composition $*$ (star) is said to form a group, if it satisfies the following postulates.

- (i) $a, b \in G \Rightarrow a * b \in G$ (closed)
- (ii) $a, b, c \in G \Rightarrow a * (b * c) = (a * b) * c \quad \forall a, b, c \in G$ (associative law)
- (iii) There exists an element $e \in G$ such that $a * e = e * a = a \quad \forall a \in G$ (the existence of an identity element in G)
- (iv) For every $a \in G$ there exists an element $a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = e$ (the existence of inverse in G)

Remarks :

- (i) A group G is said to be abelian group (or commutative) if for every $a, b \in G$
 $a * b = b * a \quad \forall a, b \in G$

A group which is not abelian is called, naturally enough, non abelian; having seen a family of examples of such groups we know that non-abelian groups do indeed exist.

Another natural characteristic of a group G is the number of elements it contains. We call this the order of G and denote it by $O(G)$. This number is, of course, most interesting when it is finite. In that case we say that G is a finite group.

- (ii) A non-empty set with a binary operation satisfying axioms (i), (ii) in group is called (closure, associative) a semi group.
- (iii) A non-empty set with a binary operation satisfying axioms (i), (ii), (iii) in group is called (closure, associative, identity) a monoid.

Some examples of groups :

- 1) $\mathbb{Z}$, the set of integers with add as binary operation, 0 is additive identity inverse of a is $-a$.

$\mathbb{Z}$ is an infinite abelian group.

2) $2\mathbb{Z} \rightarrow$ set of even integers with the binary operation of addition elements of $2\mathbb{Z}$ are of the form $2n$.

where $n \in \mathbb{Z}$.

$$2n+2m = 2(n+m) \in 2\mathbb{Z}$$

'+' is closed & associative.

$0 \in 2\mathbb{Z}$ is the additive identity inverse of $2n$ is $-2n \in 2\mathbb{Z}$.

$\circ (2\mathbb{Z}, +)$ is an abelian group.

3) $(n\mathbb{Z}, -)$ is not a group.

$$\circ (a-b)-c = a-(b-c)$$

$$\neq a-b+c$$

4) $\{1, -1\}$ with the binary operation of multiplication is a group.

5) $\mathbb{Q} - \{0\}$ with the binary operation of multiplication is a gp.

$\circ 1$ is identity

$$\circ \text{Inverse of } \frac{m}{n} \text{ is } \frac{n}{m}$$

6) $\mathbb{Q}$ set of all rational numbers.

$$= \left\{ \frac{m}{n} : n \neq 0; m, n \in \mathbb{Z} \right\}$$

$\mathbb{Q}$ with the binary operation of add is a group.

$0 \rightarrow$ identity.

$$\text{Inverse of } \frac{m}{n} \text{ is } \frac{-m}{n}$$

7) The set of rational numbers G is an odd integer as the denominator.

$$G = \left\{ \frac{p}{q} : q \in \mathbb{O} \text{ integer } p \in \mathbb{Z} \right\}$$

$$\frac{a}{b}, \frac{c}{d} \in G. \text{ where } b, d \in \mathbb{O}.$$

$$\circ bd \in \mathbb{O}.$$

$$\circ \frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \in \mathbb{Z}$$

◦ '+' is closed.

$$\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in G$$

where $p, d, f, \in O.z$

$$\circ bd, df \in O.z$$

$$\circ bdf \in O.z$$

$$\begin{aligned} \frac{a}{b} + \left(\frac{c}{d} + \frac{e}{f} \right) &= \frac{a}{b} + \left(\frac{cf + de}{df} \right) \\ &= \frac{adf + cbf + cde}{bdf} \quad \text{----- (1)} \\ &\in O.z \end{aligned}$$

$$\begin{aligned} \left(\frac{a}{b} + \frac{c}{d} \right) + \frac{e}{f} &= \frac{ad + bc}{bd} + \frac{e}{f} \\ &= \frac{adf + bcf + bde}{bdf} \quad \text{----- (2)} \\ &\in O.z \end{aligned}$$

$$(1) = (2)$$

◦ '+' is associative.

◦ o is the additive identity

$$\frac{a}{b} \in z \text{ where } b \in O.z$$

◦ $\frac{-a}{b}$ is the inverse of $\frac{a}{b}$

$$\frac{a}{b}, \frac{c}{d} \in z \quad b, d \in O.z$$

$$bd \in O.z$$

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + cb}{bd} = \frac{c}{d} + \frac{a}{b} \in z$$

◦ '+' is commulative.

◦ (G, +) is an abelian group.

Some preliminary Lemmas :

Lemma (i) :

If G is a group, then

- The identity element of G is unique.
- Every $a \in G$ has a unique inverse in G .

Proof of (a) :

Let G be a group having two identity e and f .
since e is an identity.

$$a.e = e.a = a \quad \forall a \in G \quad \text{----- (1)}$$

Since f is an identity

$$a.f = f.a = a \quad \forall a \in G \quad \text{----- (2)}$$

equation (1) put $a = f$.

$$f.e = e.f = f \quad \text{----- (3)}$$

equation (2) put $a = e$

$$e.f = f.e = e \quad \text{----- (4)}$$

From (3) & (4)

$$e = f$$

The identity element is unique.

Proof of (b) :

Let G be a group.

Let $a \in G$. Let a' , a'' be two inverse of G .

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

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

$$\circ a' = a'.e$$

$$= a'.e$$

$$= a'.(a.a'')$$

$$= (a'.a).a''$$

$$= e.a''$$

$$\circ a' = a''$$

$\circ$ The inverse of an element is unique.

Lemma (ii) :

Left and Right Cancellation Laws :

If G is a group. $a, x, y \in G$. Then

- (i) $a.x = a.y \Rightarrow x=y$ (left cancellation law)
- (ii) $x.a = y.a \Rightarrow x=y$ (right cancellation law)

Proof of (i) :

Let $a.x = a.y$

Sub Premultiply by both sides a^{-1} .

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

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

$$\Rightarrow e.x = e.y$$

$$\Rightarrow x = y$$

which is called the left cancellation law.

Proof of (ii) :

III^{by} Let $x.a = y.a \Rightarrow x = y$

Postmultiply by both sides a^{-1} .

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

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

$$\Rightarrow x.e = y.e$$

$$\Rightarrow x = y$$

which is called the right cancellation law.

Lemma (i) :

Lemma (iii) :

If G is a group then

- (i) For every $a \in G$, $a^{-1})^{-1} = a$
- (ii) For all $a, b \in G$, $(a, b)^{-1} = b^{-1}.a^{-1}$

Proof of (i) :

Let a^1 be the inverse of a^{-1} .

$$\Rightarrow a^1.a^{-1} = a^{-1}.a^1 = e$$

Let a be the inverse of a^{-1} .

$$\Rightarrow a.a^{-1} = a^{-1}.a = e$$

By right cancellation law,

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

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

Proof of (ii) :

Let $a.b$ is inverse of $b^{-1}.a^{-1}$

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

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

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

$$= e$$

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

$$= (b^{-1}.e).b = b^{-1}.b = e$$

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

Hence the Lemma.

Lemma (iv) :

If G is a group the operation $a.x = b$ & $y.a = b$ have unique solution for x & y .

Proof :

Let $a.x = b$

Premultiply the above equation by a^{-1} .

$$\text{We get, } a^{-1}.(a.x) = a^{-1}.b$$

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

$$\Rightarrow e.x = a^{-1}.b$$

$$\Rightarrow x = a^{-1}.b$$

Let x', x'' are two solution,

If the equation $a.x = b$

$$\Rightarrow a.x' = b \text{ \& } a.x'' = b$$

then

$$a.x' = a.x''$$

By the left cancellation law,

$$\Rightarrow x' = x''.$$

$\circ x = a^{-1}.b$ is the unique solution of the equation $a.x = b$.

III^{ly} we can P.T. $y.a = b$

$\circ y = b.a^{-1}$ is the unique solution of the equation $y.a = b$.

Hence the Lemma.

Subgroups :

We have seen that R , the set of real numbers, forms a group under addition and z , the set of integer also forms a group under addition. Also z is a subset of R . It is one of the many situations which prompts us to make.

Definition :

A non-empty subset H of a group G is said to be a subgroup of G , if H forms a group under the binary composition of G . Clearly, if H is a subgroup of G and K is a subgroup of H , then K is a subgroup of G .

If G is a group with identity element e then the subset $\{e\}$ and G are trivially subgroups of G and we call them the trivial subgroups. All other subgroups will be called non-trivial (or proper subgroups).

We sometimes use the notation $H \leq G$ to signify that H is a subgroup of G and $H < G$ to mean that H is a proper subgroup of G .

It would be useful to have some criterion for deciding whether a given subset of a group is a subgroup. This is the purpose of the next two lemmas.

Lemma (i) :

A non-empty subset H of the group G is a subgroup of G if and only if

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

2) $a \in H \Rightarrow a^{-1} \in H$

Proof :

If H is a subgroup then H is a group under the binary operation of G . (i) and (ii) are satisfied by the axiom of a group.

If H satisfies (i) and (ii) closure holds in H by (i)

Again $a, b, c \in H \Rightarrow a, b, c \in G \Rightarrow a(bc) = (ab)c$ By the left cancellation law

Hence associativity holds in H.

Also for any $a \in H, a^{-1} \in H$ and so by (i)

$$\circ \circ aa^{-1} \in H \Rightarrow e \in H$$

This H has identity.

Inverse of each element of H is in H by (ii).

Hence H satisfies all conditions in the definition of a group.

Thus it forms a group.

$\circ \circ H$ is a subgroup of G.

Lemma (ii) :

If H is a non-empty finite subset of a group G and H is closed under multiplication. Then H is a subgroup of G.

Proof :

Since H is non-empty. Let $a \in H$.

Since H is a finite.

Let $O(H) = n$.

$$a.a \in H \Rightarrow a^2 = a.a \in H$$

$$a^3 = a.a^2 \in H, a^4 = a.a^3 \in H \dots \dots a^K = a.a^{K-1} \in H.$$

$(\forall (+ve) \text{ integer } K)$

H contains the infinite collection $\{a^K; K=1, 2, \dots\}$

But $O(H) = n$

There are repetition the above collection. Then there exists (+ve) integer r, s $(r, s > 0)$ such that $a^r = a^s; r \neq s$

either $r < s$ or $r > s$.

Without loss of generality assume that $r > s$.

$$\circ \circ a^r = a^s$$

$$\circ \circ a^{r-s}.a^s = a^{s-s}.a^s$$

$$\Rightarrow a^{r-s}.a^s = ea^s$$

$$\Rightarrow a^{r-s} = e \in H \quad (\because aa^{-1} = e)$$

$$\Rightarrow a^{r-s-1} \cdot a = e$$

$$\Rightarrow a^{-1} = a^{r-s-1} \in H$$

$\therefore H$ is a subgroup of G .

Lemma (iii) :

A non-empty subset H of a group G is a subgroup of G iff $a, b \in H \Rightarrow ab^{-1} \in H$.

Proof :

If H is a subgroup of G .

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

Conversely, if the condition is satisfied. To prove that H is a subgroup of G . Since H is non-empty.

Let $a \in H$

then

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

So H has identity.

Again, for any $a \in H$, as $e \in H$

i.e.) H has inverse of each element.

Finally, for any $a, b \in H$

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

i.e.) H is closed under multiplication.

Hence H forms a group

$\therefore H$ is a subgroup of G .

Problems :

1) P.T. if $(ab)^2 = a^2b^2$, $\forall a, b \in G$ then G is abelian.

Solve :

$$\text{Let } (ab)^2 = a^2b^2$$

$$\Rightarrow (ab)(ab) = (a.a)(b.b)$$

$$\Rightarrow a(ba)b = a(ab).b$$

By using the left and right cancellation law,

$$ba = ab \quad \forall a, b \in G$$

$\therefore G$ is an abelian.

2) If in a group G , every element is its own inverse then G is an abelian.

Solve :

$$\text{Let } a, b \in G$$

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

$$\Rightarrow b^{-1}a^{-1} = ab$$

$$\text{Since } b^{-1} = b \text{ \& } a^{-1} = a$$

$$\therefore ba = ab$$

$\therefore G$ is an abelian.

3) Prove by induction that $(a^m)^n = a^{mn}$.

Proof :

$$\text{For } m = 1.$$

$$(a^1)^n = a^n = a^{1 \cdot n} = a^{mn}$$

$$\text{For } m = 1, \text{ the result is true.}$$

By induction hypothesis Assume the result for $m=K$.

$$\text{i.e.) } (a^K)^n = a^{Kn}$$

$$\text{For } m = K+1$$

$$\begin{aligned} (a^{K+1})^n &= (a^K \cdot a^1)^n = (a^K)^n \cdot (a^1)^n = a^{Kn} \cdot a^n = a^{Kn+n} \\ &= a^{n(K+1)} = a^{(K+1)n} = a^{mn}. \end{aligned}$$

$\therefore$ The proof is complete. $\forall$ (+ve) integers m .

$$\text{For } m = 0.$$

$$(a^0)^n = (a^0)^n = (e)^n = e = (a^n)^0 = a^{n \cdot 0} = a^{m \cdot n}$$

We have extend the result for (-ve) values of m .

If m is (-ve)

$$\circ \quad m = -k. \text{ (Where K is +ve)}$$

$$\circ \quad (a^{-K})^n = \left((a^{-1})^K \right)^n$$

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

$$\circ \quad (a^m)^n = a^{mn}$$

Hence the proof.

4) If $a^2=e$ for every a in a group of G . P.T. G is an abelian.

Solve :

$$\text{Let } a^2 = e$$

$$\Rightarrow a.a = e$$

Premultiply by both sides a^{-1}

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

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

$$\Rightarrow a = a^{-1} \forall a \in G.$$

If $a, b \in G$

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

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

$$\circ \quad (ab) = (ab)^{-1}$$

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

$$\Rightarrow ab = ba$$

$\circ$ G is an abelian.

Definition :

Let G be a group. Let

$$Z(G) = \{x \in G / xg = gx \forall g \in G\}$$

then $Z(G)$ is called centre of the group G .

Theorem :

Centre of a group G is a subgroup of G .

Proof :

Let $Z(G)$ be the centre of the group G .

Then $Z(G) \neq \phi$ as $e \in Z(G)$

Again,

$$x, y \in Z(G) \Rightarrow xg = gx$$

$$yg = gy \quad \forall g \in G$$

$$\Rightarrow g^{-1}x^{-1} = x^{-1}g^{-1}$$

$$g^{-1}y^{-1} = y^{-1}g^{-1} \quad \forall g \in G.$$

Now,

$$\begin{aligned} g(xy^{-1}) &= (gx)y^{-1} = (xg)y^{-1} \\ &= (xg)y^{-1}(g^{-1}g) \\ &= xg(y^{-1}g^{-1})g \\ &= xg(g^{-1}y^{-1})g \\ &= x(gg^{-1})y^{-1}g \\ &= (xy^{-1})g \quad \forall g \in G \\ &= xy^{-1} \in Z(G) \end{aligned}$$

Hence $z(G)$ is a subgroup.

Remark :

Clearly, G is an abelian iff $z(G) = G$.

Definition :

Let G be a group. $a \in G$ be any element. The subset $N(a) = \{x \in G / xa = ax\}$ is called normalizer (or) centralizer of a in G .

Problem :

Find centre of S_3 .

Solve :

$$\text{We have } S_3 = \{I, (12), (13), (23), (123), (132)\}$$

$$\text{Centre of } S_3 \quad z(S_3) = \{\sigma \in S_3 / \sigma\phi = \phi\sigma \quad \forall \phi \in S_3\}$$

Since $(12)(13) = (132)$

Again, Let $(13)(12) = (123)$

we find $(12), (13)$ do not commute.

$\Rightarrow (12) \& (13)$ do not belong to $z(S_3)$

Again,

$(23)(132) = (12)$

$(132)(23) = (13)$

$\Rightarrow (23), (132)$ do not belong to $z(S_3)$

Also

$(123)(12) = (13)$

$(12)(123) = (23)$

$\therefore (123) \notin z(S_3)$

Hence $z(S_3)$ contains only I .

Definition :

Let G be a group, H a subgroup of G ; for $a, b \in G$ we say a is congruent to b mod H , written as $a \equiv b \pmod{H}$ if $ab^{-1} \in H$.

It is easy to prove that this relation is an equivalence relation. Corresponding to this equivalence relation, we get equivalence classes for any $a \in G$, the equivalence class of a , we know will be given by

$$cl(a) = \{x \in G / x \equiv a \pmod{H}\}$$

Definition :

Let H be a subgroup of G and Let $a \in G$ be any element.

Then $Ha = \{ha / h \in H\}$ is called a **right coset** of H in G .

Let H be a subgroup of G and Let $a \in G$ be any element.

Then $aH = \{ah / h \in H\}$ is called a **left coset** of H in G .

We introduce a relation in G as follows :

Lemma :

The relation $a \equiv b \pmod{H}$ is an equivalence relation.

Proof :

(i) If $aa^{-1} = e \in H$ ($\because H$ is a subgroup)

$$\circledast \quad a \equiv a \pmod{H}$$

$\circledast$ This relation is (congruence modulo H) reflexive.

(ii) If $a \equiv b \pmod{H}$

$$\circledast \quad ab^{-1} \in H \quad (H \text{ is a subgroup})$$

$$\circledast \quad (ab^{-1})^{-1} = ba^{-1} \in H$$

$$\Rightarrow \quad b \equiv a \pmod{H}$$

$\circledast$ This relation is symmetric.

(iii) If $a \equiv b \pmod{H}$

$$\circledast \quad b \equiv c \pmod{H}$$

$$\circledast \quad (ab^{-1}) \in H \text{ \& } (bc^{-1}) \in H$$

$$\circledast \quad (ab^{-1})(bc^{-1}) \in H$$

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

$$\Rightarrow \quad a \equiv c \pmod{H}$$

This relation is transitive.

The congruence modulo H is an equivalence relation on G .

Lemma :

For all $a \in G$.

$$Ha = \{x \in G / x \equiv a \pmod{H}\} = cl(a)$$

Proof : .

Let $x \in Ha$

Then $x = ha$ for some $h \in H$

$$\Rightarrow \quad xa^{-1} = h$$

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

$$\Rightarrow \quad x \equiv a \pmod{H}$$

$$\Rightarrow \quad x \in cl(a)$$

Thus, $Ha \subseteq cl(a)$ ----- (1)

Again, Let $x \in cl(a)$ be any element.

Then $x \equiv a \pmod{H}$

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

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

$\Rightarrow x = ha \in Ha$

This $cl(a) \subseteq H(a)$ ----- (2)

From (1) & (2) $Ha = Cl(a)$

Hence the Lemma.

Lemma :

If $[a] = Ha$, the right coset of a .

Proof :

Let $x \in [a]$

$\circ a \equiv x \pmod{H}$

$\circ ax^{-1} \in H$

$\circ ax^{-1} = h \in H$

$\circ a = hx \Rightarrow x = h^{-1}a \in Ha$

$\Rightarrow [a] \subseteq Ha$ ----- (1)

Let $x \in Ha$

$\circ x = ha \ (\forall h \in H)$

$\circ xa^{-1} = h \in H \Rightarrow x \equiv a \pmod{H}$

$\circ a \equiv x \pmod{H} \quad ax^{-1} = h \in H$

$\circ Ha \subseteq [a]$ ----- (2)

From (1) & (2)

$\circ Ha = [a]$

The right coset of H in G are either identical or disjoint

If $b \in Ha \Rightarrow Hb = Ha$
 If $b \notin Ha$
 $\therefore Ha \cap Hb = \phi$.

Lemma :

There is a one-one correspondence between any two right cosets of H in G .

Proof :

Let Ha, Hb be any two right cosets of H in G .

Define a mapping $f : ha \rightarrow Hb$ s.t

$$f(ha) = hb$$

$$\text{Then } h_1a = h_2a \Rightarrow h_1 = h_2 \Rightarrow h_1b = h_2b$$

$$\Rightarrow f(h_1a) = f(h_2a)$$

i.e., f is well defined.

$$f(h_1a) = f(h_2a) \Rightarrow h_1b = h_2b \Rightarrow h_1 = h_2 \Rightarrow h_1a = h_2a$$

Showing f is 1-1.

That f is onto, is easily seen, as for any $hb \in Hb$, ha would be its pre-image.

Theorem : (Lagrange's)

If G is a finite group and H is a subgroup of G then $O(H)$ divides $O(G)$.

Proof :

Define a relation in G as follows.

$a \equiv b \pmod{H}$ if $ab^{-1} \in H$. First of all To verify that this relation is an equivalence relation.

$$1) \text{ If } a.a^{-1} = e \in H (\because H \text{ is a subgroup})$$

$$\therefore a \equiv a \pmod{H}$$

This relation is reflexive.

$$2) \text{ If } a \equiv b \pmod{H}$$

$$\therefore ab^{-1} \in H (\because H \text{ is a subgroup})$$

$$\Rightarrow (ab^{-1})^{-1} = ba^{-1} \in H$$

$$\Rightarrow b \equiv a \pmod{H}$$

This relation is symmetric.

$$3) \text{ If } a \equiv b \pmod{H}$$

and

$$b \equiv c \pmod{H}$$

$$\circ ab^{-1} \in H \text{ \& } bc^{-1} \in H$$

$$\circ (ab^{-1})(bc^{-1}) \in H = a(b^{-1}b)c^{-1} \in H$$

$$= ac^{-1} \in H$$

$$\Rightarrow a \equiv c \pmod{H}$$

$\circ$ This relation is transitive. This is an equivalence relation on G. This equivalence relation on G into disjoint equivalence classes.

$$[a] = Ha$$

$$\text{If } x \in [a]$$

$$\circ a \equiv x \pmod{H}$$

$$\circ ax^{-1} \in H$$

$$\Rightarrow ax^{-1} = h \in H \Rightarrow a = hx \in H \Rightarrow x = h^{-1}a \in Ha$$

$$\circ [a] \subset Ha \quad \text{----- (1)}$$

$$\text{If } x \in Ha$$

$$\circ x = ha \ (\forall h \in H)$$

$$\circ a^{-1}x = h \in H \Rightarrow x = a \pmod{H}$$

$$\circ a \equiv x \pmod{H} \Rightarrow ax^{-1} \in H \Rightarrow x \in [a]$$

$$\circ Ha \subset [a] \quad \text{----- (2)}$$

From (1) & (2)

$$Ha = [a]$$

The right coset of H in G are either disjoint or identical.

$$\text{If } b \in Ha$$

$$\circ \quad Hb = Ha$$

$$\text{If } b \notin Ha$$

$$\circ \quad Ha \cap Hb = \phi$$

$$\circ \quad G = \cup Ha$$

If Ha and Hb are two disjoint right cosets. Let ϕ be a mapping from Ha into Hb .

Defined as follows.

$$\phi(ha) = hb.$$

This mapping is one-one and onto.

$$\circ \quad \phi(h_1 a) = \phi(h_2 a)$$

$$\Rightarrow h_1 b = h_2 b$$

$$\Rightarrow h_1 = h_2 \quad \circ \quad \phi \text{ is 1-1.}$$

A typical element will be of the form

$$h(b) = \phi(ha)$$

$\circ \quad \phi$ is onto.

$\circ \quad \phi$ is a one-one & onto correspondence between the two right cosets Ha and Hb .

$$\circ \quad O(Ha) = O(Hb)$$

All the distinct two right cosets H in G have the same order.

i.e.) $O(H)$

$$\circ \quad O(Ha) = O(H) = O(Hb)$$

$$\circ \quad G = \cup Ha.$$

$$\Rightarrow O(G) = \Sigma O(Ha)$$

If H & K are distinct right cosets.

Then

$$O(G) = KO(H)$$

$$\circ \quad \frac{O(H)}{O(G)} \text{ Hence the theorem.}$$

Definition :

Let G be a group and H , a subgroup of G . Then index of H in G is the number of distinct right (left) cosets of H in G . It is denoted by $i_G(H)$ or $[G:H]$

If G is a finite group

$$i_G(H) = \frac{O(G)}{O(H)}$$

Lagrange's Theorem :

If H is a subgroup of a finite group G , then $\frac{O(H)}{O(G)}$.

Proof :

Let $H = \{h_1, h_2, \dots, h_k\}$ be the distinct elements of H .

If $H = G$ there is nothing to prove.

If $H \neq G$

Let $a \in G, a \notin H$

We now get 2 rows of elements of H .

G as follows :

$h_1, h_2, \dots, h_k$

$h_1a, h_2a, \dots, h_ka$

$\therefore h_i a = h_j a$

$\Rightarrow h_i = h_j$

The elements in the second and all distinct

If $h_i a = h_j$

Then $a = h_i^{-1} h_j \in H$

This is a $\Rightarrow \Leftarrow$

we find that $a \notin H$.

$\therefore$ The two rows of elements contain $2K$ distinct elements of G .

If G does not contain any other element.

$\therefore O(G) = 2K = 2O(H)$

$$\Rightarrow \frac{O(H)}{O(G)}$$

∴ The proof is complete in this case.

If G contains a element b not belongs to this two rows.

Then we can get three rows of elements of H of G as follows.

$h_1, h_2, \dots, h_K$

$h_1a, h_2a, \dots, h_Ka$

$h_1b, h_2b, \dots, h_Kb$

∴ $h_ib = h_jb$

$\Rightarrow h_i = h_j$

The elements in the third row and all distinct.

If $h_ib = h_jb$

$\Rightarrow b = h_i^{-1} h_j \in H$ (∵ H is a subgroup)

$\Rightarrow b$ belongs to the first row.

This is a $\Rightarrow \Leftarrow$ two rows.

Number of elements in the third row.

Consider with an element on the first row.

If $h_ib = h_ja$

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

∴ $h_i^{-1} h_j \in H$

$h_i^{-1} h_j \in H = \{h_1, h_2, \dots, h_K\}$

∴ $h_i^{-1} h_j = h_e \Rightarrow b = (h_i^{-1} h_j)a = (h_e) a$

$\Rightarrow b = (h_e) a$

This contradicts the fact that b does not belongs to the second row.

Number of elements in the third row. Consider with an element in the second row.
We have not got $3K$ distinct elements of G .

If G doesnot contain any other element.

Then

$$O(G) = 3K = 3O(H)$$

$\therefore \frac{O(H)}{O(G)}$. This proof is complete in this case.

If G contains same other elements doesnot belonging to these three rows.

The new element will generated an extra K elements.

This process must three stop at some stage.

Because $O(G)$ is finite.

Suppose this process ends after n steps. Then G has n rows each containing K distinct elements.

Then $O(G) = nK = nO(H)$.

$$\therefore \frac{O(H)}{O(G)}$$

Hence the theorem.

Definition : Order of an element :

If G is a group and $a \in G$ be any element we say a is of order (or period) n if n is the least (+ve) integer s.t. $a^n = e$.

Definition : Cyclic Group :

A group G is called a cyclic group if $\exists$ an element $a \in G$, such that every element of G can be expressed as a power of a . In that case a is called generator of G . We express this fact by writting $G = \langle a \rangle$ or $G = (a)$.

Corollary (i) :

If G is a finite group and $a \in G$, then $\frac{O(a)}{O(G)}$

Proof :

Let $a \in G$ be any element.

Let $H = \{a^n / n \text{ is an integer}\}$

Then H is a cyclic subgroup of G , generated by a .

As $x, y \in H \Rightarrow x = a^n, y = a^m$

$\Rightarrow xy^{-1} = a^n \cdot a^{-m} = a^{n-m} \in H$.

By Lagrange's theorem, $\frac{O(H)}{O(G)}$

But $O(H) = O(a)$

$$\therefore \frac{O(a)}{O(G)}$$

Hence the theorem.

Corollary (ii) :

If G is a finite group and $a \in G$, then $a^{O(G)} = e$.

Proof :

By corollary (i),

$$\frac{O(a)}{O(G)}$$

$O(G) = O(a) \cdot K$ (for some K)

$$\therefore a^{O(G)} = a^{O(a) \cdot K} = \left(a^{O(a)} \right)^K = e^K = e.$$

Thus any element of a finite group has finite order.

Corollary (iii) : (EULER)

If a is an integer and n is a (+ve) integer such that a is relatively prime to n . Then $a^{\phi(n)} \equiv 1 \pmod{n}$.

Proof :

Let u_n = set of integer less than n and relatively prime to n and U_n is a group under multiplication modulo n and $O(u_n) = \phi(n)$.

By a corollary to lagrange theorem,

$$\text{If } P \in u_n.$$

$$\therefore P^{O(u_n)} \equiv 1 \pmod{n}$$

$$\therefore P^{\phi(n)} \equiv 1 \pmod{n} \quad (\forall P \in u_n)$$

$$\text{Let } a = qn + r, \text{ where } 0 \leq r < n.$$

If P is a prime divisor of n and r , then $P/a, P/n$. This contradicts the fact that a and n are relatively prime to each other.

∴ r and n are relatively prime to each other.

$$\begin{aligned} \circ \quad & r \in u_n \\ \circ \quad & r^{\phi(n)} \equiv 1 \pmod{n} \end{aligned}$$

$$\circ \quad a - r = q_n$$

$$\circ \quad \frac{r}{a-r} \Rightarrow a \equiv r \pmod{n}$$

$$\circ \quad a^{\phi(n)} \equiv r^{\phi(n)} \equiv 1 \pmod{n}$$

$$\circ \quad a^{\phi(n)} \equiv 1 \pmod{n}$$

This contradiction proof of mod n .

Corollary (iv) (Fermat) :

If P is a prime number and a is any integer, then $a^P \equiv a \pmod{P}$.

Proof :

If a is relatively prime to P .

By Euler's theorem,

$$a^{\phi(P)} \equiv 1 \pmod{P}$$

Since P is a prime number.

$$\circ \quad \phi(P) = P-1$$

$$\circ \quad a^{P-1} \equiv 1 \pmod{P}$$

$$\circ \quad a^P \equiv a \pmod{P}$$

If a is not relatively prime to P .

Since P is a prime number.

∴ P is common divisor of a and P .

$$\circ \quad \frac{P}{a} \Rightarrow a \equiv 0 \pmod{P}$$

$$\circ \quad \frac{P}{a^P} \Rightarrow a^P \equiv 0 \pmod{P}$$

$$\circ \quad a \equiv a^P \pmod{P}. \text{ Hence the proof.}$$

Corollary (v)

If G is finite group whose order is a prime number P , then G is a cyclic group.

Proof :

Let G be a group of prime order say P .

i.e.) $O(G) = P$ is a prime number.

Let $a \in G, a \neq e$.

Let H be a cyclic subgroup generated by a .

i.e.) $H = (a)$

By Lagrange's theorem

$$\frac{O(H)}{O(G)} = P$$

$$O(H) = 1 \text{ (or) } O(H) = P$$

$$O(H) = 1 \Rightarrow H = \{e\}$$

But $a \in H, a \neq e$

$$O(H) \neq 1$$

$$O(H) = P = O(a)$$

$$G = H = (a)$$

Hence G is a cyclic group.

A Counting Principle :

Lemma (i) :

HK is a subgroup of G if and only if $HK = KH$.

Proof :

$$\left[\begin{array}{l} HK = \{hk; h \in H, k \in K\} \\ \therefore KH = \{kh, k \in K, h \in H\} \end{array} \right]$$

$$\text{If } HK = KH$$

To prove that HK is a subgroup of G .

Let $x, y \in HK$

$$x \in HK \Rightarrow x = hk \text{ where } h \in H, k \in K$$

$$y \in HK \Rightarrow y = h'k' \text{ where } h' \in H, k' \in K$$

$$\begin{aligned}
 xy &= (hk)(h'k') \\
 &= h(kh')k' \quad (1) \\
 kh' &\in KH = HK
 \end{aligned}$$

$$kh' = h_2k_2 \quad \text{where } h_2 \in H, k_2 \in K$$

substituting in (1)

we get,

$$\begin{aligned}
 xy &= h(h_2k_2)k' \\
 &= (hh_2)(k_2k') \\
 &\in HK
 \end{aligned}$$

$$x^{-1} = (hk)^{-1} = k^{-1}h^{-1} \in KH$$

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

HK is a subgroup of G.

Conversely,

If HK is a subgroup of G.

To prove that $HK = KH$.

$$\% \text{ Let } x \in HK \Rightarrow x^{-1} \in HK \quad (\because HK \text{ is a subgroup})$$

$$\% \quad x^{-1} = hk \text{ where } h \in H, k \in K$$

$$\Rightarrow \quad x = (hk)^{-1} = k^{-1}h^{-1} \in KH$$

$$\% \quad HK \subset KH \quad (a)$$

$$\text{Let } x \in KH$$

$$x = kh \text{ where } k \in K, h \in H$$

$$(h^{-1}k^{-1}) \in HK \quad (\because HK \text{ is a subgroup})$$

$$\% \quad (h^{-1}k^{-1})^{-1} \in HK$$

$$\% \quad kh = x \in HK$$

$$KH \subset HK \quad (b)$$

From (a) & (b)

$$\% \quad HK = KH$$

Hence the lemma.

Corollary :

If H, K are subgroups of the abelian group G , then HK is a subgroup of G .

Proof :

Since G is an abelian.

$$\circledast HK = KH$$

$\circledast$ By the previous lemma.

$\circledast HK$ is a subgroup of G .

Hence the proof.

Theory :

If H and K are finite subgroups of G of orders $O(H)$ and $O(K)$, respectively, then

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

Proof :

Let $x \in H \cap K$

To find out how many times an element hk in HK is repeated.

So we proceed as follows.

$$hk = hek$$

$$= h(e)k$$

$$= h(xx^{-1})k$$

$$= (hx)(x^{-1}k)$$

$$[\because h \in H, x \in H \cap K]$$

$$hx \in H, x^{-1}k \in K$$

$$k \in K, x^{-1} \in K, x^{-1}k \in K]$$

$$\Rightarrow hk = h'k'$$

The element hk is repeated at least as many times as $O(H \cap K)$.

$\circledast$ If there is some other repetition of the hk (say)

$$\circledast hk = h_1k_1 \quad \left[\begin{array}{l} h^1 = hx \in H \\ \therefore k^1 = x^{-1}k \in K \end{array} \right]$$

[where $h_1 \in H, k_1 \in K$]

$$\Rightarrow k = h^{-1}h_1k_1$$

$$\circ x = kk_1^{-1} = h^{-1}h_1 \in H \cap K$$

$$\circ x = h^{-1}h_1;$$

$$\circ x = kk_1^{-1}$$

$$\Rightarrow hx = h_1$$

$$\Rightarrow k_1 = x^{-1}k$$

$$\Rightarrow k_1 = x^{-1}k$$

$$\Rightarrow k^{-1}k = k_1$$

Any other repetition h_1k_1 of HK all be of the form

$$h_1k_1 = (hx)(x^{-1}k)$$

$\circ$ Every repetition of hk comes only from an element of $H \cap K$.

$\circ$ Every element hk of HK is repeated exactly $O(H \cap K)$ times.

$\circ$ Total number of element in the distinct of

$$\circ HK = O(H)O(K)$$

$\circ$ Total number of distinct elements of

Theorem :

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

Proof : Hence the theorem.

Corollary :

If H and K are subgroups of G and $O(H) > \sqrt{O(G)}$, $O(K) > \sqrt{O(G)}$ then $H \cap K \neq \{e\}$ (or) $O(H \cap K) > 1$.

Proof :

Let H and K are subgroup of group G .

$$O(HK) < O(G)$$

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

$$\begin{aligned} \circ O(G) &> \frac{O(H) \cdot O(K)}{O(H \cap K)} > \frac{\sqrt{O(G)} \cdot \sqrt{O(G)}}{O(H \cap K)} \\ &= \frac{O(G)}{O(H \cap K)} \end{aligned}$$

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

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

$$\Rightarrow H \cap K \neq \{e\}.$$

Hence the proof.

Lemma :

If $O(a) = n$ and $a^m = e$ for some $m \in \mathbb{Z}$ then n/m .

Proof :

By division algorithm $m = qn + r$

where $0 \leq r < n$.

Given that

$$a^m = e$$

$$\Rightarrow a^{qn+r} = e$$

$$\Rightarrow a^{qn} \cdot a^r = e$$

$$\Rightarrow (a^n)^q \cdot a^r = e$$

$$\Rightarrow a^r = e$$

Since $O(a) = n$ and $r < n$.

$$\circ \quad r = 0 \quad [\circ O(a) = n]$$

$$\circ \quad m = qn \quad a^m = e$$

$$\circ \quad n/m \quad \circ O(a)/m]$$

Hence the proof.

Normal subgroups and Quotient groups :

The subgroups which have the property that all their right cosets equal the corresponding left cosets play a very significant role in the study of groups. In fact that lead us to the formation of another class of groups that are known as quotient groups. We single out such subgroups and call them normal subgroups.

Definition :

A subgroup H of a group G is called a **normal subgroup** of G if $Ha = aH \forall a \in G$.

A normal subgroup is also called **invariant** or self conjugate subgroup.

Clearly G and $\{e\}$ are normal subgroups of G and are referred to as the trivial normal subgroups. A group not having any non-trivial normal subgroup is called a **simple group**.

It is easy to see that if H is normal subgroup of G and K is a subgroup of G s.t. $H \subseteq K \subseteq G$ then H is normal in K .

Again, if G is abelian, all its subgroups will be normal.

Ex. :

$H = \{1, -1\}$ is a normal subgroup of the quaternion group G . Indeed $Ha = \{a, -a\} = aH \forall a \in G$.

Theorem :

H is a normal subgroup of G iff $g^{-1}Hg = H$ for all $g \in G$.

Proof :

Let H be normal in G .

Then $Hg = gH \forall g \in G$

$$g^{-1}Hg = g^{-1}(gH) = (g^{-1}g)H = H$$

$$\therefore g^{-1}Hg = H$$

Conversely,

Let $g^{-1}Hg = H \forall g \in G$.

Premultiplying by both sides g .

$$g(g^{-1}Hg) = gH$$

$$\Rightarrow (gg^{-1})Hg = gH$$

$$\Rightarrow Hg = gH$$

Hence H is normal subgroup.

Theorem :

A subgroup H of G is normal in G iff every left coset of H in G is equal to a right coset of H in G .

Proof :

If H is a normal subgroup of G .

$$g^{-1}Hg = H \quad \forall g \in G$$

Premultiplying both sides by g

$$g(g^{-1}Hg) = gH \quad \forall g \in G$$

$$\Rightarrow (gg^{-1})Hg = gH \quad \forall g \in G$$

$$\Rightarrow Hg = gH \quad \forall g \in G$$

Conversely,

If every left coset of H in G is also a right coset.

Let aH be any left coset of H in G .

$\therefore aH =$ some right coset of H in G .

Since $a \in aH$.

$\therefore aH =$ The right coset of H in G containing a .

Since right cosets are either identical or disjoint a belongs to exactly one right coset namely Ha .

$$\therefore aH = Ha \quad \forall a \in G$$

Premultiplying both sides by a^{-1}

$$\therefore a^{-1}(aH) = a^{-1}(Ha)$$

$$\Rightarrow (a^{-1}a)H = a^{-1}Ha \quad \forall a \in G$$

$$\Rightarrow a^{-1}Ha = H \quad \forall a \in G$$

Theorem :

A subgroup H is normal in a group G iff the product of two right cosets is again a right coset of H in G .

Proof :

Let H be a normal subgroup of G .

$$\therefore aH = Ha \quad \forall a \in G$$

Let Ha, Hb are two distinct right cosets of H in G .

$$\begin{aligned} \therefore (Ha)(Hb) &= H(aH)b \quad (\text{By hypothesis}) \\ &= H(Ha).b \\ &= (H.H)(ab) \\ &= H(ab) \end{aligned}$$

The product of two right cosets is again a right coset of H in G .

Conversely,

If this property holds to prove that H is a normal subgroup of G .

Let Ha, Hb be two distinct right cosets of H in G .

Given :

$(Ha)(Hb) = \text{a right coset of } H \text{ in } G.$

Since $ab = (ea)(eb)$

$\in (Ha)(Hb)$

$\therefore (Ha)(Hb) = \text{The right coset containing } ab.$

Since right cosets are either disjoint or identical.

There is exactly one right coset containing ab , namely $H(ab)$.

$$\therefore (Ha)(Hb) = H(ab) \quad a, b \in G$$

Let $g \in G, h \in H$

$$g^{-1}hg = (eg^{-1})(hg)$$

$$\in (Hg^{-1})(Hg) \quad \forall g \in G, \forall h \in H$$

$$g^{-1}hg \in (Hg^{-1})(Hg)$$

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

$$= H.e = H$$

$\therefore H$ is normal in G .

Theorem :

If H is a normal subgroup of G . G/H is the collection of distinct right cosets of H in G , then G/H is a group under the binary operation of multiplication of subsets of G .

Proof :

Let $x, y \in G/H$

∴ $x = Ha, y = Hb$ for some $a, b \in G$

$$\begin{aligned} x.y &= (Ha).(Hb) \\ &= H(ab) \quad [\because H \text{ is normal}] \end{aligned}$$

Let $x, y, z \in G/H$

$x = Ha, y = Hb, z = Hc$ for some $a, b, c \in G$

$$\begin{aligned} x(yz) &= Ha(Hb.Hc) \\ &= Ha(Hbc) \\ &= Ha(bc) \quad [\because H \text{ is normal}] \end{aligned}$$

$$\begin{aligned} &= H(ab).c \\ &= H(ab)Hc \quad [\because H \text{ is normal}] \\ &= (Ha.Hb).Hc \end{aligned}$$

$$\Rightarrow x(yz) = (x.y).z$$

∴ The associative law is satisfied in G/H .

Let $He = H$ (where e is the identity of G)

Let $X \in G/H$

∴ $X = Ha$ for some $a \in G$ [$\because H$ is normal]

$$x.He = Ha.He = H(ae) = Ha = x$$

III^{ly}

$$He.x = x$$

∴ $He = H$ is the identity of G/H .

If $x = Ha \in G/H$

$$\begin{aligned} (Ha)(Ha^{-1}) &= H(aa^{-1}) \\ &= He \end{aligned}$$

III^{ly}

$$\circ (Ha^{-1})(Ha) = He$$

$\circ Ha^{-1}$ is the inverse of $X = Ha$

$\circ G/H$ is a group

Hence the theorem.

Lemma :

Lemma :

If H is a normal subgroup of G and K is a subgroup of G . Then HK is a subgroup of G .

Proof :

Let $h \in H, k \in K \subset G$

Since H is a normal subgroup of G .

$$\circ k^{-1}hk \in H$$

$$\Rightarrow k^{-1}hk = h^{-1} \in H$$

$$\Rightarrow hk = kh^{-1} \in KH$$

$$\Rightarrow HK \subset KH \quad \text{----- (1)}$$

$$\circ khk^{-1} \in H$$

$$\circ khk^{-1} = h'' \in H$$

$$\Rightarrow kh = h''k \in HK$$

$$\Rightarrow KH \subset HK \quad \text{----- (2)}$$

From (1) & (2)

$$HK = KH$$

$\circ HK$ is a subgroup of G .

Lemma :

Lemma :

If H and K are both normal subgroups of G , then HK is a normal subgroup of G .

Proof :

Proof :

Let $g \in G, x \in HK$

To prove $g^{-1}xg \in HK$

Since $x \in HK$

$$\circ x = hk \quad \circ g^{-1}hg \in H \quad [\because H \text{ is normal}]$$

$$\circ g^{-1}xg = g^{-1}(hk)g \quad \circ g^{-1}kg \in K \quad [\because H \text{ is normal}]$$

$$= (g^{-1}h)(g^{-1}k)g$$

$$= (g^{-1}h)(gg^{-1})(kg)$$

$$\Rightarrow g^{-1}xg = (g^{-1}hg)(g^{-1}kg)$$

$$\Rightarrow g^{-1}xg \in HK \quad (\forall g \in G, \forall x \in HK)$$

$\circ HK$ is a normal subgroup of G .

Lemma :

If H & K are normal subgroups of G s.t. $H \cap K = \{e\}$. Show that for any $h \in H, k \in K$, $hk = kh$.

Proof :

Then every element of H commutes with every element of K .

Let $h \in H, k \in K$. To P.T. $hk = kh$.

Consider

$$x = hkh^{-1}k^{-1} \quad (\text{commutator of } H \text{ \& } K)$$

$$= (hkh^{-1})k^{-1}$$

$$\circ hkh^{-1} \in K \quad [\because K \text{ is a normal subgroup}]$$

$$\circ x = (hkh^{-1})k^{-1} \in K \quad (\because x \in K)$$

$$\circ kh^{-1}k^{-1} \in H \quad [\because K \text{ is a normal subgroup}]$$

$$\circ x = h(kh^{-1}k^{-1}) \in H \quad [\because x \in H \text{ \& } x \in K]$$

$$\circ x \in H \cap K = \{e\}$$

$$\circ x = \{e\} \quad hkh^{-1}k^{-1} = e$$

Post multiply by K

$$hkh^{-1}(k^{-1}k) = k$$

$$\Rightarrow hkh^{-1} = k$$

Post multiply by h

$$hkh^{-1}h = kh$$

$$\Rightarrow hk(h^{-1}h) = kh$$

$$\Rightarrow hk = kh.$$

Hence the lemma.

Lemma :

If H and K are both normal then $H \cap K$ is a normal subgroup.

Proof :

$$\begin{aligned} \text{If } g &\in G \quad x \in H \cap K \\ \circ &g^{-1}xg \in H \quad (\because H \text{ is normal}) \\ \circ &g^{-1}xg \in K \quad (\because K \text{ is normal}) \\ \circ &g^{-1}xg \in H \cap K \quad \forall g \in G, \forall x \in H \cap K \\ \Rightarrow &H \cap K \text{ is a normal subgroup of } G. \end{aligned}$$

Lemma :

If H is a subgroup and K is a normal subgroup then HK is normal in H .

Proof :

$$\begin{aligned} \text{If } h &\in H, x \in H \cap K \\ \circ &h^{-1}xh \in H \\ \circ &h^{-1}xh \in K \quad (\because K \text{ is normal in } G) \\ \circ &h^{-1}xh \in H \cap K \quad \forall h \in H, \forall x \in K \\ \circ &H \cap K \text{ is normal in } H. \end{aligned}$$

Lemma :

The centre of a group is a normal subgroup.

Proof :

Let z be the centre of G .

$$z = \{x: ax=xa, \forall a \in G\}$$

$$\text{Let } g \in G, x \in z$$

$$\begin{aligned}
 \circ g^{-1}xg &= g^{-1}(xg) \\
 &= g^{-1}(gx) \quad [\because x \in z] \\
 &= (g^{-1}g)x = x \in z
 \end{aligned}$$

$$\circ g^{-1}xg \in z, \forall x \in z, \forall g \in G$$

$\Rightarrow z$ is a normal subgroup of G .

Lemma :

Every subgroup of an abelian group is normal.

Proof :

Let H be any subgroup of an abelian group G .

Let $g \in G, h \in H$

$$\circ g^{-1}hg = g^{-1}(hg) = g^{-1}(gh) = (g^{-1}g)h = h \in H$$

$\circ H$ is a normal in G .

Lemma :

A subgroup of index 2 is always a normal subgroup.

Proof :

Let H be a subgroup of index 2 in a group G .

Then H has exactly two distinct right coset and two distinct left cosets in G .

Let $a \in G, a \notin H$

The distinct right cosets of H are $He = H$

$\circ He = H$ and Ha

The distinct left cosets of H are

$$eH = H \text{ and } aH$$

$$\circ G = H \cup Ha$$

$$= H \cup aH$$

$$\circ Ha = aH (\forall a \in G)$$

H is a normal.

Lemma :

If H is the only subgroup of a particular order in G , then H is normal in G .

Proof :

Let $g \in G$, $g^{-1}Hg$ is a subgroup of G and

$$O(g^{-1}Hg) = O(H)$$

$$\therefore g^{-1}Hg = H \quad \forall g \in G$$

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

Theorem :

If H is a subgroup of G , let

$$N(H) = \{g \in G / x^{-1}Hx = H\} \text{ prove}$$

- $N(H)$ is a subgroup of G .
- H is normal in $N(H)$.
- H is normal in G if and only if $N(H) = G$

Proof (a) :

To P.T. $N(H)$ is a subgroup of G .

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

$$\therefore x^{-1}Hx = H$$

$$\therefore y^{-1}Hy = H$$

$$(xy)^{-1}H(xy) = y^{-1}(x^{-1}Hx)y$$

$$= y^{-1}Hy$$

$$\Rightarrow (xy)^{-1}H(xy) = H \Rightarrow xy \in N(H)$$

If $x \in N(H)$

$$\therefore x^{-1}Hx = H$$

$$\Rightarrow Hx = xH$$

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

$$\Rightarrow (x^{-1})^{-1}Hx^{-1} = H \Rightarrow x^{-1} \in N(H)$$

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

Proof of (b) :

To P.T. H is normal in $N(H)$.

Let $h \in H$

$$\circ h^{-1}Hh = H$$

$$\Rightarrow h \in N(H)$$

$$\circ H \subset N(H)$$

Let $x \in N(H)$

By definition

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

$\circ H$ is normal in $N(H)$.

Proof of (c) :

Let M be any other subgroup inside which H is normal.

By definition,

Let $x \in M$

$$\circ x^{-1}Hx = H$$

$$\Rightarrow x \in N(H)$$

$$\circ M \subset N(H)$$

$\circ N(H)$ is the largest subgroup inside which H is normal.

If $N(H) = G$

$\circ H$ is normal subgroup of G .

If H is a normal subgroup of G .

Then $G = N(H)$

$\circ N(H) = G$ iff H is normal in G .

Hence the theorem.

Theorem :

If G is a finite group and N is a normal subgroup of G , then $O\left(\frac{G}{N}\right) = \frac{O(G)}{O(N)}$

Proof :

Since G is finite.

using lagrange's theorem.

$$\circ \frac{O(G)}{O(N)} = \text{number of distinct right cosets of } N \text{ in } G.$$

$$\circ \frac{O(G)}{O(N)} = O\left(\frac{G}{N}\right)$$

Hence the theorem.

Definition - Homomorphisms :

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

Let G be a group with identity e .

$$f: G \rightarrow G$$

$$\circ f(x) = e$$

$$\text{Let } x, y \in G$$

$$\circ f(x) = e \text{ and } f(y) = e$$

$$f(xy) = e = e \cdot e = f(x) \cdot f(y)$$

f - trivial homomorphism or zero homomorphism.

Define the map $f: G \rightarrow G$ and $f(x)=x$, $f(y)=y$

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

$\circ f$ is called the identity homomorphism.

This map f is one-to-one and f is onto.

$G \rightarrow$ group of real numbers and addition.

$\bar{G} \rightarrow$ group of non-zero real numbers under multiplication.

Example :

Let $f: G \rightarrow \bar{G}$ and $f(x) = 2^x$, $f(y) = 2^y$

$$\circ f(x+y) = 2^{x+y} = 2^x \cdot 2^y = f(x) \cdot f(y)$$

$$f(x) = f(y) \Rightarrow 2^x = 2^y$$

$$\Rightarrow x = y$$

∴ f is one-to-one

∴ f is not onto.

Example :

$$\text{Let } f : \overline{G} \rightarrow \overline{G} \text{ and } f(x) = x^2$$

$$f(xy) = (xy)^2 = x^2 y^2 = f(x)f(y)$$

∴ f is not one-to-one

∴ f is not onto.

Example :

$$\text{Let } f : G \rightarrow G \text{ and } f(x) = x+1, f(y) = y+1$$

$$f(x+y) = x+y+1+1$$

$$f(x)+f(y) = x+1+y+1 = x+y+2$$

∴ f is not homomorphism.

Example :

G = set of non-zero numbers under multiplication

$$\overline{G} = \{1, -1\} \text{ under multiplication.}$$

Define $f : G \rightarrow \overline{G}$ as follows

$$f(x) = 1, \text{ if } x > 0$$

$$f(x) = -1, \text{ if } x < 0$$

Let $x, y \in G$.

Case (i) :

If $x > 0, y > 0, xy > 0$

$$f(x) = 1, f(y) = 1$$

$$f(xy) = 1 = 1.1 = f(x).f(y)$$

Case (ii) :

If $x > 0, y < 0, xy < 0$

$$f(x) = 1, f(y) = -1.$$

$$f(xy) = -1 = 1 \cdot -1 = f(x) \cdot f(y)$$

Case (iii) :

III^{ly} when $x < 0, y > 0$

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

Case (iv) :

If $x < 0, y < 0, xy > 0$

$$f(x) = -1, f(y) = -1, f(xy) = 1$$

$$= (-1) \cdot (-1)$$

$$= f(x) \cdot f(y)$$

∴ f is an isomorphism.

∴ f is not one-to-one.

$$\text{∴ } f(5) = 1$$

$$f(-5) = -1$$

∴ f is onto.

This is same as the proof on G -set of (+ve) real numbers under multiplication.

$\overline{G} \rightarrow$ set of real numbers and addition.

Example :

Let $f : G \rightarrow \overline{G}$ as follows.

$$f(x) = \log_{10} x, f(y) = \log_{10} y$$

$$f(xy) = \log_{10}^{xy}$$

$$= \log_{10}^x + \log_{10}^y$$

$$= f(x) + f(y)$$

∴ f is a homomorphism.

$$f(x) = f(y) = \log_{10} x = \log_{10} y$$

∴ f is one-to-one.

Let $x \in \mathbb{R}$

$$f(10^x) = \log_{10} 10^x = x$$

∴ f is onto.

Theorem :

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

Proof :

Let $x, y \in G$

$$\begin{aligned} \phi(xy) &= N(xy) \quad [\because N \text{ is normal}] \\ &= N(x)N(y) \\ &= \phi(x)\phi(y) \end{aligned}$$

∴ ϕ is an homomorphism.

Let $x \in G/N$

$$\phi(x) = Nx \text{ for some } x \in G$$

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

⇒ ϕ is onto.

Hence ϕ is a homomorphism of G onto G/N. this homomorphism is called the natural homomorphism or the canonical homomorphism.

Definition :

If ϕ is a homomorphism of G into $\bar{G}$, The Kernel of ϕ , K_ϕ is defined by $K_\phi = \{x \in G / \phi(x) = \bar{e}, \bar{e} = \text{identity element of } \bar{G}\}$.

Lemma :

If ϕ is a homomorphism of G into $\bar{G}$. Then

(i) $\phi(e) = \bar{e}$, the unit element of $\bar{G}$.

(ii) $\phi(x^{-1}) = [\phi(x)]^{-1}$ for all $x \in G$.

Proof :

(i) Let $x \in G$

$$x = x.e$$

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

$$\Rightarrow \phi(x).\bar{e} = \phi(x).\phi(e)$$

(Left cancellation law)

$$\Rightarrow \phi(e) = \bar{e}$$

(ii) Let $x \in G$

$$x.x^{-1} = e = x^{-1}.x$$

$$\Rightarrow \phi(x.x^{-1}) = \phi(e) = \bar{e}$$

$$\Rightarrow \phi(x).\phi(x^{-1}) = \bar{e} \quad [\because e \text{ is the identity of } G \text{ and } \bar{e} \text{ is the identity of } \bar{G}]$$

III^{ly}

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

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

Hence the lemma.

Lemma :

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

Proof :

Let $x, y \in K_\phi$

$$\phi(x) = \bar{e}, \phi(y) = \bar{e}$$

since ϕ is a homomorphism.

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

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

$$= \bar{e}$$

$$xy \in K_\emptyset$$

$$\text{Let } x \in K_\emptyset, \emptyset(x) = \bar{e}$$

$$\begin{aligned}\emptyset(x^{-1}) &= [\emptyset(x)]^{-1} = (\bar{e})^{-1} \\ &= \bar{e}\end{aligned}$$

$$\Rightarrow x^{-1} \in K_\emptyset$$

∴ $K_\emptyset$ is a subgroup of G .

$$\text{Let } g \in G, x \in K_\emptyset$$

$$\therefore \emptyset(x) = \bar{e}$$

Since $\emptyset$ is a homomorphism.

$$\begin{aligned}\emptyset(g^{-1}xg) &= \emptyset(g^{-1}) \cdot \emptyset(x) \cdot \emptyset(g) \\ &= [\emptyset(g)]^{-1} \cdot \bar{e} \cdot \emptyset(g) \\ &= [\emptyset(g)]^{-1} \cdot \emptyset(g)\end{aligned}$$

$$\Rightarrow \emptyset(g^{-1}xg) = \bar{e}$$

$$\Rightarrow g^{-1}xg \in K_\emptyset$$

∴ $K_\emptyset$ is a normal subgroup of G .

Lemma :

If f be a homomorphism of G onto $\bar{G}$ with Kernel K , then the set of all inverse images of $\bar{g} \in \bar{G}$ and $f^{-1}(\bar{g}) = Kg$. Where g is any element such that $f(g) = \bar{g}$.

Proof :

$$\text{Let } x \in f^{-1}(\bar{g})$$

$$\therefore f(x) = \bar{g} = f(g)$$

$$\Rightarrow f(x) = f(g)$$

Post multiply by $[f(g)]^{-1}$

$$f(x) \cdot [f(g)]^{-1} = f(g) \cdot [f(g)]^{-1}$$

$$\Rightarrow f(x) \cdot f(g^{-1}) = \bar{e} \quad [\because f \text{ is a homomorphism}]$$

$$\Rightarrow f(x)f(g^{-1}) = \bar{e}$$

$$\Rightarrow f(xg^{-1}) = \bar{e}$$

$$\Rightarrow xg^{-1} \in f^{-1}(\bar{e})$$

$$\Rightarrow xg^{-1} \in K \quad [\because f \text{ is a homomorphism}]$$

$$\Rightarrow (xy)(xg^{-1}) = k \in K \text{ (where } k \in K)$$

$$\Rightarrow x = kg \in Kg$$

$$\therefore f^{-1}(\bar{g}) \subset Kg \quad \text{----- (1)}$$

$$\text{Let } x \in Kg$$

$$\therefore x = kg \quad (\because k \in K)$$

$$\Rightarrow f(x) = f(kg)$$

$$\Rightarrow f(x) = f(k)f(g) \quad [\because f \text{ is a homomorphism}]$$

$$\Rightarrow f(x) = \bar{e} \cdot \bar{g} = \bar{g}$$

Corollary :

$$\Rightarrow x \in f^{-1}(\bar{g})$$

$$\Rightarrow x \in f^{-1}(\bar{g})$$

Proof :

$$kg \subset f^{-1}(\bar{g}) \quad \text{----- (2)}$$

From (1) & (2)

$$\text{Then } f^{-1}(\bar{g}) = Kg.$$

Hence the lemma.

Definition :

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

Definition :

Two groups G and $\bar{G}$ are said to be isomorphic if there is an isomorphism of G onto $\bar{G}$. We denote this $G \approx \bar{G}$.

Properties :

Isomorphism induces an equivalence relation in the class of all groups. To verify the following three facts.

(i) $G \approx G$. (reflexive)

(ii) $G \approx \bar{G} \Rightarrow \bar{G} \approx G$. (symmetric)

(iii) $G \approx \bar{G}, \bar{G} \approx \bar{\bar{G}} \Rightarrow G \approx \bar{\bar{G}}$. (transitive)

Proof :

(i) Let G be any group. Then $G \approx G$.

Let $I : G \rightarrow G$ be the identity mapping.

$$\circ x.I = x \quad \forall x \in G$$

$\circ I$ is an identity one-to-one and onto.

$\circ I$ is an isomorphism of G onto G .

$$\circ G \approx G.$$

$\circ$ The relation of isomorphism is reflexive.

(ii) If $G \approx \bar{G}$ then $\bar{G} \approx G$.

If f is an isomorphism of G onto $\bar{G}$.

f is one-to-one and onto.

$f^{-1} : \bar{G} \rightarrow G$ exists

f^{-1} is one-to-one and onto.

Let $\bar{x}, \bar{y} \in \bar{G}$

Since f is onto. then there is an $x, y \in G$.

Such that $f(x) = \bar{x}, f(y) = \bar{y}$

$$f^{-1}(\bar{x}) = x, f^{-1}(\bar{y}) = y$$

$$f(xy) = f(x).f(y) \quad [\because f \text{ is a homomorphism}]$$

$$= \bar{x}.\bar{y}$$

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

$\circ f^{-1}$ is an isomorphism of $\bar{G}$ onto G .

$$\circ \bar{G} \approx G.$$

$\circ$ The relation of isomorphism is symmetric.

(iii) If $G \approx \bar{G}$ and $\bar{G} \approx \bar{\bar{G}}$ then $G \approx \bar{\bar{G}}$. Let f be an isomorphism of G onto $\bar{G}$. Let g be an isomorphism of $\bar{G}$ onto $\bar{\bar{G}}$. $f \circ g$ is a one-to-one mapping G onto $\bar{\bar{G}}$. P.T. it is a homomorphism.

$$\begin{aligned} \text{Let } x, y &\in G \\ (xy)(f \circ g) &= [(xy)f]g \quad [\because f \text{ is a homomorphism}] \\ &= [(xf)(yf)]g \\ &= (xf)g \cdot (yf)g \\ (xy)(f \circ g) &= [x(f \circ g)] \cdot [y(f \circ g)] \end{aligned}$$

$\Rightarrow f \circ g$ is a isomorphism of G onto $\bar{\bar{G}}$.

$$\therefore G \approx \bar{\bar{G}}.$$

From (i), (ii), (iii) isomorphism is an equivalence relation in the collection of all groups.

Hence the property.

Corollary :

A homomorphism $f : G \rightarrow G^1$ is one-to-one iff $\text{Ker } f = \{e\}$.

Proof :

Let $f : G \rightarrow G^1$ be one-one.

Let $x \in \text{Ker } f$ be any element.

Then $f(x) = e^1$ and as $f(e) = e^1$

$\Rightarrow f(x) = f(e) \Rightarrow x = e$ as f is 1-1

Hence $\text{Ker } f = \{e\}$.

Conversely,

Let $\text{Ker } f$ contain only the identity element.

Let $f(x) = f(y)$

Then $f(x) (f(y))^{-1} = e^1$

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

$\Rightarrow xy^{-1} \in \text{Ker } f = \{e\}$

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

$\Rightarrow x = y$ or that f is one-one.

Hence the proof.

Theorem : (first law of homomorphism) (or) (fundamental theorem of group homomorphism) :

If f is a homomorphism of G onto $\bar{G}$ with Kernel K , then $G/K \cong \bar{G}$.

Proof :

Define a mapping $\psi : G/K \rightarrow \bar{G}$ as follows.

If $x \in G/K$, $x = Kx$ (for some $x \in G$)

Define

$$\psi(x) = \psi(Kx)$$

$$\psi(x) = f(x) \in \bar{G}$$

To prove that ψ is well defined.

Let $y \in Kx$, $y = kx$ (for some $k \in K = \text{Kernel of } f$)

Then

$$Ky = Kx$$

$$\therefore f(y) = f(Kx) = f(K)f(x)$$

$$= e \cdot f(x) \quad [\because f \text{ is a homomorphism}]$$

$$\Rightarrow f(y) = f(x) \quad [\because k \in K = \text{Kernel of } f]$$

$$\therefore \psi(Ky) = f(y) = f(x) = \psi(Kx)$$

$\Rightarrow \psi$ is well defined.

To prove that ψ is a homomorphism.

Let $x, y \in G/K$

$$\therefore x = Kx, y = Ky \text{ (for some } x, y \in G)$$

$$\therefore \psi(xy) = \psi(Kx.Ky)$$

$$= \psi(K(xy)) \quad [\because K \text{ is normal}]$$

$$= f(xy) = f(x).f(y) \quad [\because f \text{ is a homomorphism}]$$

$$= \psi(x).\psi(y)$$

$\therefore \psi$ is a homomorphism of G/K onto $\bar{G}$.

Let $\bar{x} \in \bar{G}$

Since $f : G \rightarrow \bar{G}$ is onto.

$$\bar{x} = f(x) \quad (\% \text{ for some } x \in G)$$

$$\Rightarrow \bar{x} = \psi(Kx)$$

$\Rightarrow \psi$ is onto.

$$\text{Let } \psi(x) = \psi(y) \quad (\% \text{ for some } x, y \in G/K)$$

$$\% \quad x = Kx, y = Ky \quad (\% \text{ for some } x, y \in G)$$

$$\% \quad \psi(x) = \psi(Kx)$$

$$\Rightarrow \psi(x) = f(x)$$

$$\% \quad \psi(y) = \psi(Ky)$$

$$\psi(y) = f(y)$$

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

$$\text{Post multiply by } [f(y)]^{-1} \% f(y)[f(y)]^{-1} = f(y)[f(y)^{-1}]$$

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

$$\Rightarrow f(x)f(y)^{-1} = \bar{e}$$

$$\Rightarrow f(xy^{-1}) = \bar{e} \quad (\because f \text{ is a homomorphism})$$

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

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

$$\% \quad x = ky \in Ky$$

$$\Rightarrow Kx = Ky$$

$$\Rightarrow x = y$$

$\Rightarrow \psi$ is one-to-one.

ψ is an isomorphism of G/K onto $\bar{G}$.

Hence, $G/K \approx \bar{G}$.

Hence the theorem.

Simple groups :

A group G is said to be simple if it has no proper normal subgroup.

(or)

G is said to be simple if it has no proper homomorphic images.

Cauchy's Theorem for Abelian groups :

Suppose G is a finite abelian group and $P|O(G)$, where P is a prime number, then there is an element $a \neq e \in G$ such that $a^P = e$.

Proof :

The proof is by induction on the order of G .

If $O(G) = 1$, $G = \{e\}$.

The theorem is trivially true in this case.

Let $O(G) = n > 1$.

Induction hypothesis, Let us assume that the theorem is true for all groups with order $< n$. To prove the theorem for a group G with order $= n$.

Case (i) :

If G has no proper subgroup.

• G is cyclic say $G = \langle a \rangle$ and G is a prime order $O(G) = n$ is a prime number.

• The only prime number dividing n .

• $a \neq e$, $a^n = e$

• The proof of the theorem is complete in this case.

Case (ii) :

If G has a proper subgroup say T .

Let $P|O(T)$.

• $O(T) < O(G) = n$

By the induction hypothesis, the theorem is true for T .

Then $\exists a \in T \subset G$, $a \neq e$ such that $a^P = e$.

• This completes the proof in this case.

Case (iii) :

We may assume that $P \nmid O(T)$

Let $P|O(G)$

Since G is abelian and T is a normal subgroup.

Consider the quotient group G/T .

$$\circ \quad O\left(\frac{G}{T}\right) = \frac{O(G)}{O(T)}$$

Since $P/O(G)$ but $PXO(T)$

$$\circ \quad P / \frac{O(G)}{O(T)} = O\left(\frac{G}{T}\right)$$

Since T is a proper subgroup.

$$\circ \quad O\left(\frac{G}{T}\right) < O(G) = n$$

$$\text{and } P / O\left(\frac{G}{T}\right)$$

By the induction hypothesis, the theorem is true for G/T .

Then $\exists$ an element $X \in G/T$ such that $X \neq T$, $X^P = T$

$\exists$ an $b \in G$ such that $X = Tb \neq T$

$$\circ \quad X^P = (Tb)^P = Tb^P = T$$

$$\circ \quad Tb \neq Te$$

$$\Rightarrow Tb^P = Te$$

$$\circ \quad b \notin T \text{ but } b^P \in T$$

By a corollary to Lang's theorem

$$(b^P)^{O(T)} = e$$

$$\Rightarrow [b^{O(T)}]^P = e$$

$$\text{Let } a = b^{O(T)}$$

$$\text{If } a = e, b^{O(T)} = e$$

$$\circ \quad (Tb)^{O(T)} = Tb^{O(T)}$$

$$\Rightarrow (Tb)^{O(T)} = T$$

$$(Tb)^P = T$$

$$\circ \quad O(Tb) = P$$

$$\circ \quad (Tb)^{O(T)} = T$$

$$\circ \quad P/O(T). \text{ This is } \Rightarrow \Leftarrow$$

Our hypothesis that $PXO(T)$.

$$\circledast a \neq e, \text{ but } a^p = e$$

This complete be proof of the theorem by induction.

Sylow's theorem for Abelian groups :

If G is an abelian group of order $O(G)$, and if P is a prime number, such that $P^\alpha | O(G)$, $P^{\alpha+1} \nmid O(G)$, then G has a subgroup of order P^α .

Proof :

$$\text{If } \alpha = 0$$

$$\circledast P^0 = 1/O(G)$$

$$\circledast P^1 \nmid O(G)$$

$$\circledast \{e\} \text{ is the required subgroup of order } P^0=1.$$

Assume therefore that $\alpha > 0$.

$$\circledast P | O(G)$$

By Cauchy's theorem for abelian groups.

$\exists$ an element $a \neq e \in G$ such that $a^p = e$

$$\text{Let } S = \left\{ x \in G : x^{p^n} = e \text{ for some integer } n \right\}$$

To prove that S is a subgroup.

Since G is finite.

We only have to verify the closure property.

$$\text{Let } x, y \in S.$$

$$\circledast x^{p^n} = e \quad (\because \text{for some integer } n)$$

$$y^{p^m} = e \quad (\because \text{for some integer } m)$$

$$\circledast (xy)^{p^{m+n}} = x^{p^{m+n}} \cdot y^{p^{m+n}} \quad (\because G \text{ is an abelian})$$

$$= \left(x^{p^m} \right)^{p^n} \left(y^{p^m} \right)^{p^n}$$

$$= (e)^{p^n} \cdot (e)^{p^n}$$

$$\Rightarrow (xy)^{p^{m+n}} = e$$

$$\Rightarrow xy \in S \Rightarrow S \text{ is a subgroup of } G$$

To prove that $O(S) = P^\alpha$

Let q be a prime distinct from $P/O(S)$

By Cauchy's theorem for abelian groups,

$\exists a \in S$ such that $a \neq e, a^q = e$

$$\circ \circ \quad O(a) = q$$

$$a \in S \Rightarrow a^{p^n} = e \quad (\because \text{for some integer } n)$$

$$\Rightarrow q/p^n$$

This is absurd.

$$\circ \circ \quad O(S) = p^\beta$$

$$\circ \circ \quad O(S)/O(G) \quad (\text{By Langange's theorem})$$

By hypothesis

$$\text{Let } p^\alpha/O(G)$$

$$p^{\alpha+1}XO(G)$$

$$\circ \circ \quad O(S) = p^\beta \Rightarrow \beta \leq \alpha$$

Let us assume that $\beta < \alpha$

Since α is a subgroup of G and G is an abelian.

$\circ \circ \quad S$ is a normal subgroup of G .

Consider,

$$\frac{G}{S}, \frac{O(G)}{S} = \frac{O(G)}{O(S)}$$

$$\circ \circ \quad p^\alpha/O(\alpha)$$

$$\circ \circ \quad O(S) = p^\beta \text{ where } \beta < \alpha$$

$$\circ \circ \quad p/O\left(\frac{G}{S}\right)$$

By Cauchy's theorem for abelian groups applied to G/S .

$$\exists x \in G/S \text{ such that } x \neq S.$$

$$\circ \circ \quad x^p = S$$

$$\circ \quad x \in G/S \Rightarrow x = Sb$$

$$\circ \quad Sb \neq S, (Sb)^p = s$$

$$\circ \quad b \notin S, \text{ but } b^p \in S$$

$$\circ \quad b^p \in S \Rightarrow (b^p)^{p^n} = e \text{ (for some integer } n)$$

$$\Rightarrow b^{p^{n+1}} = e$$

$$\Rightarrow b \in S \text{ (by definition of } S)$$

$$\Rightarrow \Leftarrow$$

$$\circ \quad \beta = \alpha$$

$$\circ \quad O(S) = p^\alpha$$

$\circ$ S is the required subgroup of G of order p^α .

Hence the theorem.

Cor :

If G is abelian of order $O(G)$ and $p^\alpha/O(G)$, $p^{\alpha+1}XO(G)$, then there is a unique subgroup of G of order p^α .

Proof :

Let S, T be two different subgroups of G of order p^α .

$$\circ \quad O(S) = p^\alpha, O(T) = p^\alpha$$

$$\circ \quad S \neq T$$

$$\text{Since } S \cap T \neq S \text{ and}$$

$$O(S \cap T)/O(S) = p^r$$

$$\circ \quad O(S \cap T) = p^r \text{ (where } r < \alpha)$$

Since G is an abelian

$$ST = TS$$

$\circ$ ST is a subgroup of G

$$\circ \quad O(ST) = \frac{O(S)O(T)}{O(S \cap T)}$$

$$O(ST) = \frac{p^\alpha \cdot p^\alpha}{p^r} = p^{\alpha+(\alpha-r)}$$

By Langange's theorem,

$$O(ST)/O(G)$$

$$\text{i.e.) } P^{\alpha+(\alpha-r)}/O(G)$$

This contradicts to be hypothesis that α is be largest prime of P which divisor $O(G)$.

∴ G has a unique subgroup of order p^α .

Hence the theorem.

In the non-abelian case, this corollary need not be true.

Let $S_3 = A(S)$ where $S = \{a, b, c\}$

$$\text{∴ } O(S) = 6 = 2 \times 3$$

$$\text{∴ } 2^1/O(S_3), 2^2/XO(S_3)$$

By sylow's theorem for abelian groups, S_3 has a subgroup of order 2 and G has subgroup of order S_3 .

Lemma :

Let f be a homomorphism of G onto $\bar{G}$ with Kernal K . For $\bar{H}$ subgroup of $\bar{G}$ Let H be defined by $H = \{x \in G / f(x) \in \bar{H}\}$. Then H is a subgroup of G and $H \supset K$; if $\bar{H}$ is normal in $\bar{G}$, then H is normal in G . Moreover, this association sets up a one-to-one mapping from the set of all subgroups of $\bar{G}$ onto the set of all subgroups of G which contain K .

Proof :

Let $\bar{H}$ be the subgroup of $\bar{G}$.

Let

$$H = f^{-1}(\bar{H}) = \{x \in G / f(x) \in \bar{H}\}$$

First we prove that H is a subgroup of G .

Let $x, y \in H$, $f(x), f(y) \in \bar{H}$

Since $\bar{H}$ is a subgroup of $\bar{G}$

$$\text{∴ } f(x) f(y) \in \bar{H}$$

Since f is a homomorphism.

$$f(xy) = f(x).f(y) \bar{H}$$

$$\Rightarrow xy \in H$$

$$\circ \quad x \in H \Rightarrow f(x) \in \bar{H}$$

Since $\bar{H}$ is a subgroup $[f(x)]^{-1} \in \bar{H}$

Since f is a homomorphism

$$f(x^{-1}) = [f(x)]^{-1} \in \bar{H}$$

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

$\circ$ H is a subgroup of G .

If $\bar{H}$ is normal in $\bar{G}$.

To prove that H is normal in G .

Let $g \in G, h \in H$

$$\circ \quad h \in H \Rightarrow f(h) \in \bar{H}$$

If $\bar{H}$ is a normal subgroup of $\bar{G}$.

Let $f(g) \in \bar{G}, f(h) \in \bar{H}$.

$$\circ \quad [f(g)]^{-1} f(h) f(g) \in \bar{H}$$

Since f is a homomorphism.

$$\begin{aligned} f(g^{-1}hg) &= f(g^{-1})f(h)f(g) \\ &= [f(g)]^{-1} f(h) f(g) \in \bar{H} \\ &\Rightarrow g^{-1}hg \in H \end{aligned}$$

$\Rightarrow H$ is a normal subgroup of G .

If $K \in \text{Kernal of } f = K$.

$$\circ \quad f(K) = \bar{e} \in \bar{H}$$

$$\Rightarrow K \in H$$

$$\circ \quad K \subset H$$

Conversely,

If H is a subgroup of G contain K . To prove that $f(H)$ is a subgroup of $\bar{G}$.

$$\circ \quad f(H) = \{f(x); x \in H\}$$

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

∴ $f(x)f(y) = f(xy)$ [$\because f$ is a homomorphism]

Since H is a subgroup.

$$x, y \in H \Rightarrow xy \in H$$

∴ $f(x)f(y) \in f(H)$

If $f(x) \in f(H)$

$$x \in H \Rightarrow x^{-1} \in H \quad (\because H \text{ is a subgroup})$$

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

∴ $f(H)$ is a subgroup of G

Let $T = f^{-1}(f(H)) \supset H$, clearly $T \supset H$ ----- (1)

Let $x \in T$

∴ $f(x) \in f(H)$

∴ $f(x) = f(h) \quad (\because \text{for some } h \in H)$

Post multiply by $[f(h)]^{-1}$

$$\Rightarrow f(x)[f(h)]^{-1} = f(h)[f(h)]^{-1}$$

$$\Rightarrow f(x)[f(h)]^{-1} = \bar{e}$$

$$f(xh^{-1}) = \bar{e} \quad [\because f \text{ is a homomorphism}]$$

$$\Rightarrow xh^{-1} \in K \subset H$$

$$xh^{-1}H \in \text{ and } h \in H$$

$$(xh^{-1})h = x \in H$$

$$T \subset H \quad \text{----- (2)}$$

From (1) & (2)

$$T = H$$

The correspondence is a one-to-one correspondence between subgroups of $\bar{G}$ and subgroups of G contain K .

Second law of homomorphism :

If f is a homomorphism of G onto $\bar{G}$ with Kernel K and if $\bar{N}$ is a normal subgroup of $\bar{G}$ and $N = f^{-1}(\bar{N})$. Then $G/N \approx \bar{G}/\bar{N}$, Equivalently $G/N \approx (G/K)/(N/K)$.

Proof :

Define a mapping $\phi : G \rightarrow \bar{G}/\bar{N}$ as follows :

$$\begin{aligned} \phi(x) &= \bar{N}, f(x) \\ \text{If } x, y &\in G \\ \phi(xy) &= \bar{N} f(xy) \quad [\because f \text{ is a homomorphism}] \\ &= \bar{N} f(x).f(y) \\ &= [\bar{N} f(x)][\bar{N} f(y)] \\ &= \phi(x).\phi(y) \end{aligned}$$

∴ ϕ is a homomorphism.

∴ A typical element of $\bar{G}/\bar{N}$ is of the form m .

∴ $\bar{N} \bar{x}$ where $\bar{x} \in \bar{G}$

Since $f : G \rightarrow \bar{G}$ is onto

$$\begin{aligned} \bar{x} &= f(x) \text{ for some } x \in G \\ \Rightarrow \bar{N} \bar{x} &= \bar{N} f(x) \\ &= \phi(x) \end{aligned}$$

∴ ϕ is onto.

Let $x \in \text{Kernal of } \phi$

$$\begin{aligned} \phi(x) &= \bar{N} \\ \phi(x) &= \bar{N} = f(x) = \bar{N} \end{aligned}$$

$$f(x) \in \bar{N} \Rightarrow x \in N$$

$$\text{Kernal of } \phi \subset N \quad \text{----- (1)}$$

$$\text{If } x \in N, f(x) \in \bar{N}$$

$$\begin{aligned} \phi(x) &= \bar{N} f(x) = \bar{N} \\ &= (\text{the identity of } \bar{G}/\bar{N}) \end{aligned}$$

$\Rightarrow x \in \text{Kernal of } \phi$.

$$N \subset \text{Kernal of } \phi. \quad \text{----- (2)}$$

From (1) & (2)

∴ Kernal of $\phi = N$

∴ ϕ is a homomorphism of G onto $\overline{G}/\overline{N}$ with Kernal N .

By the first law of homomorphism

$$\therefore G/N \approx \overline{G}/\overline{N}$$

$$\therefore G/K \approx \overline{G}$$

[by theorem f is a homomorphism of G onto $\overline{G}$ with Kernal K].

$$N/K \approx \overline{N}$$

∴ The restriction of f to N is a homomorphism of N onto $\overline{N}$ with Kernal K .

$$G/K \approx \overline{G}$$

$$N/K \approx \overline{N}$$

$$\therefore \frac{G/K}{N/K} \approx \overline{G}/\overline{N} \approx G/N$$

$$\text{Hence } \frac{G/K}{N/K} \approx G/N$$

Hence the proof.

Third law of homomorphism :

If M, N are normal subgroups of G , then $\frac{MN}{N} \approx \frac{M}{M \cap N}, \frac{MN}{M} \approx \frac{N}{M \cap N}$.

Proof :

Define a mapping $f : M \rightarrow \frac{MN}{N}$

Let $f(m) = Nm$ [$\because M \subset MN$]

If $m, m^1 \in M$

$$\begin{aligned} f(mm^1) &= n(mm^1) \\ &= (Nm)(Nm^1) \\ &= f(m)f(m^1) \end{aligned}$$

∴ f is a homomorphism.

To P.T. f is onto.

Let $x \in \frac{MN}{N}$

$$\circledast \quad X = Nx \text{ (where } x \in MN \text{)}$$

Since M and N are normal subgroups.

$\circledast$ MN is a normal subgroup.

$$\circledast \quad MN = NM$$

$$x \in MN = NM$$

$$\Rightarrow x = nm \text{ (where } n \in N, m \in M \text{)}$$

$$x = Nx = N(nm)$$

$$= (Nn)m$$

$$= Nm$$

$$= f(m)$$

$\Rightarrow f$ is onto.

To prove that Kernel of $f = M \cap N$

Let $x \in \text{Kernel of } f, x \in M$

$$f(x) = N = Nx$$

$$\Rightarrow x \in N \Rightarrow x \in M \cap N$$

$$\circledast \quad \text{Kernel of } f \subset M \cap N$$

Conversely,

If $x \in M \cap N$

$$f(x) = Nx$$

$$= N$$

(identity element of MN/N)

$$\circledast \quad x \in \text{Kernel of } f$$

$$\circledast \quad M \cap N \subset \text{Kernel of } f$$

$$\circledast \quad \text{Kernel of } f = M \cap N$$

f is a homomorphism of M onto MN/N with kernel $M \cap N$.

$\circledast$ By the first law of homomorphism

$$\frac{M}{M \cap N} \approx \frac{MN}{N}$$

III^{ly}, we can prove that

$$\frac{N}{M \cap N} \approx \frac{MN}{N}$$

Hence the proof.

Lemma :

The homomorphic image of an abelian group is abelian.

Proof :

Let $f : G \rightarrow \bar{G}$ be a homomorphism of G onto $\bar{G}$.

If G is an abelian to prove.

Let $\bar{x}, \bar{y} \in \bar{G}$

Since f is onto.

$$\bar{x} = f(x), \bar{y} = f(y) \quad (\text{for some } x, y \in G)$$

$$\begin{aligned} \bar{x}\bar{y} &= f(x).f(y) \\ &= f(xy) \quad (\because f \text{ is a homomorphism}) \end{aligned}$$

$$\begin{aligned} \Rightarrow \bar{x}\bar{y} &= f(yx) \quad (\because G \text{ is abelian}) \\ &= f(y).f(x) \end{aligned}$$

$$\bar{x}\bar{y} = \bar{y}\bar{x}$$

$\therefore \bar{G}$ is an abelian.

Lemma :

The homomorphic image of a cyclic group is cyclic.

Proof :

Let $f : G \rightarrow \bar{G}$ be a homomorphism of G onto $\bar{G}$.

If G is cyclic.

Let $G = (a)$

Let $\bar{x} \in \bar{G}$.

Since f is onto.

$$\bar{x} = f(x) \quad (\because \text{for some } x \in G = (a))$$

∴

$$x = a^r \quad (\because \text{for some integer } r)$$

$$\bar{x} = f(x) = f(a^r) = [f(a)]^r \quad [\because f \text{ is a homomorphism}]$$

∴ $\bar{G}$ is cyclic generated by $f(a)$

Hence the proof.

Problems :

G^1 = subgroup generated by $\{aba^{-1}b^{-1}; ab \in G\}$

To prove that G/G^1 is abelian.

Proof :

Let $X, Y \in G/G^1$

∴ $X = G^1a, Y = G^1b$ (for some $a, b \in G$)

$$XY = (G^1a)(G^1b)$$

$$= G^1(ab)$$

$$YX = (G^1b)(G^1a)$$

$$= G^1(ba)$$

∴ $aba^{-1}b^{-1} \in G^1$

Let $aba^{-1}b^{-1} = g^1 \in G^1$

Post multiply by b

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

Post multiply by a

$$ab = g^1(ba)$$

∴ $ab \in G^1(ba)$ ∴ $G^1(ab) = G^1(ba)$

$$\Rightarrow XY = YX \quad (\forall X, Y \in G/G^1)$$

$\Rightarrow G/G^1$ is abelian.

Automorphisms - Definition :

An automorphism of a group G is an isomorphism of the group onto itself.

Example 1 :

Let Z = group of integers under addition.

Then $f = \mathbb{Z} \rightarrow \mathbb{Z}$ s.t. $f(n) = -n$ is an automorphism.

As $f(n) = f(m) \Rightarrow -n = -m \Rightarrow n = m$

$\Rightarrow f$ is 1-1.

Again, Since for any $n \in \mathbb{Z}$.

$f(-n) = n$

$\Rightarrow f$ is onto.

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

Shows that f is a homomorphism and hence an automorphism.

Example :

If G be an abelian group and $f : G \rightarrow G$ be such that $f(x) = x^{-1}$ then as $f(xy) = (xy)^{-1} = y^{-1}x^{-1} = x^{-1}y^{-1} = f(x)f(y)$,

$\therefore f$ is a homomorphism.

Again, $f(x) = f(y) \Rightarrow x^{-1} = y^{-1}$

$\Rightarrow x = y \Rightarrow f$ is 1-1

And hence f is clearly onto and hence an automorphism.

Theorem :

Let G be a group. Let $\text{Aut } G$ denote the set of all automorphisms of G and $A(G)$ be the group of all permutations of G . Then $\text{Aut } G$ is a subgroup of $A(G)$.

Proof :

Since $I \in \text{Aut}(G)$

$\therefore \text{Aut } G \neq \emptyset$.

Let $T \in \text{Aut } G$.

Then T is 1-1 onto from G to G .

$\therefore T$ is a permutation of G .

$\therefore T \in A(G)$

So $\text{Aut } G \subseteq A(G)$

Let $T_1, T_2 \in \text{Aut } G$

Then $(T_1 T_2)(xy) = T_1(T_2(xy))$

$$\begin{aligned}
&= T_1(T_2(x)T_2(y)) \quad [\because T_2 \text{ is a homomorphism}] \\
&= T_1(T_2(x)).T_1(T_2(y)) \quad [\because T_1 \text{ is a homomorphism}] \\
&= (T_1 T_2)(x).(T_1 T_2)(y) \quad \forall x, y \in G
\end{aligned}$$

∴ $T_1 T_2$ is a homomorphism from G into G .

Again, $(T_1 T_2)(x) = (T_1 T_2)(y)$

$$\Rightarrow T_1(T_2(x)) = T_1(T_2(y))$$

$$\Rightarrow T_2(x) = T_2(y) \quad [\text{As } T_1 \text{ is 1-1}]$$

$$\Rightarrow x = y \quad [\text{As } T_2 \text{ is 1-1}]$$

∴ $T_1 T_2$ is 1-1.

Let $x \in G$

Since $T_1: G \rightarrow G$ is onto

$$\exists y \in G \text{ s.t. } T_1(y) = x$$

Again $T_2: G \rightarrow G$ is onto

$$\exists z \in G \text{ s.t. } T_2(z) = y$$

$$\Rightarrow T_1(T_2(z)) = x$$

$$\Rightarrow (T_1 T_2)(z) = x$$

∴ $T_1 T_2$ is also onto.

∴ $T_1 T_2 \in \text{Aut } G$.

Let $T \in \text{Aut } G$

Then T is 1-1 onto $\Rightarrow T$ is invertible

and $T^{-1}: G \rightarrow G$ s.t. $T^{-1}(x) = y \Leftrightarrow T(y) = x$

$$\text{As } TT^{-1} = I = T^{-1}T$$

T^{-1} is 1-1

$$\circ T^{-1}(x_1) = T^{-1}(x_2)$$

$$\Rightarrow TT^{-1}(x_1) = TT^{-1}(x_2)$$

$$\Rightarrow I(x_1) = I(x_2)$$

$$\Rightarrow x_1 = x_2$$

Let $x \in G$, Then $y = T(x) \in G$

$$T^{-1}(y) = T^{-1}(Tx) = (T^{-1}T)x = x$$

∴ T^{-1} is onto

Let $T^{-1}(xy) = z$

then $T(z) = xy$

Let $T^{-1}(x) = x_1, T^{-1}(y) = y_1$

Then

⇒ $x = T(x_1), y = T(y_1)$

∴ $T(z) = xy = T(x_1)T(y_1) = T(x_1y_1)$

∴ T is a homomorphism.

∴ $z = x_1y_1$ as T is 1-1

∴ $T^{-1}(xy) = z = x_1y_1 = T^{-1}(x)T^{-1}(y) \quad \forall x, y \in G$

⇒ T^{-1} is a homomorphism.

Thus $T^{-1} \in \text{Aut } G$.

Hence $\text{Aut } G$ is a subgroup of $A(G)$.

If G is non-abelian for every $x \in G$ define $T_x : G \rightarrow G$ as follows. $gT_x = x^{-1}gx$.

Theorem :

If $I(G)$ = collection of inner automorphism of a group G , then $I(G)$ is a normal subgroup of $\text{Aut}(G)$.

Proof :

Let $T_x, T_y \in I(G)$

(g) $T_x.T_y = (x^{-1}gx)T_y$

$= y^{-1}(x^{-1}gx)y$

$= (xy)^{-1}g(xy)$

$= gT_{xy}$

⇒ $T_x.T_y = T_{xy} \in I(G) \quad \forall x, y \in G$

$gT_e = e^{-1}ge = g = gI$

⇒ $T_e = I$

If $T_x \in I(G)$

$T_x.T_x^{-1} = T_{xx^{-1}} = T_e = I$

III^{ly}

$$T_x^{-1} \cdot T_x = I$$

$$\Rightarrow T_x^{-1} = (T_x)^{-1} \in I(G)$$

$I(G)$ is a subgroup of $\text{Aut}(G)$.

Let $T \in \text{Aut}(G)$

Let $T_x \in I(G)$

$$\begin{aligned} g(T^{-1} \cdot T_x \cdot T) &= [x^{-1}(gT^{-1})x]T \\ &= (x^{-1}T)(gT^{-1})T(xT) \\ &= (xT)^{-1}(g)(xT) \\ &= y^{-1}gy \text{ where } y = xT \end{aligned}$$

$$\Rightarrow g(T^{-1} \cdot T_x \cdot T) = gTy \quad \forall g \in G$$

$$\Rightarrow T^{-1} \cdot T_x \cdot T = T_y \in I(G)$$

$\Rightarrow I(G)$ is a normal subgroup of $\text{Aut}(G)$.

$\text{Aut}(G)/I(G)$ is called a group of outer automorphism.

Suppose G is abelian $gT_x = x^{-1}gx = x^{-1}xg = g$

$$\Rightarrow T_x = I \Rightarrow g(G) = [I]$$

Theorem :

$I(G) \approx G/Z$, where $I(G)$ is the group of inner automorphisms of G , and z is the centre of G .

Proof :

Define a mapping ϕ from G into $I(G)$ as follows.

$$\phi(x) = T_x$$

$$\begin{aligned} \text{Then } \phi(xy) &= T_{xy} = T_x \cdot T_y \\ &= \phi(x) \cdot \phi(y) \end{aligned}$$

$\Rightarrow \phi$ is a homomorphism.

A typical inner automorphism is of the form T_x . $\therefore \phi$ is a homomorphism of G onto $I(G)$

Let $x \in \text{Kernal of } \phi$.

$$\therefore \phi(x) = I$$

$$\Rightarrow \quad \phi(x) = T_x = I$$

$$gT_x = gI, \quad \forall g \in G$$

$$x^{-1}gx = g \quad \forall g \in G$$

Premultiply by x

$$gx = xg \quad \forall g \in G$$

$$\Rightarrow \quad x \in Z, \text{ the centre of } G$$

$$\therefore \text{ Kernel of } \phi \subset Z \quad \text{----- (1)}$$

$$\text{Let } z \in Z$$

$$zg = gz, \quad \forall g \in G$$

$$gT_z = z^{-1}gz \quad (\because \text{ since } z \text{ is centre})$$

$$= z^{-1}(zg)$$

$$\Rightarrow \quad gT_z = g \quad \forall g \in Z$$

$$\Rightarrow \quad T_z = I$$

$$\therefore \quad \phi(z) = I$$

$$\therefore z \subset \text{Kernel of } \phi \quad \text{----- (2)}$$

From (1) & (2)

$$\therefore z = \text{Kernel of } \phi$$

$\therefore \phi$ is a homomorphism of G onto $I(G)$ with Kernel z .

By the 1st law of homomorphism,

$$I(G) \approx G/Z$$

Lemma :

Let G be a group and ϕ an automorphism of G . If $a \in G$ is of order $O(a) > 0$, then $O(\phi(a)) = O(a)$.

Proof :

Let $O(a) = n$, a finite (+ve) integer

$$\therefore \quad a^n = e$$

$$[\phi(a)]^n = \phi(a^n) \quad [\because \phi \text{ is a homomorphism}]$$

$$\Rightarrow [\phi(a)]^n = \phi(a^n) \\ = \phi(e) = e$$

$$\Rightarrow O(\phi(a))/n = O(a)$$

$$\text{If } O(\phi(a)) = m < n$$

$$[\phi(a)]^m = e \Rightarrow \phi(a^m) = e = \phi(e)$$

Since ϕ is one-one

$$\circ a^m = e$$

This contradicts the fact that

$$O(a) = n > m$$

$$\circ O(\phi(a)) = O(a)$$

If $O(a)$ is finite and if $[\phi(a)]^m = e$ [for some (+ve) integer m]

$$[\phi(a)]^m = \phi(a^m) = e = \phi(e)$$

Since ϕ is one-one.

$$\circ a^m = e \text{ since } O(a) = +\alpha \quad \text{we have } m = O$$

$$\circ O(\phi(a)) = +\alpha$$

Hence $O(\phi(a)) = O(a)$.

Theorem :

In G is a finite cyclic group of order n $\text{Aut } G$ is isomorphism to u_n where u_n is the set of (+ve) integer less than n and relatively prime to n with the binary operation of multiplication modulo n . $\text{Aut } G \approx u_n$.

Proof :

Let $\phi \in \text{Aut } G$

Since G is cyclic of order n .

Let G be generated by a .

$$\circ O(a) = n$$

$$O(\phi(a)) = n$$

$$\circ \phi(a) \in G = \langle a \rangle$$

$$\circ \phi(a) = a^r \text{ (where } 0 < r < n)$$

Let d be a common divisor of r and n .

Let $n = n_1 d$

$$r = r_1 d$$

$$\phi(a^{n_1}) = [\phi(a)]^{n_1} = a^{r n_1} = a^{r_1 d n_1}$$

$$= a^{r_1 n} = (a^n)^{r_1} = e$$

$$\phi(a^{n_1}) = e = \phi(e)$$

Since ϕ is one-one, $a^{n_1} = e$

But $O(a) = n$

This is $\Rightarrow \Leftarrow$

$\therefore r$ and n are relatively prime to each other.

Let $r \in u_n$.

Define a mapping $\psi: \text{Aut } G \rightarrow u_n$

$$\psi(\phi) = r$$

where

$$\phi(a) = a^r$$

Conversely,

If $r \in u_n$ define a mapping $\phi: G \rightarrow G$ as follows.

$$\phi(x) = x^r$$

$$\phi(x.y) = (xy)^r = x^r . y^r$$

$$= \phi(x) . \phi(y) \quad [G \text{ is abelian}]$$

$$\text{If } \phi(x) = \phi(y)$$

$$\Rightarrow x^r = y^r$$

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

By rule,

$$O(xy^{-1})/r$$

$$\therefore O(xy^{-1})/O(G) = n$$

Since $r \in u_n$

$$O(xy^{-1})/r$$

$$\& O(xy^{-1})/n \Rightarrow O(xy^{-1})$$

$$\circ \circ \quad xy^{-1} = e$$

$$\Rightarrow \quad x = y$$

$\circ \circ \quad \emptyset$ is one-to-one

Since G is finite and $\emptyset$ is an automorphism of G ,

$\circ \circ \quad \emptyset$ is onto

Let $\emptyset_1, \emptyset_2 \in \text{Aut } G$

$$\text{Let} \quad \emptyset_1(a) = a^{r_1} \quad \forall r_1 \in u_n$$

$$\emptyset_2(a) = a^{r_2} \quad \forall r_2 \in u_n$$

$$(a)(\emptyset_1 \cdot \emptyset_2) = (a^{r_1})\phi_2$$

$$= (a^{r_1})^{r_2}$$

$$= a^{r_1 \otimes r_2}$$

$$\circ \circ \quad \psi(\emptyset_1 \cdot \emptyset_2) = r_1 \otimes r_2$$

$$= \psi(\emptyset_1) \otimes \psi(\emptyset_2)$$

$\circ \circ \quad \psi$ is a homomorphism of the finite group set G onto the finite group u_n .

$\circ \circ \quad \psi$ is an isomorphism of $\text{Aut } G$ onto u_n

$\circ \circ \quad \text{Aut } G \approx u_n$

Hence the proof.

Cayley's Theorem :

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

Proof :

Given a group G .

Let $S = G$.

For every $g \in G$, define $l_g: S \rightarrow S$ as follows

$$x/g = xg$$

$$\text{If} \quad x/g = y/g$$

$$\Rightarrow xg = yg$$

$$\Rightarrow x = y$$

$\Rightarrow l_g$ is one-to-one.

$$\text{Let } y \in S, yg^{-1} \in S$$

$$\begin{aligned}(yg^{-1})/g &= (yg^{-1})g \\ &= y\end{aligned}$$

$\Rightarrow l_g$ is onto

$$\Rightarrow l_g \in A(S)$$

For every $g \in G$,

We know have $l_g \in A(S)$

Define a mapping $\emptyset: G \rightarrow A(S)$ as follows.

$$\emptyset(g) = l_g$$

$$\text{If } g, h \in G$$

$$\emptyset(gh) = l_{gh}$$

$$(x)/gh = x(gh)$$

$$(x)/gh = (xg)h$$

$$\begin{aligned}(x)/gh &= (x/g)/h \\ &= x(lg./h)\end{aligned}$$

$$\Rightarrow /gh = lg./h$$

$$\Rightarrow \emptyset(gh) = \emptyset(g) \cdot \emptyset(h)$$

$\Rightarrow \emptyset$ is a homomorphism of G into $A(S)$.

Let $g_0 \in \text{Kernal of } \emptyset$.

$$\emptyset(g_0) = I \quad (\text{the identity mapping})$$

$$lg_0 = I$$

$$\Rightarrow x/g_0 = xI = x \quad (\forall x \in G)$$

$$\Rightarrow xg_0 = x \quad (\forall x \in G)$$

$$\Rightarrow xg_0 = xe \quad (\forall x \in G)$$

$$\Rightarrow g_0 = e$$

∴ Kernel of $\phi = \{e\}$

∴ ϕ is an isomorphism of G into $A(S)$.

Hence the proof.

Definition :

A subgroup H of G is called a characteristic subgroup of G if $T(H) \subseteq H$ for all $T \in \text{Aut } G$.

Lemma :

Show that a characteristic subgroup of a group G is a normal subgroup of G . Is the converse true?

Proof :

Let H be a characteristic subgroup of G .

Let $g \in G, h \in H$

Now $T(H) \subseteq H, (\forall T \in \text{Aut } G)$

In particular, $T_g(H) \subseteq H$,

T_g being inner automorphism.

Thus $ghg^{-1} = T_g(h) \in T_g(H) \subseteq H$

∴ H is a normal subgroup of G .

Converse, however is not true.

Let G be an abelian group of order 4.

Then $G = \{e, a, b, ab/a^2=e=b^2=(ab)^2, ab=ba\}$

Let $H = \{e, a\} \leq G$

Then H is normal subgroup of G as index of H in G is 2.

Let $T : G \rightarrow G$ s.t. $T(a) = b, T(b) = a, T(ab) = ab, T(e) = e$

Then $T \in \text{Aut } G$

But $T(a) = b \notin H \Rightarrow H$ is not characteristic subgroup of G .

Hence the proof.

Theorem :

Let H be a subgroup of a group G . Let G/H be the collection of distinct right cosets of H in G . Let $S=G/H$. Then $\exists$ a homomorphism ϕ from G into $A(S)$. The Kernel of this homomorphism is the largest normal subgroup of G inside H .

Proof :

For every $g \in G$, define a mapping

$$t_g : S \rightarrow S \text{ as follows.}$$

$$\text{If } X \in S = G/H, X = Ha \text{ for some } a \in G$$

$$Xt_g = (Ha)t_g = H(ag) \in G/H$$

The mapping t_g is well-defined.

To prove t_g is one-to-one.

If

$$t_g(X) = t_g(Y) \text{ (for all } X, Y \in S)$$

$$\therefore X = Ha, Y = Hb \text{ (for some } a, b \in G)$$

$$xt_g = Yt_g$$

$$\Rightarrow (Ha)t_g = (Hb)t_g$$

$$\Rightarrow Hag = Hbg$$

$$\Rightarrow Ha = Hb$$

$\therefore t_g$ is one-one.

To prove t_g is onto.

$$\text{Let } X = Ha \in S$$

$$H(ag^{-1}) \in S$$

$$(H(ag^{-1}))t_g = H(ag^{-1})g = Ha = X$$

$\therefore t_g$ is onto.

$\therefore t_g \in A(S)$ (for every $g \in G$)

Define $\phi: G \rightarrow A(S)$ as follows $\phi(g) = t_g$

Let $g_1, g_2 \in G$

$$\text{Then } \phi(g_1 g_2) = t_{g_1 g_2} \text{ (for any } X \in S)$$

$$\circ \quad X = Ha \text{ (for some } a \in G)$$

$$\begin{aligned} X t_{g_1 g_2} &= (Ha) t_{g_1 g_2} = H a g_1 g_2 = (H a g_1) g_2 \\ &= (H a g_1) t_{g_2} = ((Ha) t_{g_1}) t_{g_2} \\ &= (X t_{g_1}) t_{g_2} \\ &= X t_{g_1 \cdot t_{g_2}} \end{aligned}$$

$$\circ \quad t_{g_1 g_2} = t_{g_1} \cdot t_{g_2}$$

$$\begin{aligned} \text{i.e.) } \quad \emptyset(g_1 g_2) &= t_{g_1 g_2} = t_{g_1} \cdot t_{g_2} \\ &= \emptyset(g_1) \cdot \emptyset(g_2) \end{aligned}$$

$\Rightarrow \emptyset$ is a homomorphism of G into $A(S)$.

Let $g \in \text{Kernal of } \emptyset$.

$$\emptyset(g) = \text{identity mapping of } S.$$

$$\Rightarrow t_g = \text{identity mapping of } S.$$

$$(Ha) t_g = Ha$$

$$\Rightarrow H a g = Ha$$

$$\text{Let } K = \{x \in G; H a x = Ha, \forall a \in G\}$$

$$\text{Kernal of } \emptyset \subset K$$

$$\text{Let } x \in K, H a x = Ha, \forall a \in G$$

$$(Ha) t_x = Ha, \forall a \in G$$

$$\circ \quad t_x = \text{identity mapping of } S$$

$$\circ \quad \emptyset(x) = t_x = \text{identity mapping}$$

$$\Rightarrow x \in \text{Kernal of } \emptyset.$$

$$\text{Kernal of } \emptyset = K$$

$$= \{x: H a x = Ha, \forall a \in G\}$$

Since the Kernal of a homomorphism is a normal subgroup.

K is a normal subgroup of G .

$$\text{Let } x \in K,$$

$$\text{Then } H a x = Ha \quad \forall a \in G$$

If $a = e$,

$$Hex = He = H$$

$$Hx = H \Rightarrow x \in H$$

$$\% K \subset H$$

Let M be any other normal subgroup of G inside H.

Since M is normal.

If $x \in M', a \in G$

$$a^{-1}xa \in M$$

$$\% a^{-1}xa = m \in M$$

[Post multiply by a^{-1}]

$$\Rightarrow a^{-1}x = ma^{-1} \text{ (where } m \in M \subset H)$$

$$a^{-1}x \in Ha^{-1}$$

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

$$\Rightarrow Ha^{-1}x = Ha^{-1} \quad \forall a \in G$$

$$Hax = Ha \quad \forall a \in G$$

$$\Rightarrow x \in K$$

$$\Rightarrow M \subset K$$

$\% K$ is the largest normal subgroup of G inside H.

Hence the proof.

Lemma :

If G has a subgroup H s.t. $O(G)$ doesnot divide $\angle i(H)$. Then G has a proper normal subgroup inside H.

Proof :

If $S=G/H$ be collection of distinct right cosets of H in G.

$\exists$ a homomorphism ϕ of G into $A(S)$.

Where Kernal K is the largest normal subgroup of G inside H.

If ϕ is an isomorphism.

Then $O(G) = O(\phi(G))$

$O(G)$ is a subgroup of $A(S)$.

By Lagrange's theorem,

$$O(\phi(G)) \mid O(A(S))$$

$$O(S) = O(G/H) = i_G(H)$$

$$O(A(S)) = \angle i(H)$$

$$\therefore O(G) \nmid \angle i(H)$$

This contradicts our hypothesis,

$\therefore \phi$ is not an isomorphism

$\therefore K = \text{Kernel of } \phi = \{e\}$

$\therefore G$ has a proper normal subgroup K inside H

Hence the proof.

Lemma :

A group of order 36 is not simple.

Sol :

Let G be a group of order $36 = 2^2 \cdot 3^2$

By Sylow's theorem,

G has a subgroup H of order 3^2 .

$$O(H) = 9$$

$$i(H) = 36/9 = 4$$

$$\angle i(H) = \angle 4 = 24$$

$$O(G) = 36$$

$$O(G) > \angle i(H)$$

$O(G)$ does not divide $\angle i(H)$

$\therefore G$ has a proper normal subgroup inside H .

$\therefore G$ is not simple.

Lemma :

A group of order 99 has a normal subgroup of order 11.

Sol :

Let G be a group of order 99.

$$O(G) = 99 = 3^2 \times 11$$

By sylow's theorem,

G has a subgroup H of order 11.

$$i(H) = O(G)/O(H) = 9$$

$$\angle i(H) = \angle 9$$

$$O(G) = 99$$

$O(G)$ does not divide $\angle i(H)$

∴ G has a proper normal subgroup say K inside H .

$$O(K)/O(H)$$

$$\Rightarrow O(K)/11$$

$$\Rightarrow O(K) = 11 = O(H)$$

$$\Rightarrow K = H$$

∴ G has a normal subgroup of order 11.

Hence the theorem.

Lemma :

An abelian group of order 6 is cyclic.

Proof :

Let G be an abelian group of order 6.

$$\exists a \in G, a \neq e, a^2 = e.$$

$$\exists b \in G, b \neq e, b^3 = e$$

$$O(ab)/6 = O(G)$$

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

This is $\Rightarrow \Leftarrow$

If $O(ab) = 2, (ab)^2 = e$

$$a^2b^2 = e \Rightarrow b^2 = e$$

This is $\Rightarrow \Leftarrow$

$$O(ab) = 3, (ab)^3 = e$$

$$a^3b^3 = e \Rightarrow a^3 = e \Rightarrow a = e$$

This is $\Rightarrow \Leftarrow$

$$\circ O(ab) = 6$$

$\circ G$ is the cyclic subgroup generated by ab .

Lemma :

Any group of order $2n$ contains $a \neq e$ element a s.t. $a^2 = e$

Proof :

If this result is not true.

Then for any $a \in G$.

$$a \neq e,$$

$$\circ a^2 \neq e \neq a^{-1}$$

For any $a \neq e$

Partition G into disjoint subsets, each subset consisting of $\{a, a^{-1}\}$

$\{e\}$ stands in a class by itself.

If there are K such subsets

$$O(G) = 2K+1$$

$$\Rightarrow \Leftarrow$$

This fact that $O(G)$ is even.

$$\circ \exists a \in G \text{ s.t. } a^2 = e$$

Lemma :

A non-abelian group of order 6 is isomorphic to S_3 .

Proof :

Let G be a non-abelian group of order 6.

$$\exists a \in G, a \neq e \text{ s.t. } a^2 = e$$

Let $H = \langle a \rangle$. The cyclic subgroup generated

$$H = \{e, a\}$$

If H is a normal subgroup of G .

$$\text{Let } b \in G$$

$$bab^{-1} \in H = \{e, a\}$$

$$bab^{-1} = e \Rightarrow a = e$$

$$\text{Since } a \neq e, bab^{-1} = a$$

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

Post multiply by b

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

$$\Rightarrow a \in \text{Centre of } G$$

$$H \subset \text{Centre of } G$$

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

$N(b)$ is a subgroup of G containing b and H .

If $b \neq a$

$N(b)$ is a subgroup of G larger than H .

$$[\exists b \in N(b) \text{ and } b \notin H]$$

By Lagrange's theorem,

$$|O(H)/O(N(b))| \mid |O(G)|$$

$$\Rightarrow |Z/O(N(b))| \mid 6$$

$$\Rightarrow |O(N(b))| = 6 = |O(G)|$$

$$\Rightarrow N(b) = G$$

$$\Rightarrow b \in \text{Centre of } G$$

$$\Rightarrow G = \text{Centre of } G$$

$\Rightarrow G$ is abelian

Contradicts the hypothesis that G is non-abelian.

∴ H is not a normal subgroup of G . If $S = G/H$. Then $\exists$ a homomorphism ϕ of G into $A(S)$.

Whose Kernel is the largest normal subgroup of G inside $H = \{e, a\}$

Since H is not normal, Kernel of $\phi = \{e\}$

∴ ϕ is an isomorphism of G into $A(S)$

$$O(S) = O\left(\frac{G}{H}\right) = \frac{O(G)}{O(H)}$$

∴ G is isomorphic to a subgroup of $A(S) = S_3$

But $O(G) = 6$, $O(S_3) = 6$

∴ G is isomorphic to S_3

Hence the proof.

Direct Products :

$A \times B = \{(a, b), a \in A, b \in B\}$ ordered pairs.

$A \times B \neq B \times A$

$A_1 \times A_2 \times \dots \times A_n = \{(G_1 G_2 \dots G_n)\} \quad a_i \in A_i \quad \forall i=1, \dots, n$

ordered n tuples.

$O(A), O(B)$ are finite

$$O(A \times B) = O(A) \cdot O(B)$$

If A and B are groups define a binary operation on $A \times B$ as follows.

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

with respect to component wise multiplication $A \times B$ is group.

$$(a_1 b_1) (a_2 b_2) = (a_1 a_2, b_1 b_2) \quad (a_1 a_2 \in A, b_1 b_2 \in B)$$

Let $(a_1, b_1), (a_2, b_2), (a_3, b_3) \in A \times B$

$$(a_1, b_1) [(a_2, b_2) (a_3, b_3)] = (a_1, b_1) [(a_2 a_3, b_2 b_3)]$$

$$= a_1 (a_2 a_3), b_1 (b_2 b_3)$$

$$= [(a_1 a_2) a_3, (b_1 b_2) b_3]$$

[A and B satisfy the association]

$$= (a_1 a_2, b_1 b_2) (a_3 b_3) \\ = [(a_1, b_1) (a_2, b_2) (a_3, b_3)]$$

∴ The associative law is verify the $A \times B$.

Let e be the identity of A

and f be the identity of B .

$$(ef)(ab) = (ea, fb) \\ = (a, b) \quad \forall (a, b) \in A \times B$$

III^{ly}

$$(ab)(ef) = (ab) \quad \forall (a, b) \in A \times B$$

∴ (e, f) is the identity of $A \times B$.

If $(a, b) \in A \times B$

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

$$\circ \quad (ab)(a^{-1}b^{-1}) = (aa^{-1}, bb^{-1}) = (e, f)$$

III^{ly}

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

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

$$\circ \quad \bar{G} = A \times B \text{ is a group}$$

$\bar{G}$ is called the external direct product of A and B .

$$\text{Define} \quad \bar{A} = \{(a, f) \mid a \in A\}$$

$$\text{If} \quad (a_1, f), (a_2, f) \in \bar{A}$$

$$(a_1, f) (a_2, f) = (a_1 a_2, f) \in \bar{A}$$

$$[(a_1, f)^{-1}] = [a^{-1}, f^{-1}] = (a_1^{-1}, f) \in \bar{A}$$

$\bar{A}$ is a subgroup of $\bar{G}$

$$\text{Let} \quad (a, b) \in \bar{G}, (a_1, f) \in \bar{A}$$

$$(a, b) (a_1, f) (a_1 b)^{-1} = (aa_1, b)(a^{-1}b^{-1})$$

$$= (aa_1 a^{-1}, f) \in \bar{A}$$

$\bar{A}$ is a normal subgroup of $\bar{G}$.

Let $\phi: A \rightarrow \bar{A}$ be defined as follows.

$$\phi(a) = (a, f)$$

$$\phi(a) = (a^1) \Rightarrow (a, f) = (a^1, f)$$

$$\Rightarrow a = a^1 \Rightarrow \phi \text{ is one-one.}$$

Any element of $\bar{A}$ is of the form

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

$$\Rightarrow \phi \text{ is onto.}$$

$$\phi(aa^1) = (aa^1, f) = (aa^1, f.f)$$

$$= (a, f) (a^1, f)$$

$$\phi(aa^1) = \phi(a)\phi(a^1)$$

$\therefore \phi$ is isomorphism of A onto $\bar{A}$.

IIIly, if we define.

$$\bar{B} = \{(e, b); b \in B\}$$

$\therefore$ Then $\bar{B}$ is a normal subgroup of $\bar{G}$ is isomorphic to B .

$$\begin{aligned} \text{If } (a, b) &\in \bar{G} \\ (a, b) &= (ae, fb) \\ &= (a, f) (e, b) \in \bar{A} \cdot \bar{B} \end{aligned}$$

$$\begin{aligned} \text{If } (a, b) &\in \bar{G} \text{ and} \\ (a, b) &= \bar{x} \bar{y} \text{ where } \bar{x} \in \bar{A}, \bar{y} \in \bar{B} \end{aligned}$$

$$\bar{x} \in \bar{A} \Rightarrow \bar{x} = (c, f) \text{ where } c \in A$$

$$\bar{y} \in \bar{B} \Rightarrow \bar{y} = (e, d) \text{ where } d \in B$$

$$\begin{aligned} \therefore (a, b) &= \bar{x} \bar{y} \\ &= (c, f) (e, d) \\ &= (ce, cd) = (c, d) \end{aligned}$$

$$\Rightarrow a = c, b = d$$

$$\begin{aligned} \therefore (a, f) &= (c, f) = \bar{x} \\ (e, b) &= (e, d) = \bar{y} \end{aligned}$$

Every element of $\bar{G}$ has therefore a unique representation as the product of an element of $\bar{A}$ and $\bar{B}$.

∴ $\bar{G}$ is said to be the internal direct product of $\bar{A}$ and $\bar{B}$.

If $G_1, G_2, \dots, G_n$ are groups. We add a binary operation.

$\bar{G} = G_1 \times G_2 \times \dots \times G_n$ as follows.

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

If e_i is the identity of G_i , $[i = 1, \dots, n]$

then $(e_1, e_2, \dots, e_n)$ is the identity of

$$\bar{G} = G_1 \times G_2 \times \dots \times G_n.$$

$$(x_1, x_2, \dots, x_n)^{-1} = (x_1^{-1}, x_2^{-1}, \dots, x_n^{-1})$$

Define $\bar{G}_1 = \{(x_1, e_2, e_3, \dots, e_n) \mid \forall x_1 \in G_1\}$

$\bar{G}_1$ is a normal subgroup of $\bar{G}$ is isomorphic to G_1 .

$$\bar{G}_2 = \{(e_1, x_2, e_3, \dots, e_n) \mid x_2 \in G_2\}$$

$\bar{G}_2$ is a normal subgroup of $\bar{G}$ is isomorphic to G_2 .

$$\dots$$

$$\bar{G}_n = \{(e_1, e_2, \dots, e_{n-1}, x_n) \mid x_n \in G_n\}$$

$\bar{G}_n$ is a normal subgroup of $\bar{G}$ is isomorphic to G_n .

$$\bar{G}_n = (\bar{G}_1, \bar{G}_2, \dots, \bar{G}_n)$$

Every element of $\bar{G}$ has a unique representation as a product of elements of $\bar{G}_1, \bar{G}_2, \dots, \bar{G}_n$.

$\bar{G}$ is the internal direct product of $\bar{G}_1, \bar{G}_2, \dots, \bar{G}_n$.

∴ $\bar{G}$ is the external direct product of $\bar{G}_1, \bar{G}_2, \dots, \bar{G}_n$.

Definition :

A group G is said to be the internal direct product of its normal subgroups $N_1, N_2, \dots, N_K$ if the following two conditions are satisfied.

- (i) $G = N_1 N_2 \dots N_K$
- (ii) Every element $x \in G$ has a unique representation as a product of elements of $N_1, N_2, \dots, N_K$.

Lemma (i) :

If G is the internal direct product of its normal subgroups $N_1, N_2, \dots, N_K$ then

- (i) $N_i \cap N_j = \{e\}$ for $i \neq j$
- (ii) Every element of N_i commutes with every element of N_j , for $i \neq j$.

Proof :

Let $x \in N_i \cap N_j$, $i \neq j$

$$x = e.e \dots \dots e.x.e. \dots \dots e$$

$$= e_1, e_2 \dots \dots e_{i-1} x e_{i+1} \dots \dots e_K \quad \text{----- (1)}$$

Where $e_1 = e_2 = \dots \dots = e_{i-1} = e_{i+1} = \dots \dots = e_K = e$

Since $x \in N_j$.

$$x = f_1 f_2 \dots \dots f_{j-1} x f_{j+1} \dots \dots f_K \quad \text{----- (2)}$$

where

$$f_1 = f_2 = \dots \dots = f_{j-1} = f_{j+1} = \dots \dots = f_K = e$$

Since x has a unique representation as G product of elements of $N_1 N_2 \dots N_j$.

Equation the i^{th} form of the representation (1) and (2).

$$N_i \cap N_j = \{e\} \quad \forall i \neq j$$

(ii) Let $a \in N_i, b \in N_j, i \neq j$

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

$$= (aba^{-1})b^{-1} \in N_j$$

$$\circ x \in N_j \quad [\because N_j \text{ is a normal subgroup of } G]$$

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

$$\circ x \in N_i \quad [\because N_i \text{ is a normal subgroup of } G]$$

$$\circ x \in N_i \cap N_j = \{e\}$$

$$\Rightarrow x = aba^{-1}b^{-1} = e \Rightarrow ab = ba$$

Hence the lemma.

Theorem :

Let G be a group and suppose that G is the internal direct product of $N_1, \dots, N_K$.

Let $T = N_1 \times N_2 \times \dots \times N_K$. Then G and T are isomorphic.

Proof :

Define $\phi : N_1 \times N_2 \times \dots \times N_K \rightarrow G (= N_1 N_2 \dots N_K)$ as follows.

$$\phi(n_1, n_2, \dots, n_K) = n_1 n_2 \dots n_K.$$

$$\text{If } \phi(n_1, n_2, \dots, n_K) = \phi(n_1^{-1}, n_2^{-1}, \dots, n_K^{-1})$$

$$n_1 n_2 \dots n_K = n_1^{-1} n_2^{-1} \dots n_K^{-1}$$

Since every element in G has a unique representation as a product of elements of $N_1, N_2, \dots, N_K$ from the above equation.

We must have

$$n_1 = n_1^{-1}, n_2 = n_2^{-1}, \dots, n_K = n_K^{-1}$$

$$(n_1, n_2, \dots, n_K) = (n_1^{-1}, n_2^{-1}, \dots, n_K^{-1})$$

$\therefore \phi$ is one-one.

$$\text{If } x \in G = N_1 N_2 \dots N_K$$

Then x can be written as

$$x = n_1 n_2 \dots n_K \text{ when } n_i \in N_i \quad [\forall i = 1 \dots K]$$

$$x = n_1 n_2 \dots n_K = \phi(n_1, n_2, \dots, n_K)$$

$\therefore \phi$ is onto.

$$\text{Let } x, y \in T = N_1 \times N_2 \times \dots \times N_K$$

$$x = (x_1, x_2, \dots, x_K), \quad y = (y_1, y_2, \dots, y_K)$$

$$\phi(x) = x_1 x_2 \dots x_K \quad \text{----- (1)}$$

$$\phi(y) = y_1 y_2 \dots y_K \quad \text{----- (2)}$$

$$xy = (x_1, x_2, \dots, x_K) (y_1, y_2, \dots, y_K)$$

$$= (x_1 y_1, x_2 y_2, \dots, x_K y_K)$$

$$\phi(xy) = (x_1 y_1)(x_2 y_2) \dots (x_K y_K)$$

$$= x_1(y_1 x_2)(y_2 x_3) \dots (y_{K-1} x_K) y_K$$

Since G is the internal direct product of $N_1, N_2, \dots, N_K$, every element of N_i commutes with every element of N_j .

$\therefore \phi(xy)$ can be written as

$$\phi(xy) = (x_1 x_2 \dots x_K)(y_1 y_2 \dots y_K)$$

$$= \phi(x)\phi(y) \quad \text{(from equ. (1) & (2))}$$

$$\therefore \phi(xy) = \phi(x)\phi(y) \quad \forall x, y \in T$$

∴ ϕ is a homomorphism.

∴ ϕ is an isomorphism of T onto G .

Hence the theorem.

Lemma (ii) :

If G is the direct product of the normal subgroups $N_1, N_2, \dots, N_K$ iff

- 1) $G = N_1, N_2, \dots, N_K$
- 2) $N_i \cap (N_1 N_2 \dots N_{i-1} N_{i+1} \dots N_K) = \{e\}$ for $i = 1, 2, \dots, K$

Proof :

If G is the direct product of $N_1, N_2, \dots, N_K$.

Let
$$x \in N_i \cap (N_1 N_2 \dots N_{i-1} N_{i+1} \dots N_K)$$

$$x \in N_i \Rightarrow x = e_1 e_2 \dots e_{i-1} x e_{i+1} \dots e_K \quad \text{--- (1)}$$

where
$$e_1 = e_2 = \dots = e_{i-1} = e_{i+1} = \dots = e_K = e$$

$$x \in N_1 N_2 \dots N_{i-1} N_{i+1} \dots N_K$$

x can be also written as

$$x = n_1 n_2 \dots n_{i-1} e n_{i+1} \dots n_K \quad \text{--- (2)}$$

where
$$n_1 \in N_1, \dots, n_K \in N_K$$

Since x should have a unique representation as G a product of elements of $N_1, N_2, \dots, N_K$ equating the i th term in the representation (1) and (2).

$$\therefore x = e$$

$$\therefore N_i \cap (N_1 N_2 \dots N_{i-1} N_{i+1} \dots N_K) = \{e\} \quad [\forall i = 1, 2, \dots, K]$$

Conversely,

If
$$G = N_1 N_2 \dots N_K$$

and
$$N_i \cap (N_1 \dots N_{i-1} N_{i+1} \dots N_K) = \{e\} \quad [\text{for } i = 1, 2, \dots, K]$$

To prove that G is the direct product of $N_1, N_2, \dots, N_K$.

Let $x \in G$. Let x have the representation.

$$x = x_1 x_2 \dots x_K, x_i \in N_i, i = 1, 2, \dots, K$$

$$y = y_1 y_2 \dots y_K, y_i \in N_i, i = 1, 2, \dots, K$$

If $i \neq j$

$$N_i \cap N_j \subset N_i \cap (N_1 N_2 \dots N_{i-1} N_{i+1} \dots N_K) = \{e\}$$

$$\Rightarrow N_i \cap N_j = \{e\} \quad \forall i \neq j$$

Every element of N_i commutes with every element of N_j .

$$\begin{aligned} x_1 x_2 \dots x_K &= y_1 y_2 \dots y_K \\ x_K^{-1} x_K &= (x_1 x_2 \dots x_{K-1})^{-1} (y_1 y_2 \dots y_{K-1}) \\ &= (x_{K-1}^{-1} x_{K-2}^{-1} \dots x_1^{-1}) (y_1 y_2 \dots y_{K-1}) \\ &= (x_1^{-1} y_1) (x_2^{-1} y_2) \dots (x_{K-1}^{-1} y_{K-1}) \end{aligned}$$

Because every element of N_i commutes with every element of N_j for $i \neq j$.

L.H.S. is an element of N_K

R.H.S. is an element of $N_1 N_2 \dots N_{K-1}$

Since $N_K \cap (N_1 N_2 \dots N_{K-1}) = \{e\}$

$$\begin{aligned} x_K^{-1} x_K &= e \\ x_K &= x_K \\ x_1 \dots x_{K-1} &= y_1 \dots y_{K-1} \end{aligned}$$

III^{ly} proceeding, we can prove that

$$\begin{aligned} x_{K-1} &= y_{K-1} \\ x_{K-2} &= y_{K-2} \\ \dots &\dots \dots \\ x_1 &= y_1 \end{aligned}$$

Every element in G has a unique representation as a product of elements of $N_1, N_2, \dots, N_K$.

∴ G is the direct product of $N_1, N_2, \dots, N_K$.

This proves the Lemma.

Lemma (iii) :

If G is the direct product of its normal subgroups $N_1, N_2, \dots, N_K$ iff

- 1) $G = N_1 N_2 \dots N_K$
- 2) $N_i \cap (N_1 N_2 \dots N_{i-1}) = \{e\} \quad \forall i = 1, \dots, K.$

Proof :

If G is the direct product of $N_1, N_2, \dots, N_K$

then $G = N_1 N_2 \dots N_K$

$$N_i \cap (N_1 N_2 \dots N_{i-1} N_{i+1} \dots N_K) = \{e\}$$

$$N_i \cap (N_1 N_2 \dots N_{i-1}) \subset N_i \cap (N_1 N_2 \dots N_{i-1} N_{i+1} \dots N_K) = \{e\}$$

$$\therefore N_i \cap (N_1 N_2 \dots N_{i-1}) = \{e\} \quad [i = 1, 2, \dots, K]$$

Conversely,

If $G = N_1 N_2 \dots N_K$

and

$$N_i \cap (N_1 N_2 \dots N_{i-1}) = \{e\} \text{ for } i = 2, 3, \dots, K.$$

To P.T. G is the direct product of $N_1, N_2, \dots, N_K$

For $i \neq j$

without loss of generality assume $i < j$.

$$\text{Then given } N_j \cap (N_1 N_2 \dots N_{j-1}) = \{e\}$$

$$N_j \cap N_i \subset N_j \cap (N_1 N_2 \dots N_{j-1}) = \{e\}$$

$$\therefore N_j \cap N_i = \{e\} \text{ for } i \neq j$$

Every element of N_i commutes with every element of N_j .

$$\text{Let } x = x_1 x_2 \dots x_K$$

$$x = y_1 y_2 \dots y_K$$

$$\begin{aligned} x_K^{-1} x_K &= (x_1 x_2 \dots x_{K-1})^{-1} (y_1 y_2 \dots y_{K-1}) \\ &= (x_{K-1}^{-1} x_{K-2}^{-1} \dots x_1^{-1}) (y_1 y_2 \dots y_{K-1}) \\ &= (x_1^{-1} y_1) (x_2^{-1} y_2) \dots (x_{K-1}^{-1} y_{K-1}) \end{aligned}$$

Because every element of N_i commutes with every element of N_j .

for $i \neq j$.

L.H.S. is an element of N_K

R.H.S. is an element of $N_1 N_2 \dots N_{K-1}$

Since $N_K \cap (N_1 N_2 \dots N_{K-1}) = \{e\}$

$$x_K^{-1} x_K = e$$

$$\Rightarrow x_K = x_K$$

$$\therefore x_1 \dots x_K = y_1 \dots y_{K-1}$$

III^{ly} proceeding, we can prove that

$$x_{K-1} = y_{K-1}$$

$$x_{K-2} = y_{K-2}$$

$$\dots \dots \dots$$

$$\dots \dots \dots$$

$$x_1 = y_1$$

Every element in G has a unique representation as a product of element of $N_1 N_2 \dots \dots \dots N_K$.

∴ G is a direct product of $N_1 N_2 \dots \dots \dots N_K$.

This proves the Lemma.

Theorem :

A finite product of nilpotent groups is nilpotent.

Proof :

Let A, B be nilpotent groups.

To P.T $A \times B$ is nilpotent.

Then ∃ (+ve) integer K, ℓ such that

$$A_{(K)} = \{e\}, B_{(\ell)} = \{f\}$$

where e and f are the induction of A and B respectively.

Without loss of generality assume $K \leq \ell$

$$A_{(K)} = \{e\}, A_{(\ell)} = \{e\}$$

$$A_{(e)} \times B_{(\ell)} = \{(e, f)\}$$

Let

$$\bar{x} \in (A \times B)_{(1)}$$

$$\bar{x} = \bar{x}_1, \bar{x}_2, \dots \dots \dots \bar{x}_r \text{ where}$$

$$\bar{x}_j = \bar{c}_j \bar{d}_j (\bar{c}_j)^{-1} (\bar{d}_j)^{-1}$$

$$\bar{c}_j = (a_j, b_j) \in A \times B$$

$$\bar{d}_j = (a_j^{-1}, b_j^{-1}) \in A \times B$$

$$\bar{x}_j = (a_j b_j) (a_j^{-1} b_j^{-1}) (a_j^{-1} b_j^{-1}) (a_j b_j)^{-1}$$

$$\Rightarrow \quad \overline{x_j} = \left(a_j a_j^{-1} a_j^{-1} a_j^{-1}, b_j b_j^{-1} b_j^{-1} b_j^{-1} \right) \\ \in A_{(1)} \times B_{(1)}$$

$$\overline{x} = \overline{x_1}, \overline{x_2}, \dots, \overline{x_r} \in A_{(1)} \times B_{(1)}$$

$$\circ (A \times B)_{(1)} \subset A_{(1)} \times B_{(1)}$$

Induction hypothesis,

$$(A \times B)_{(i-1)} \subset A_{(i-1)} \times B_{(i-1)}$$

To prove that

$$(A \times B)_{(i)} \subset A_{(i)} \times B_{(i)}$$

Let

$$\overline{x} \in (A \times B)_{(i)}$$

$$\overline{x} = \overline{x_1}, \overline{x_2}, \dots, \overline{x_r}$$

$$\text{where each } \overline{x_j} = \overline{c_j} \overline{d_j} (\overline{c_j})^{-1} (\overline{d_j})^{-1}$$

$$\text{where } \overline{c_j} \in A \times B, \overline{d_j} \in (A \times B)_{(i-1)} \subset A_{(i-1)} \times B_{(i-1)}$$

$$\overline{c_j} = (a_j, b_j), \overline{d_j} = (a_j^{-1}, b_j^{-1})$$

$$a_j^{-1} \in A_{(i-1)}, b_j^{-1} \in B_{(i-1)}$$

$$\overline{x_j} = (a_j, b_j) (a_j^{-1}, b_j^{-1}) (a_j^{-1}, b_j^{-1})^{-1} (a_j^{-1}, b_j^{-1})^{-1}$$

$$= \left(a_j a_j^{-1} a_j^{-1} a_j^{-1}, b_j b_j^{-1} b_j^{-1} b_j^{-1} \right)$$

$$\in A_{(i)} \times B_{(i)} \quad (\forall i = 1, 2, \dots, r)$$

$$\overline{x} = \overline{x_1}, \overline{x_2}, \dots, \overline{x_j} \in A_{(i)} \times B_{(i)}$$

$$\circ (AB)_{(i)} \subset A_{(i)} \times B_{(i)} \quad (\forall (+ve) \text{ integer})$$

In particular for $i = \ell$

$$(A \times B)_{\ell} \subset A_{(\ell)} \times B_{(\ell)} = \{(e, f)\}$$

$$\circ (A \times B)_{(\ell)} = \{(e, f)\}$$

$\circ A \times B$ is nilpotent.

Induction hypothesis, Let the product of nilpotent groups be nilpotent.

Let $G_1, G_2, \dots, G_n$ be nilpotent groups.

By the induction hypothesis.

$G_1 \times G_2 \times \dots \times G_{n-1}$ is nilpotent.

∴ $(G_1 \times G_2 \times \dots \times G_{n-1}) \times G_n$ is nilpotent.

Since $(G_1 \times G_2 \times \dots \times G_{n-1}) \times G_n$ is isomorphic to $G_1 \times G_2 \times \dots \times G_n$

∴ $G_1 \times G_2 \times \dots \times G_n$ is nilpotent.

A finite product of nilpotent groups is nilpotent.

Lemma :

If P is a P -sylow subgroup of G . P.T. $N(N(P)) = N(P)$.

Proof :

P is a p -sylow subgroup of G .

P is a p -sylow subgroup of $N(P)$

P is a normal subgroup of $N(P)$

Any other p -sylow subgroup of $N(P)$ is of the form xpx^{-1} , $x \in N(P)$

Since $xpx^{-1} = P$

P is the only p -sylow subgroup of $N(P)$

Let $x \in N(N(P))$

$$xN(P)x^{-1} = N(P)$$

$$P \subset N(P)$$

$$\therefore xpx^{-1} \subset xN(P)x^{-1} = N(P)$$

$$xpx^{-1} \subset N(P)$$

$$O(xpx)^{-1} = O(P)$$

∴ xpx^{-1} is a p -sylow subgroup of $N(P)$

P is the only p -sylow subgroup of $N(P)$

$$\therefore xpx^{-1} = P$$

$$\Rightarrow x \in N(P)$$

$$\therefore N(N(P)) \subset N(P)$$

$$N(P) \subset N(N(P))$$

$$\therefore N(N(P)) = N(P)$$

Hence the lemma.

Theorem :

A finite group is nilpotent iff it is the direct product of its sylow subgroups.

Proof :

Let G be the direct product of its sylow subgroups.

i.e.) Let $G = P_1 \times P_2 \times \dots \times P_K$

where $P_1, P_2, \dots, P_K$ are the sylow subgroups of G

Let $O(P_i) = P_i^{\alpha_i}$

$\therefore$ each P_i is nilpotent

$\therefore G$ is a finite product of nilpotent groups.

$\therefore G$ is nilpotent

Conversely,

Let G be a finite nilpotent group.

where $P_1, P_2, \dots, P_K$ are the distinct prime dividing $O(G)$.

Let $O(G) = P_1^{\alpha_1} P_2^{\alpha_2} \dots P_K^{\alpha_K}$

G has a p_1 -sylow subgroup, say P_1

G has a p_2 -sylow subgroup, say P_2

" " " " "

" " " " "

" " " " "

G has a p_K -sylow subgroup, say P_K

$$O(P_i) = P_i^{\alpha_i} \quad [\forall i=1,2,\dots,K]$$

Let $H = N(P_i)$

Since G is nilpotent, if H is a proper subgroup of G .

$$H \neq N(H)$$

Since P_i is a sylow subgroup.

$$\begin{aligned} N(N(P_i)) &= N(P_i) \\ \text{i.e.) } N(H) &= H \\ \circ N(P_i) &= G \end{aligned}$$

$\circ$ each P_i is a normal subgroup of G $[\forall i=1,2,\dots,K]$

$$O(P_1 \cap P_2) / O(P_1) = P_1^{\alpha_1}$$

$$\text{Proof: } O(P_1 \cap P_2) / O(P_2) = P_2^{\alpha_2}$$

$$\Rightarrow O(P_1 \cap P_2) = 1$$

$$\circ P_1 \cap P_2 = \{e\}$$

$$O(P_1 P_2) = \frac{O(P_1)O(P_2)}{O(P_1 \cap P_2)} = P_1^{\alpha_1} P_2^{\alpha_2}$$

Induction hypothesis, Assume

$$P_i \cap (P_1 P_2 \dots P_{i-1}) = \{e\}$$

and

$$O(P_1 P_2 \dots P_i) = P_1^{\alpha_1} P_2^{\alpha_2} \dots P_i^{\alpha_i}$$

$$O(P_{i+1} \cap (P_1 P_2 \dots P_i)) / P_{i+1}^{\alpha_{i+1}}$$

$$O(P_{i+1} \cap (P_1 P_2 \dots P_i)) / P_1^{\alpha_1} P_2^{\alpha_2} \dots P_i^{\alpha_i}$$

Since P_{i+1} is distinct from

$P_1 P_2 \dots P_i$, we have

$$O(P_{i+1} \cap (P_1 P_2 \dots P_i)) = 1$$

$$\circ P_{i+1} \cap (P_1 P_2 \dots P_i) = \{e\}$$

$$O(P_1 P_2 \dots P_{i+1}) = \frac{O(P_1 \dots P_i) O(P_{i+1})}{O(P_{i+1} \cap P_1 P_2 \dots P_i)}$$

$$= P_1^{\alpha_1} P_2^{\alpha_2} \dots P_i^{\alpha_i} P_{i+1}^{\alpha_{i+1}}$$

In particular for $i = K$

$$O(P_1 P_2 \dots P_K) = P_1^{\alpha_1} P_2^{\alpha_2} \dots P_K^{\alpha_K}$$

$$\Rightarrow G = P_1 P_2 \dots P_K$$

and

$$P_i \cap (P_1 P_2 \dots P_{i-1}) = \{e\} \quad (\forall i = 1, 2, \dots, K)$$

∴ G is the direct product of its sylow subgroups $P_1 P_2 \dots P_K$.

Hence the theorem.

Theorem :

P.T. a group of order P^2 is either cyclic or is isomorphic to a direct product of two cyclic groups each of order P .

Proof :

Let G be a group of order P^2 .

If $\exists a \in G$ s.t. $O(a) = P^2$

Then $G = (a)$, the cyclic subgroup generated by a .

∴ G is cyclic.

If G doesnot contain any element of order P^2 .

If $a \in G, a \neq e$

$$O(a) = P$$

Let $H = (a)$, the cyclic subgroup generated by a .

Let $b \in G, b \notin H$

∴ $b \neq e, O(b) = P$

Let $K = (b)$, the cyclic subgroup generated by b .

Since G is abelian, both H and K are normal in G .

$H \cap K$ is a subgroup of H .

$$H \cap K = H$$

$$\Rightarrow K \subset H$$

$$\Rightarrow K = H$$

This is a $\Rightarrow \Leftarrow$

Because $b \in K, b \notin H$

$$\therefore H \cap K = \{e\}$$

$$O(HK) = \frac{O(H) \cdot O(K)}{O(H \cap K)} = P \cdot P = P^2 = O(G)$$

∴

$$G = HK \text{ and } H \cap K = \{e\}$$

∴ G is isomorphic to $H \times K$

Hence the theorem.

Theorem (i) :

Every finite abelian group is a direct product of its sylow-subgroups.

Proof :

Let G be a finite abelian group.

Let $P_1, P_2, \dots, P_K$ be the distinct prime dividing $O(G)$.

$$O(G) = P_1^{\alpha_1} P_2^{\alpha_2} \dots P_K^{\alpha_K} \text{ where each } \alpha_i \geq 1.$$

G has a p_1 -sylow subgroup, say P_1

G has a p_2 -sylow subgroup, say P_2

∴ ∴ ∴ ∴ ∴

G has a p_K -sylow subgroup, say P_K

Since G is abelian, $P_1 P_2, \dots, P_K$ are all normal in G.

$$O(P_i) = P_i^{\alpha_i} \quad [i=1, 2, \dots, K]$$

$$O(P_1 \cap P_2) / O(P_1) \Rightarrow O(P_1 \cap P_2) / P_1^{\alpha_1}$$

$$O(P_1 \cap P_2) / O(P_2) \Rightarrow O(P_1 \cap P_2) / P_2^{\alpha_2}$$

$$\therefore O(P_1 \cap P_2) = 1$$

$$\Rightarrow P_1 \cap P_2 = \{e\}$$

$$O(P_1 P_2) = \frac{O(P_1) O(P_2)}{O(P_1 \cap P_2)}$$

$$= P_1^{\alpha_1} P_2^{\alpha_2}$$

Induction hypothesis,

Assume that $P_i \cap P_1 P_2 \dots P_{i-1} = \{e\}$

$$\text{and } O(P_1 P_2 \dots P_i) = P_1^{\alpha_1} P_2^{\alpha_2} \dots P_i^{\alpha_i}$$

$$O(P_{i+1} \cap P_1 P_2 \dots P_i) / O(P_{i+1}) = P_{i+1}^{\alpha_{i+1}}$$

$$O(P_{i+1} \cap P_1 P_2 \dots P_i) / O(P_1 P_2 \dots P_i) = P_1^{\alpha_1} P_2^{\alpha_2} \dots P_i^{\alpha_i}$$

Since P_{i+1} is distinct from $P_1, P_2, \dots, P_i$

$$O(P_{i+1} P_1 P_2 \dots P_i) = 1$$

$$\Rightarrow P_{i+1} \cap P_1 P_2 \dots P_i = \{e\}$$

$$O(P_1 P_2 \dots P_{i+1}) = O(P_1 P_2 \dots P_i) O(P_{i+1})$$

$$= P_1^{\alpha_1} P_2^{\alpha_2} \dots P_i^{\alpha_i}$$

$$O(P_1 P_2 \dots P_{i+1}) = P_1^{\alpha_1} P_2^{\alpha_2} \dots P_{i+1}^{\alpha_{i+1}}$$

$$O(P_1 P_2 \dots P_K) = P_1^{\alpha_1} P_2^{\alpha_2} \dots P_K^{\alpha_K} = O(G)$$

$$\Rightarrow G = P_1 P_2 \dots P_K$$

and

$$P_i \cap (P_1 P_2 \dots P_{i-1}) = \{e\}$$

$\therefore G$ is the direct product of $P_1 P_2 \dots P_K$.

i.e.) G is the direct product of its sylow subgroups.

This proves the theorem.

Theorem :

Any abelian group of order P^n where P is a prime, then G can be expressed as a direct product of cyclic subgroup.

Proof :

Let G be an abelian group of order P^n .

If $\exists a \in G$ s.t. $O(a) = P^n$

Then $G = \langle a \rangle$, the cyclic subgroup generated by a .

$\therefore G$ is cyclic.

If G doesnot contain any element of order P^n .

Let a_1 be the element of G .

Whose order is a maximum in G .

Let $O(a_1) = P^{n_1}, n_1 < n$

$$\begin{aligned}\text{If } x \in G, O(x) &= p^r, r \leq n_1 \\ x^{p^{n_1}} &= x^{p^r} \cdot p^{n_1-r} \\ &= \left(x^{p^r}\right)^{p^{n_1-r}} = e\end{aligned}$$

Let $A_1 = \langle a_1 \rangle$ the cyclic subgroup generated by a_1 .

$$O(A_1) = p^{n_1}$$

$$A_1 \neq G$$

Consider the element of maximum order G/A_1

Let $A_1 b_2$ be the element in G/A_1 of maximum order, say p^{n_2} .

$$\begin{aligned}O(A_1 b_2) &= p^{n_2} \\ (A_1 x)^{p^{n_2}} &= A_1 \quad (\forall x \in G)\end{aligned}$$

$$b_2^{p^{n_1}} = e$$

$$(A_1 b_2)^{p^{n_1}} = A_1 b_2^{p^{n_1}} = A_1$$

$$\Rightarrow p^{n_2}/p^{n_1} \Rightarrow n_2 \leq n_1$$

$$(A_1 b_2)^{p^{n_2}} = A_1$$

$$\Rightarrow A_1 b_2^{p^{n_2}} = A_1$$

$$\Rightarrow b_2^{p^{n_2}} \in A_1 = \langle a_1 \rangle$$

$$\Rightarrow b_2^{p^{n_2}} = a_1^i$$

$$\left(b_2^{p^{n_2}}\right)^{p^{n_1-n_2}} = \left(a_1^i\right)^{p^{n_1-n_2}}$$

$$b_2^{p^{n_1}} = a_1^{i p^{n_1-n_2}}$$

$$e = a_1^{i p^{n_1-n_2}}$$

$$\Rightarrow O(a_1) = p^{n_1} \Rightarrow p^{n_1}/i p^{n_1-n_2}$$

$$\Rightarrow p^{n_1} \cdot p^{n_2}/i p^{n_1-n_2}$$

$$\Rightarrow p^{n_2}/i$$

Let $i = jP^{n_2}$

$\circ \quad b_2^{P^{n_2}} = a_1^i$

$\Rightarrow b_2^{P^{n_2}} = a_1^{jP^{n_2}}$

$\Rightarrow (b_2^{P^{n_2}})(a_1^{-j})^{P^{n_2}} = e \Rightarrow (b_2 a_1^{-j})^{P^{n_2}} = e$

Let $a_2 = b_2 a_1^{-j}$

Then $a_2^{P^{n_2}} = e$

Let $A_2 = \langle a_2 \rangle$ be the cyclic subgroup generated by a_2 .

$O(A_2) = P^{n_2}$

Let $x \in A_1 \cap A_2$

$x = a_2^t \in A_1$
 $= (b_2 a_1^{-j})^t \in A_1$
 $= b_2^t a_1^{-jt} \in A_1$

$\circ \quad b_2^t \in A_1$

$\circ \quad A_1 b_2^t = A_1$

$\Rightarrow (A_1 b_2)^t = A_1$

Since $O(A_1 b_2) = P^{n_2}$

$\Rightarrow P^{n_2}/t$

$t = KP^{n_2} \quad \circ \quad x = a_2^t$
 $x = a_2^{KP^{n_2}}$

$x = \left(a_2^{P^{n_2}} \right)^K = e$

$\circ \quad A_1 \cap A_2 = \{e\}$

If $G = A_1 A_2$

The proof all abelian.

If $G \neq A_1 A_2$

Consider the element of maximum orders in $G/A_1 A_2$, say $A_1 A_2 b_3$.

Let $O(A_1 A_2 b_3) = P^{n_3}$

If $(A_1 b_3)^{P^{n_2}} = A_1$

$\Rightarrow A_1 b_3^{P^{n_2}} = A_1$

$\Rightarrow b_3^{P^{n_2}} \in A_1 \subset A_1 A_2$

$A_1 A_2 b_3^{P^{n_2}} = A_1 A_2$

$(A_1 A_2 b_3)^{P^{n_2}} = A_1 A_2$

$\circ \circ \quad P^{n_3} / P^{n_3} = n_3 \leq n_2 \leq n_1$

$(A_1 A_2 b_3)^{P^{n_3}} = A_1 A_2$

Hence the $b_3^{P^{n_3}} \in A_1 A_2$

$b_3^{P^{n_3}} = a_1^{i_1} \cdot a_2^{i_2}$

$\left(b_3^{P^{n_3}} \right)^{P^{n_1-n_3}} = a_1^{i_1 P^{n_1-n_3}} \cdot a_2^{i_2 P^{n_1-n_3}}$

$\Rightarrow b_3^{P^{n_1}} = a_1^{i_1 P^{n_1-n_3}} \cdot a_2^{i_2 P^{n_1-n_3}}$

$\Rightarrow e = a_1^{i_1 P^{n_1-n_3}} \cdot a_2^{i_2 P^{n_1-n_3}}$

$\Rightarrow a_1^{i_1 P^{n_1-n_3}} = a_2^{-i_2 P^{n_1-n_3}} = \{e\} \in A_1 \cap A_2 = \{e\}$

$\Rightarrow a_1^{i_1 P^{n_1-n_3}} = e$

$\Rightarrow O(a_1) = P^{n_1}$

$\Rightarrow P^{n_1} / i_1 P^{n_1-n_3}$

$\Rightarrow P^{n_3} / i_1$

$\Rightarrow i_1 = j_1 P^{n_3}$

$b_3^{P^{n_3}} = a_1^{i_1} \cdot a_2^{i_2}$

$\Rightarrow \left(b_3^{P^{n_3}} \right)^{P^{n_2-n_3}} = \left(a_1^{i_1} \right)^{P^{n_2-n_3}} \cdot \left(a_2^{i_2} \right)^{P^{n_2-n_3}}$

$$\Rightarrow b_3^{p^{n_2}} = a_1^{i_1(p^{n_2-n_3})} \cdot a_2^{i_2(p^{n_2-n_3})}$$

$$\Rightarrow b_3^{p^{n_2}} \in A_1 \Rightarrow a_2^{i_2(p^{n_2-n_3})} \in A_1$$

$$\circ \circ \quad p^{n_2} / i_2 p^{n_2-n_3}$$

$$\Rightarrow p^{n_3} / i_2$$

$$\text{Let } i_2 = j_2 p^{n_3}$$

$$b^{p^{n_3}} = a_1^{i_1} \cdot a_2^{i_2}$$

$$\Rightarrow b_3^{p^{n_3}} = a_1^{j_1 p^{n_3}} \cdot a_2^{j_2 p^{n_3}}$$

$$\Rightarrow (b_3^{p^{n_3}}) = a_1^{j_1 p^{n_3}} \cdot a_2^{j_2 p^{n_3}}$$

$$\Rightarrow (b_3 a_1^{-j_1} a_2^{-j_2})^{p^{n_3}} = e$$

$$\text{Let } a_3 = b_3 a_1^{-j_1} a_2^{-j_2}$$

$$(a_3^{p^{n_3}}) = e$$

Let $A_3 = \langle a_3 \rangle$ be the cyclic subgroup generated by a_3 .

$$O(A_3) = p^{n_3}$$

$$\text{Let } x \in A_3 \cap A_1 A_2$$

$$x = a_3^t \in A_1 A_2$$

$$\Rightarrow (b_3 a_1^{-j_1} a_2^{-j_2})^t \in A_1 A_2$$

$$\Rightarrow b_3^t a_1^{-j_1 t} a_2^{-j_2 t} \in A_1 A_2$$

$$\Rightarrow b_3^t \in A_1 A_2$$

$$\Rightarrow A_1 A_2 b_3^t = A_1 A_2$$

$$(A_1 A_2 b_3)^t = A_1 A_2$$

$$O(A_1 A_2 b_3) = p^{n_3}$$

$$\Rightarrow p^{n_3} / t$$

$$\Rightarrow t = r p^{n_3}$$

$$\circ \circ \quad x = a_3^t = a^{r p^{n_3}} = e$$

$$\circ \quad A_3 \cap A_1 A_2 = \{e\}$$

$$\text{If} \quad G = A_1 A_2 A_3$$

Then G is the direct product of A_1, A_2, A_3 .

Otherwise, we consider $G/A_1 A_2 A_3$ to obtain a subgroup $A_4 = (a_4)$ of order p^{n_4} is the $n_4 \leq n_3 \leq n_2 \leq n_1$.

$$A_4 \cap A_1 A_2 A_3 = \{e\}$$

Proceeding like this, we obtain after say K steps subgroup $A_1, A_2, \dots, A_K$ of order $p^{n_1}, p^{n_2}, \dots, p^{n_K}$ with $n_1 \geq n_2 \geq n_3 \geq n_K > 0$.

s.t. $G = A_1 A_2 \dots A_K$ and

$$A_K \cap A_1 A_2 \dots A_{K-1} = \{e\}$$

G is the direct product of its cyclic subgroup $A_1, A_2, \dots, A_K$.

Hence the theorem.

Finite Abelian groups :

Theorem : (Fundamental theorem of finite abelian groups)

Every finite abelian group is the direct product of cyclic subgroups.

Proof :

We first prove the theorems (ii) and (i).

Theorem (ii) :

If G is an abelian group of order P^n where P is a prime, then G can be expressed as a direct product of cyclic subgroup.

Proof :

Already we have the proof of the theorem (ii).

Theorem (i) :

Every finite abelian group is a direct product of its sylow subgroups.

Proof :

Already we have the proof of the theorem (i).

Proof of the theorem :

Let G be a finite abelian group.

Let $O(G) = P_1^{\alpha_1} \cdot P_2^{\alpha_2} \dots P_K^{\alpha_K}$

where $P_1, P_2, \dots, P_K$ are the distinct primes dividing $O(G)$.

By theorem (ii) G is the direct product of its sylow subgroups.

Say $G = P_1 \times P_2 \times \dots \times P_K$

$O(P_i) = P_i^{\alpha_i} \quad [i=1, \dots, K]$

By theorem (i), P_i can be expressed as a direct product of cyclic subgroups for $i = 1, 2, \dots, K$.

∴ G can be expressed as a direct product of its cyclic subgroups.

Hence the fundamental theorem of finite abelian groups.

Definition :

If G is an abelian group of order P^n , P a prime and $G = A_1 \times A_2 \times \dots \times A_K$ where each A_i is cyclic of order p^{n_i} with $n_1 \geq n_2 \geq \dots \geq n_K > 0$, then the integers $n_1, n_2, \dots, n_K$ are called the invariants of G .

Definition :

If G is an abelian group and S is any integer, then $G(S) = \{x \in G / x^S = e\}$.

Lemma :

If G and G^1 are isomorphic, then for every integer S , $G(S)$ is isomorphic to $G^1(S)$ and $H(S)$ is isomorphic to $H^1(S)$.

Proof :

Let ϕ be an isomorphism of G onto G^1 .

$$G(S) = \{x \in G; x^S = e\}$$

$$G^1(S) = \{x^1 \in G^1; (x^1)^S = e^1\}$$

where e^1 is the identity of G^1 .

Let $\phi(x) = x^1 \in G^1(S)$

$$\Rightarrow x^S = e$$

$$\varnothing(x^S) = [\varnothing(x)]^S \quad [\because \varnothing \text{ is a homomorphism}]$$

$$= \varnothing(e) = e^1$$

$$\Rightarrow [\varnothing(x)]^S = e^1$$

$$\Rightarrow \varnothing(x) \in G^1(S)$$

$$\varnothing(G(S)) \subset G^1(S)$$

$$\text{Let } x^1 \in G^1(S)$$

$$(x^1)^S = e^1$$

Since $\varnothing : G \rightarrow G^1$ is onto.

$$\exists x \in G \text{ s.t. } \varnothing(x) = x^1$$

$$[\varnothing(x)]^S = e^1 = \varnothing(e)$$

$$\Rightarrow x^S = e \quad [\because \varnothing \text{ is one-one}]$$

$$\Rightarrow x \in G(S)$$

$$x^1 = \varnothing(x) \in \varnothing(G(S))$$

$$G^1(S) \subset \varnothing(G(S))$$

$$\therefore \varnothing(G(S)) = G^1(S)$$

$\therefore \varnothing$ is an isomorphism of $G(S)$ onto $G^1(S)$.

$$H(S) = \{x^S; x \in G\}$$

$$H^1(S) = \{(x^1)^S, x^1 \in G^1\}$$

To P.T. $\varnothing$ is an isomorphism.

If $H(S)$ onto $H^1(S)$.

$$\text{Let } x \in H(S) \Rightarrow x = a^S \text{ (for some } a \in G)$$

$$\varnothing(x) = \varnothing(a^S) = [\varnothing(a)]^S$$

$$\in H^1(S) \quad [\because \varnothing \text{ is a homomorphism}]$$

$$\varnothing(H(S)) \subset H^1(S)$$

$$\text{Let } x^1 \in H^1(S)$$

$$x^1 = (a^1)^S \text{ where } a^1 \in G^1$$

Since $\varnothing : G \rightarrow G^1$ is onto

$\exists a \in G$ s.t. $\phi(a) = a^1$

$$\begin{aligned} \circ \quad x^1 &= (a^1)^S = [\phi(a)]^S \\ &= \phi(a^S) \quad [\because \phi \text{ is a homomorphism}] \\ &\in \phi(H(S)) \quad [\because a^S \in H(S)] \end{aligned}$$

$$\circ \quad H^1(S) \subset \phi(H(S))$$

$$\circ \quad H^1(S) = \phi(H(S))$$

$\circ \quad \phi$ is an isomorphism of $H(S)$ onto $H^1(S)$.

This proves the theorem.

Lemma :

If G be an abelian group of order P^n . P a prime and if $G = A_1 \times A_2 \times \dots \times A_n$ where each A_i is a cyclic subgroup of order p^{n_i} , $i = 1, 2, \dots, K$ with $n_1 \geq n_2 \geq \dots \geq n_K > 0$ and if m is an integer subgroup $n_r \geq m \geq n_{r+1}$ then $G(P^m) = B_1 \times B_2 \times \dots \times B_r \times A_{r+1} \times \dots \times A_n$ where each B_i is cyclic of order P^m .

$$O(G(P^m)) = P^m \dots P^m \cdot P^{m_{r+1}} \dots P^{m_K}$$

$$= P^u \quad \text{where } u = m_r + \sum_{i=r+1}^K n_i$$

Proof :

$$G(P^m) = \{x \in G; x^{P^m} = e\}$$

$$\text{Let } B_i = (a_i^{P_i - m}) \text{ for } 1 \leq i \leq r$$

$$\text{where } A_i = (a_i) \quad B_i \subset A_i, i = 1, 2, \dots, r$$

$$(a_i^{P^{n_i} - m})^{P^m} = a_i^{P^{n_i}} = e \quad [O(A_i) = O(a_i) = P^{n_i}] \quad \forall i = 1, 2, \dots, r$$

$$O(B_i) = P^m \quad (i = 1, 2, \dots, r)$$

$$a_i^{P^{n_i} - m} \in G(P^n), \quad \forall i = 1, 2, \dots, r$$

$$B_i = (a_i^{P^{n_i} - m}) \subset G(P^n) \quad \forall i = 1, 2, \dots, r$$

For $i \geq r+1$

$$m \geq n_{r+1} \geq n_{r+2} \geq \dots \geq n_K = 0$$

$$\left(a_i^{p^m}\right) = \left(a_i^{p^{n_i}}\right)^{p^{m-n_i}}$$

$$= e$$

$$\Rightarrow G_i \in G(P^m), \quad \forall i \geq r+1$$

$$A_i = (G_i) \subset G(P^m), \quad \forall i \geq r+K$$

∴ $G(P^m)$ contains the subgroups

$$B_1, B_2, \dots, B_r, A_{r+1}, \dots, A_K$$

$$\circ \circ \quad G(P^m) \supset B_1 \times B_2 \times \dots \times B_r \times A_{r+1} \times \dots \times A_K \quad \text{----- (1)}$$

$$\text{Let } x \in G(P^m) \Rightarrow x^{p^m} = e$$

$$x \in G = A_1 \times A_2 \times \dots \times A_K$$

$$\circ \circ \quad x = a_1^{\lambda_1} a_2^{\lambda_2} \dots a_r^{\lambda_r} a_{r+1}^{\lambda_{r+1}} \dots a_K^{\lambda_K}$$

For two integers $\lambda_1, \lambda_2, \dots, \lambda_K$.

$$\text{since } x^{p^m} = e$$

$$\Rightarrow a_1^{\lambda_1 p^m} \cdot a_2^{\lambda_2 p^m} \dots a_K^{\lambda_K p^m} = e \quad [\because G \text{ is abelian}]$$

Every element in G has a unique representation as a product of elements of $A_1, A_2, \dots, A_K$.

$$a_1^{\lambda_1 p^m} = e, a_2^{\lambda_2 p^m} = e, \dots, a_r^{\lambda_r p^m} = e, \dots, a_K^{\lambda_K p^m} = e$$

$$\frac{p^{n_1}}{\lambda_1 p^m}, \frac{p^{n_2}}{\lambda_2 p^m} \dots \frac{p^{n_r}}{\lambda_r p^m}$$

$$\Rightarrow \frac{p^{n_1-m}}{\lambda_1}, \frac{p^{n_2-m}}{\lambda_2} \dots \frac{p^{n_r-m}}{\lambda_r}$$

$$\circ \circ \quad \lambda_1 = \alpha_1 p^{n_1-m}, \lambda_2 = \alpha_2 p^{n_2-m} \dots$$

$$\lambda_r = \alpha_r p^{n_r-m}$$

$$\begin{aligned}
x &= a_1^{\lambda_1} a_2^{\lambda_2} \dots a_r^{\lambda_r} a_{r+1}^{\lambda_{r+1}} \dots a_K^{\lambda_K} \\
x &\in \left(a_1^{p^{n_1-m}} \right)^{\alpha_1} \left(a_2^{p^{n_2-m}} \right)^{\alpha_2} \dots \left(a_K^{p^{n_K-m}} \right)^{\alpha_K} \\
&\in B_1 \times B_2 \times \dots \times B_r \times A_{r+1} \times \dots \times A_K \\
G(P^m) &\subset B_1 \times B_2 \times \dots \times B_r \times A_{r+1} \times \dots \times A_K \quad \text{----- (2)}
\end{aligned}$$

From (1) and (2)

$$G(P^m) = B_1 \times B_2 \times \dots \times B_r \times A_{r+1} \times \dots \times A_K$$

The invariants of $G(P^m)$ are

$$m, m, \dots, m, n_{r+1}, \dots, n_K$$

$$O(G(P^m)) = \frac{p^m \dots p^m}{r \text{ times}} \cdot p^{n_{r+1}} \dots p^{n_K}$$

$$\Rightarrow O(G(P^m)) = p^u \quad \text{where } u = m_r + \sum_{i=r+1}^K n_i$$

This proves the lemma.

Theorem :

Two abelian groups of order P^n are isomorphic if and only if they have the same invariants.

Proof :

Suppose G, G^1 are finite abelian groups of order P^n . Let G and G^1 be isomorphic and α be an isomorphism from G and G^1 .

$$\text{Let } G = A_1 \times A_2 \times \dots \times A_K$$

$$A_i = \langle a_i \rangle$$

$$O(A_i) = p^{n_i}$$

Since α is an isomorphism

$$\alpha(A_i) \text{ is normal subgroup of } G^1 \quad [\forall i=1, \dots, K]$$

$$\alpha(A_1) \dots \alpha(A_K) \text{ is a subgroup of } G^1.$$

Also

$$g^1 \in G^1 \Rightarrow \exists g \in G \text{ s.t. } \alpha(g) = g^1$$

$$\begin{aligned}
g \in G &\Rightarrow g = x_1, \dots, x_K, \quad x_i \in A_i \\
\Rightarrow g^1 &= \emptyset(g) = \emptyset(x_1) \dots \emptyset(x_K) \\
&\in \emptyset(A_1) \dots \emptyset(A_K) \\
\Rightarrow G^1 &\subset \emptyset(A_1) \dots \emptyset(A_K) \\
\Rightarrow G^1 &= \emptyset(A_1) \dots \emptyset(A_K)
\end{aligned}$$

Also

$$\emptyset(A_1) \cap \emptyset(A_2) \dots \emptyset(A_K) = \{e^1\} \quad [e^1 = \text{identity of } G^1]$$

$$\text{As } x \in \emptyset(A_1), x \in \emptyset(A_2) \dots x \in \emptyset(A_K)$$

$$\Rightarrow x = \emptyset(x_1) = \emptyset(x_2) \dots \emptyset(x_K) \quad [x_i \in A_i]$$

$$\Rightarrow \emptyset(x_1) = \emptyset(x_2 \dots x_K)$$

$$\Rightarrow x_1 = x_2 = \dots = x_K$$

$$\Rightarrow x_1^{-1} x_2 \dots x_K = e$$

$$\Rightarrow x_i = e \quad [\forall i]$$

$$\Rightarrow x = e$$

III^{ly} for other intersections,

$$\circ G^1 = \emptyset(A_1) \times \dots \times \emptyset(A_K)$$

$$\text{Since } A = \langle a_i \rangle$$

$$\emptyset(A_i) = \langle \emptyset(a_i) \rangle$$

$$\circ O(\emptyset(A_i)) = O(\emptyset(a_i)) = O(a_i) \quad \forall i$$

$$= p^{n_i} \quad \forall i$$

Thus, G and G^1 have same invariants.

Conversely,

Suppose G and G^1 have same invariants

$$\text{Let } G = A_1 \times \dots \times A_K, \quad A_i = \langle a_i \rangle$$

$$\text{Then } G^1 = B_1 \times \dots \times B_K, \quad B_i = \langle b_i \rangle$$

$$O(A_i) = O(B_i)$$

$\circ G$ and G^1 have same invariants.

Any two cyclic groups of same order are isomorphic. A_i and B_i are isomorphic $[\forall i]$

$\circ A_1 \times \dots \times A_K = G$ and $B_1 \times B_2 \times \dots \times B_K = G^1$ are isomorphic.

This proves the theorem.

Theorem :

The number of non-isomorphic abelian groups of order P^n , P a prime, equals the number of partitions of n .

Proof :

If G is a finite abelian group of order P^n .

Then $G = A_1 \times A_2 \times \dots \times A_K$

$$A_i = \langle a_i \rangle, O(A_i) = P^{n_i}$$

$$O(G) = O(A_1) \dots O(A_K)$$

$$\Rightarrow P^n = P^{n_1} \dots P^{n_K} = P^{n_1 + n_2 + \dots + n_K}$$

$$\Rightarrow n = n_1 + \dots + n_K, n_1 \geq n_2 \geq \dots \geq n_K > 0 \text{ is a partition of } n.$$

Conversely,

Consider any partition of n .

Let $n = n_1 + \dots + n_K, n_1 \geq n_2 \geq \dots \geq n_K > 0$ be a partition of n .

Let A_i be a cyclic group of order P^{n_i} $[\forall i]$

Let $G = A_1 \times \dots \times A_K$

Then G is an abelian group of order $P^{n_1 + n_2 + \dots + n_K} = P^n$.

Let $x =$ set of all non-isomorphic abelian groups of order P^n .

$y =$ set of all partitions of n .

Define $\emptyset : x \rightarrow y$ as follows.

Let $G \in x$. Let $G = A_1 \times \dots \times A_K$.

$$A_i = \langle a_i \rangle, O(A_i) = P^{n_i}$$

$$\text{Let } O(G) = n_1 + \dots + n_K = n$$

Clearly, $\emptyset$ is well - defined.

Also

$$O(G) = O(G')$$

$$\Rightarrow n_1 + \dots + n_K = m_1 + \dots + m_\ell = n$$

$$\Rightarrow K = \ell, n_i = m_i, \forall i$$

$\Rightarrow G$ and G^1 have same invariants.

$$\Rightarrow G = G^1$$

$\Rightarrow \emptyset$ is 1-1.

Let $n = n_1 + \dots + n_K$, $n_1 \geq n_2 \geq \dots \geq n_K > 0$ be a partition of n .

Then
$$G = A_1 \times A_2 \times \dots \times A_K$$

$$A_i = \langle a_i \rangle, O(A_i) = P^{n_i} \text{ is an abelian group of order } P^{n_i}.$$

$$\circ O(G) = n_1 + \dots + n_K$$

$\circ \emptyset$ is onto.

$$\circ O(x) = O(y)$$

This proves the theorem.

Corollary :

The number of non-isomorphic abelian groups of order $P_1^{\alpha_1} \dots P_K^{\alpha_K}$ where the P_i are distinct primes and where each $\alpha_i > 0$ is $P(\alpha_1)P(\alpha_2) \dots P(\alpha_K)$.

Proof :

If G is an abelian group of order $P_1^{\alpha_1} P_2^{\alpha_2} \dots P_K^{\alpha_K}$.

Then G can be expressed as a direct product of its sylow subgroups say $P_1, P_2, \dots, P_K$.

Where $O(P_i) = P_i^{\alpha_i}$ ($i=1, \dots, K$)

If G^1 is a group isomorphic to G , the sylow subgroups $P_1^1, P_2^1, \dots, P_K^1$ of G^1 are isomorphic to $P_1, P_2, \dots, P_K$.

Invariants of $P_i = \text{Invariants of } P_i^1 \quad (i=1, \dots, K)$

Number of non-isomorphic abelian groups of order.

$$P_i^{\alpha_i} = P(\alpha_i) \quad (i = 1, \dots, K)$$

Number of ways of choosing P_i is $P(\alpha_i)$ [$i=1, \dots, K$]

$\circ$ Number of non-isomorphic abelian groups of order

$$P_1^{\alpha_1} P_2^{\alpha_2} \dots P_K^{\alpha_K} \text{ is } P(\alpha_1) P(\alpha_2) \dots P(\alpha_K)$$

This proves the proof.

Problems :

- 1) Find all abelian groups of order $2^3 \times 3^4 \times 5$.

Solution :

Let G be an abelian group of order $2^3 \times 3^4 \times 5$.

Then $G = A \times B \times C$

where $O(A) = 2^3$, $O(B) = 3^4$, $O(C) = 5^1$

A can be of the following types:

- 1) A is cyclic of order 2^3
- 2) $A = A_1 \times A_2$ where A_1, A_2 are Cyclic
 $O(A_1) = 2^2$, $O(A_2) = 2^1$
- 3) $A = A_1 \times A_2 \times A_3$ where A_1, A_2, A_3 are cyclic of order 2^1 .

$$\begin{bmatrix} 3 = 3 \\ 3 = 2 + 1 \\ 3 = 1 + 1 + 1 \end{bmatrix}$$

B can be of the following types :

- 1) B is cyclic of order 3^4
- 2) $B = B_1 \times B_2$ where B_1, B_2 are Cyclic
 $O(B_1) = 3^3$, $O(B_2) = 3^1$
- 3) $B = B_1 \times B_2$ where B_1, B_2 are cyclic
 $O(B_1) = 3^2$, $O(B_2) = 3^2$
- 4) $B = B_1 \times B_2 \times B_3$ where B_1, B_2, B_3 are cyclic
 $O(B_1) = 3^2$, $O(B_2) = O(B_3) = 3^1$.
- 5) $B = B_1 \times B_2 \times B_3 \times B_4$ where B_1, B_2, B_3, B_4 are cyclic of order 3^1 .

$$\begin{bmatrix} 4 = 4 \\ 4 = 3 + 1 \\ 4 = 2 + 2 \\ 4 = 2 + 1 + 1 \\ 4 = 1 + 1 + 1 + 1 \end{bmatrix}$$

Exercise :

- 1) Find the abelian groups of order $2^4 \cdot 3^4$.
- 2) Find all finite abelian groups of order 7^5 .

Proof :

Number of non-isomorphic abelian.

Groups of order $7^5 = P(5) = 7$.

If G is an abelian group of order 7^5 , then G can be of the following types.

- 1) G is cyclic of order 7^5 .
- 2) $G = A \times B$ where A, B are cyclic
 $O(A) = 7^4, O(B) = 7^1$.
- 3) $G = A \times B$ where A, B are cyclic
 $O(A) = 7^3, O(B) = 7^2$.
- 4) $G = A \times B \times C$ where A, B, C are cyclic
 $O(A) = 7^3, O(B) = 7^1, O(C) = 7^1$

(or)

$$O(B) = O(C) = 7^1.$$

- 5) $G = A \times B \times C$ where A, B, C are cyclic
 $O(A) = 7^2, O(B) = 7^2, O(C) = 7^1$

(or)

$$O(A) = O(B) = 7^2.$$

- 6) $G = A \times B \times C \times D$ where A, B, C, D are cyclic.
 $O(A) = 7^2, O(B) = O(C) = O(D) = 7^1$

- 7) $G = A \times B \times C \times D \times E$ where A, B, C, D are cyclic
 $O(A) = O(B) = O(C) = O(D) = O(E) = 7^1$.

Exercise :

Find all finite abelian groups of order

- 1) 2^6 , 2) 11^6

Permutation Groups :

Every group can be represented isomorphically as a subgroup of $A(S)$ for some set S , and in particular, a finite group G can be represented as a subgroup of S_n , for some n , where S_n is the symmetric group of degree n or the permutation group on n symbols.

Definition :

An element $\sigma \in S_n$ is called a transposition if there exist two symbols i and j such that

$\sigma(i) = j, \sigma(j) = i, \sigma(K) = K, K \neq i, j$ we use the notation (i, j) to denote such a transposition.

Definition :

An element $\sigma \in S_n$ is called a cycle of order r if there exist r symbols $i_1, i_2, \dots, i_r$ such that

$$\sigma(i_1) = i_2, \sigma(i_2) = i_3, \dots, \sigma(i_{r-1}) = i_r, \sigma(i_r) = i_1$$

and

$$\sigma(j) = j \text{ for all } j \neq i_1, i_2, \dots, i_r.$$

We use the notation $(i_1, i_2, \dots, i_r)$ to denote such an r -cycle.

We show that every permutation can be written as a product of cycles and transpositions.

Consider the following element $\sigma \in S_8$, where

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 5 & 8 & 7 & 6 & 1 & 4 \end{pmatrix}$$

Suppose we want to test whether σ is a cycle or not. Now σ maps $1 \rightarrow 2, 2 \rightarrow 3, 3 \rightarrow 5, 5 \rightarrow 7, 7 \rightarrow 1$. Thus σ is the same as the cycle $(1 \ 2 \ 3 \ 5 \ 7)$, so far as the effects on these symbols are concerned out of the remaining symbols. 6 is fixed by σ , whereas 4 and 8 are interchanged. Thus the effect of $(1 \ 2 \ 3 \ 5 \ 7) (4 \ 8)$ and σ is the same on all symbols. ie) $\sigma = (1 \ 2 \ 3 \ 5 \ 7) (4 \ 8)$. Thus we have expressed σ as a product of two cycles, one cycle being of length 5 and the other of length 2, and the two cycles have no symbols in common (disjoint cycles).

Theorem :

Every permutation in S_n can be uniquely expressed as a product of its disjoint cycles.

Proof :

Let θ be a permutation in S_n . The cycle of θ will be of the form,

$$(a, a\theta, a\theta^2, \dots)$$

$$(b, b\theta, b\theta^2, \dots)$$

$$(c, c\theta, c\theta^2, \dots)$$

These cycles are all disjoint.

Each element belongs to one and only one cycle.

Let ℓ be the product of these disjoint cycles. The effect of ℓ on a is calculated by considering the cycle to which a belongs.

$$\circ a^\ell = a\theta.$$

This is true for every symbol.

$$\circ \ell = \theta, \text{ i.e.) } \theta \text{ is the product of its disjoint cycles.}$$

This representation is unique excepting for the order of the factor, because each symbol belongs to only one cyclic.

Lemma :

Every permutation can be expressed as a product of two cycles or transposition.

Proof :

Every permutation can be expressed as a product of its disjoint cycles.

Every cycle $(a_1, a_2, \dots, a_r) = (a_1, a_2)(a_1, a_3) \dots (a_1, a_r)$ can be expressed as a product of transposition.

A Every permutation is a product of transposition.

Definition :

σ is called an even permutation if $\epsilon\sigma = +1$ and it is called an odd permutation if $\epsilon\sigma = -1$.

Thus an even (odd) permutation is a permutation which can be expressed as a product of even (odd) number of transpositions.

Lemma :

The set A_n of all even permutations forms a subgroup of S_n and is a normal subgroup of S_n .

Proof :

Consider the group homomorphism

$$\epsilon : S_n \rightarrow \{1, -1\} \text{ defined by } \sigma \rightarrow \epsilon\sigma.$$

$$\text{Then } \text{Ker } \epsilon = \{\sigma / \epsilon\sigma = 1\} = A_n.$$

Hence A_n is a normal subgroup of S_n .

Remark :

The group A_n is called the alternating group on n symbols.

Theorem :

The set of even permutation in S_n form a normal subgroup of index 2.

Proof :

Let $W = \{1, -1\}$ to be a group under multiplication.

Define a mapping $\phi : S_n \rightarrow W$ as follows.

$\phi(\sigma) = 1$ if σ is even

$\phi(\sigma) = -1$ if σ is odd

ϕ is a mapping of S_n onto W .

Let $\sigma_1, \sigma_2 \in S_n$.

Case (i) :

If σ_1, σ_2 are both even.

σ_1, σ_2 is even.

$$\phi(\sigma_1, \sigma_2) = 1 \Rightarrow 1 \times 1 = \phi(\sigma_1)\phi(\sigma_2)$$

Case (ii) :

If σ_1 is even, σ_2 is odd

σ_1, σ_2 is odd

$$\phi(\sigma_1, \sigma_2) = -1$$

$$\begin{aligned} &= 1 \times -1 \\ &= \phi(\sigma_1)\phi(\sigma_2) \end{aligned}$$

Case (iii) :

III^{ly} if σ_1 is odd, σ_2 is even

σ_1, σ_2 is odd

$$\phi(\sigma_1, \sigma_2) = \phi(\sigma_1)\phi(\sigma_2)$$

Case (iv) :

If σ_1 and σ_2 are both odd.

$\sigma_1 \sigma_2$ is even.

$$\begin{aligned}\emptyset(\sigma_1 \sigma_2) &= 1 \Rightarrow (-1) \times (-1) \\ &= \emptyset(\sigma_1) \emptyset(\sigma_2)\end{aligned}$$

∴ $\emptyset$ is a homomorphism of S_n onto W .

$$\begin{aligned}\text{Kernal of } \emptyset &= \{\sigma; \emptyset(\sigma) = 1\} \\ &= \text{set of even permutation} = A_n.\end{aligned}$$

∴ A_n is a normal subgroup of S_n .

By the first law of homomorphism,

$$\begin{aligned}\frac{S_n}{A_n} &\approx W \\ O\left(\frac{S_n}{A_n}\right) &= O(W) = 2 \\ i(A_n) &= 2\end{aligned}$$

This proves the theorem.

Theorem :

For $n \geq 3$, A_n is generated by its 3 cycle.

Proof :

Every 3 cycle $(a, b, c) \in A_n$ is an even permutation.

∴ All the 3 cycles belong to A_n .

Let $\sigma \in A_n$.

∴ σ can be expressed as a product of an even number of transpositions.

Let $\sigma = t_1, t_2, \dots, t_{2n}$.

where $t_1, t_2, \dots, t_{2n}$ are transpositions.

$$\sigma = (t_1 t_2) (t_3 t_4) \dots (t_{2i-1} t_{2i})$$

Consider

$$t_{2i-1} t_{2i} = (ab) (cd)$$

If $(ab) = (cd)$

$(ab)(cd) = \text{identity}$

If $(ab) \neq (cd)$

If one of the symbols in (a, b)

Consider with one of the symbols in (c, d) say $a = c$.

Then $(ab)(cd)$

$$\begin{aligned} t_{2i-1} \cdot t_{2i} &= (ab)(cd) \Rightarrow (ab)(ad) \\ &= (a b d) \end{aligned}$$

If a, b, c, d are all distinct.

$$\begin{aligned} t_{2i-1} \cdot t_{2i} &= (ab)(cd) \\ &= (a b d)(a c d) \end{aligned}$$

$t_{2i-1} \cdot t_{2i}$ is either a 3 cycle or is a product of two 3 cycles.

$$\begin{aligned} \sigma &= (t_1 t_2)(t_3 t_4) \dots (t_{2i-1} t_{2i}) \dots (t_{2n-1} t_{2n}) \\ &= \text{Product of 3 cycles } A_n \text{ is generated by its 3 cycle.} \end{aligned}$$

Theorem :

For $n \geq 3$, if N is a normal subgroup of A_n containing even a single 3 cycle, $N = A_n$.

Proof :

Let N be a normal subgroup of A_n containing a 3 cycle say $(a b c)$

$$\begin{aligned} (a c b) &= (a b c)^{-1} \\ &= [(a b c)]^2 \in N \quad [\because N \text{ is a subgroup of } G] \end{aligned}$$

Let $(a^1 b^1 c^1)$ be any other 3 cycle different from $(a b c)$.

If a^1, b^1, c^1 are distinct from a, b, c

Consider $\sigma = (a a^1)(b b^1)(c c^1)(a c) \in A_n$.

$(a b c) \in N$ and N is a normal subgroup of A_n .

$$\sigma^{-1}(a b c) \sigma \in N$$

$$(a^1 b^1 c^1) \in N$$

If one of the symbols of $(a\ b\ c)$ consider with one of the symbols of a^1, b^1, c^1 say.

Without loss of generality.

$$b = b^1$$

Consider $\sigma = (aa^1)(cc^1) \in A_n$.

$$(a\ b\ c) \in N \quad [\because N \text{ is a normal subgroup of } A_n]$$

$$\sigma^{-1}(a\ b\ c)\sigma \in N$$

$$(a^1\ b^1\ c^1) \in N$$

If two of the symbols of $(a\ b\ c)$ consider with two of the symbols of $(a^1\ b^1\ c^1)$.

Without loss of generality.

Let $\sigma = (a\ a^1)(b\ c) \in A_n$.

$$(a^1\ b^1\ c^1) \in N$$

If two of the symbols of $(a\ b\ c)$ consider with two of the symbols of $(a^1\ b^1\ c^1)$.

Without loss of generality.

Without loss of generality.

Let $\sigma = (a\ a^1)(b\ c) \in A_n$.

$$(a\ b\ c) \in N \text{ and } N \text{ is a normal subgroup of } A_n.$$

$$\therefore \sigma^{-1}(a\ b\ c)\sigma \in N$$

$$(a^1\ c^1\ b^1) \in N$$

$$\therefore (a^1\ b^1\ c^1) = (a^1\ c^1\ b^1)^{-1} \in N$$

$\therefore N$ contains all the 3 cycles.

Since the 3 cycles generated by A_n .

$$\therefore A_n = N.$$

Lemma :

The converse of langrange theorem is not true.

Proof :

$$O(\text{subgroup}) / O(\text{group})$$

[By langrange's theorem]

$$\therefore G = \{A_n\}$$

$$O(G) = 12$$

6/12. If H is a subgroup of A_n .

If A_n of order 6.

$$i(H) = 2$$

H is a normal subgroup of A_n of order 6.

H has of contain atleast one 3 cycles.

$$\therefore H = A_n$$

$\therefore A_n$ doesnot contain a subgroup of order 6.

Problems :

1) Compute $a^{-1} b a$ where $a = (1 \ 3 \ 5) (1 \ 2)$, $b = (1 \ 5 \ 7 \ 9)$.

Solution :

$$\text{We have } a = (1 \ 3 \ 5) (1 \ 2)$$

$$= (1 \ 2 \ 3 \ 5)$$

$$\Rightarrow a^{-1} = (5 \ 3 \ 2 \ 1)$$

Thus

$$a^{-1} b a = (5 \ 3 \ 2 \ 1) (1 \ 5 \ 7 \ 9) (1 \ 2 \ 3 \ 5)$$

$$a^{-1} b a = (3 \ 7 \ 9 \ 5)$$

Theorem :

Let $\sigma = (a_1 \dots a_{n_e}) \dots (b_1 \dots b_{n_k})$ be a permutation of a finite set S, written as product of disjoint cycles. Let $O(S) = n$ and $n_1 + \dots + n_k = n$.

$$\text{Then } \theta \sigma \theta^{-1} = (\theta(a_1) \dots \theta(a_{n_e})) \dots (\theta(b_1) \dots \theta(b_{n_k})) \quad \forall \theta \in S_n$$

Proof :

$$\text{Let } S = \{a_1, \dots, a_{n_1}, \dots, b_1, \dots, b_{n_k}\}$$

Then

$$\theta(S) = \{\theta(a_1), \dots, \theta(a_{n_e}), \dots, \theta(b_1), \dots, \theta(b_{n_k})\}$$

Since $\theta: S \rightarrow S$ is 1-1 all elements in $\theta(S)$ are distinct.

Also θ is onto $\Rightarrow \theta(S) = S$.

Now

$$= (\theta\sigma\theta^{-1})(\theta x_i)$$

$$= (\theta\sigma)(\theta^{-1}\theta x_i)$$

$$= (\theta\sigma)(x_i)$$

$$= \theta(\sigma(x_i))$$

$$= \theta(x_{i+1})$$

$\therefore \theta\sigma\theta^{-1}$ takes any element $\theta(x_i)$ of $\theta(S) = S$ to $\theta(x_{i+1})$ and so does the mapping.

Proof:

$$(\theta a_1 \dots \theta a_{n_e}) \dots (\theta b_1 \dots \theta b_{n_k})$$

$$\therefore \theta\sigma\theta^{-1} = (\theta a_1 \dots \theta a_{n_e}) \dots (\theta b_1 \dots \theta b_{n_k})$$

This proves the theorem.

Problem :

Show that there does not exist a permutation θ of $S = \{1, 2, \dots, 8\}$ such that

$$\theta(1\ 2\ 3)\theta^{-1} = (1\ 3)(5\ 7\ 8)$$

Solution :

Now

$$\theta(1\ 2\ 3)\theta^{-1} = (\theta(1)\ \theta(2)\ \theta(3)) \text{ and it does not have cycle of length 2 while}$$

$$(1\ 3)(5\ 7\ 8) \text{ has a cycle of length 2.}$$

So, there does not exist θ such that

$$\theta(1\ 2\ 3)\theta^{-1} = (1\ 3)(5\ 7\ 8)$$

Remark :

Since identity is even permutation, all members of $A(S)$ cannot be odd permutation.

Problem :

Find orbits and cycles of the permutation

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 3 & 1 & 2 \end{pmatrix}$$

Solution :

Let $f(1) = 6, f^2(1) = 2, f^3(1) = 5, f^4(1) = 1$

Thus

$(1\ 6\ 2\ 5)$ is a cycle and $\{1, 6, 2, 5\}$ is orbit of 1, 6, 2, 5.

If we consider

$$f(3) = 4, f^2(3) = 3$$

Thus $(3\ 4)$ is cycle and $\{3, 4\}$ is orbit of 3 and 4.

Definition :

If $\sigma \in S_n$, then the signature of σ is defined as the product $\prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i}$

The signature of σ is denoted by the symbol $\epsilon \sigma$. We note that the value of $\epsilon \sigma$ is either +1 or -1.

For instance if

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}, \text{ then}$$

$$\epsilon \sigma = \frac{(2-3)(2-1)(2-4)(3-1)(3-4)(1-4)}{(1-2)(1-3)(1-4)(2-3)(2-4)(3-4)}$$

$$\epsilon \sigma = +1$$

CONJUGATE CLASSES AND CLASS EQUATION

Definition :

If $a, b \in G$ then b is said to be a conjugate of a in G if there exists an element $c \in G$ such that $b = c^{-1}ac$.

For this, $a \sim b$ and shall refer to this relation as conjugacy.

Lemma :

Conjugacy is an equivalence relation on G .

Proof :

we must prove that,

- 1) $a \sim a$;
- 2) $a \sim b \Rightarrow b \sim a$;
- 3) $a \sim b, b \sim c \Rightarrow a \sim c \forall a, b, c \in G$

1) For every $a \in G$,

$$\begin{aligned} a &= e^{-1} a e \\ &\Rightarrow a \sim a \end{aligned}$$

Conjugacy is reflexive.

2) If $a \sim b$, then $b = c^{-1}ac$ for some $c \in G$

$$\begin{aligned} a &= cb c^{-1} \\ &= (c^{-1})^{-1} b c^{-1} \\ &\Rightarrow b \sim a \end{aligned}$$

conjugacy is symmetric.

3) If $a \sim b$ and $b \sim c$

$$a \sim b \Rightarrow b = x^{-1}ax \quad (\text{for some } x \in G)$$

$$b \sim c \Rightarrow c = y^{-1}by \quad (\text{for some } y \in G)$$

$$c = y^{-1}(x^{-1}ax)y$$

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

$$\Rightarrow a \sim c$$

∴ Conjugacy is transitive.

Conjugacy defines an equivalence relation in G .

The partitions G into disjoint equivalence classes.

These equivalence classes are called the conjugate classes of G .

The conjugate class of a denoted by

$$c(a) = \{b \mid a \sim b\}$$

$$= \{x^{-1}ax; x \in G\}$$

$$O(c(a)) = c_a$$

$$O(G) = \sum O(c(a))$$

$$= \sum c_a$$

where the summation ranges over one element from each conjugate class.

$$N(a) = \{x \in G; ax = xa\}$$

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

$$N(a) = G \text{ iff } a \in \text{centre of } G.$$

If G is finite $O(N(a)) = O(G)$ if $a \in \text{centre of } G$.

Definition :

The equivalence classes under the relation $b \sim a$ iff $b = xax^{-1}$, $x \in G$ are called conjugate classes.

Remark :

We denote by $C(a)$, the conjugate class containing a .

Lemma :

Let G be a group and $a \in G$. Then $c(a) = \{a\}$ if and only if $a \in Z(G)$

Proof :

Since $a \in c(a)$, for any $b \in G$,

$$bab^{-1} \in c(a)$$

$$\circ \quad c(a) = \{a\},$$

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

$$\circ \quad ba = ab$$

Thus $a \in z(G)$

conversely,

Let $a \in z(G)$ and $b \in c(a)$.

then $b = xax^{-1}$ for some $x \in G$

$$\circ \quad a \in z(G)$$

$$b = xax^{-1} = axx^{-1} = ae = a$$

$$\circ \quad c(a) = \{a\}$$

Defintion :

$C(a)$ is called a trivial conjugate class if it contains just one element a .

Theorem :

If G is a finite group, then $C_a = O(G)/O(N(a))$ in other words, the number of elements conjugate to $a \in G$ is the index of the normalizer of $a \in G$

Proof :

Define a mapping $\emptyset: G/N(a) \rightarrow C_a$ as follows.

$$\emptyset(N(a)x) = x^{-1}ax$$

If $yN(a)x, y = nx$ where $n \in N(a)$

$$\circ \quad na = an$$

$$y^{-1}ay = (nx)^{-1}a(nx)$$

$$= x^{-1}n^{-1}anx$$

$$= x^{-1}(n^{-1}an)x$$

$$(or) \quad x^{-1}(n^{-1}na)x$$

$$y^{-1}ay = x^{-1}ax \quad [\circ n \in N(a)]$$

The mapping $\emptyset$ is well defined.

If $\emptyset(N(a)x) = \emptyset(N(a)y)$

$$\Rightarrow x^{-1}ax = y^{-1}ay.$$

Premultiply by y and postmultiply by x .

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

$$\Rightarrow yx^{-1} = n \in N(a)$$

$$\Rightarrow y = nx \in N(a)x$$

$$\circledast N(a)y = N(a)x$$

$\Rightarrow \emptyset$ is one-one.

Any element of C_a is of the form $x^{-1}ax$ for some $x \in G$

$$x^{-1}ax = \emptyset(N(a)x)$$

$\circledast \emptyset$ is onto.

$\circledast \emptyset$ is a one-one correspondence between $G/N(a)$ and C_a .

$$O\left(\frac{G}{N(a)}\right) = O(C_a)$$

$$\Rightarrow C_a = i_G(N(a)). \text{ This proves the thm.}$$

Class Equation of G :

Theorem :

Let G be a finite group, $a \in G$

$$\text{then } O(c/(a)) = \frac{O(G)}{O(N(a))}$$

Proof :

Since $N(a) \leq G$, G can be written as union of disjoint right cosets of $N(a)$ in G .

$$\text{Let } G = \bigcup_{i=1}^t N(a)x_i \quad [t \leq n = O(G)]$$

$$\text{Let } S = \{x_1^{-1}ax_1, \dots, x_i^{-1}ax_i\}$$

suppose

$$x_i^{-1}ax_i = x_j^{-1}ax_j \quad \text{for } i \neq j$$

Remark :

then

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

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

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

This is $a \Rightarrow \Leftarrow$

$\therefore$ All elements in s are distinct

ie.) $O(S) = t$

Also

$$O(G) = t.O(N(a))$$

$$\therefore \frac{O(G)}{O(N(a))} = t = O(S)$$

we show that $s = \text{cl}(a)$

Let $s \in S$ then $s = x_i^{-1} a x_i$, for some i , $1 \leq i \leq n$

$\Rightarrow s$ is conjugate of a .

$\Rightarrow s \in \text{cl}(a) \Rightarrow S \subseteq \text{Cl}(a)$

Again

$$x \in \text{Cl}(a) \Rightarrow x = g^{-1} a g, g \in G$$

$$g \in G \Rightarrow g \in N(a) x_i \text{ for some } i, 1 \leq i \leq n$$

$$\Rightarrow g = y x_i, y \in N(a)$$

Thus

$$x = x_i^{-1} y^{-1} a y x_i$$

$$= x_i^{-1} a x_i \text{ as } y a = a y$$

$$\Rightarrow x \in s$$

$$\text{cl}(a) \subseteq S \Rightarrow S = \text{Cl}(a)$$

(or)

$$O(\text{Cl}(a)) = O(S) = \frac{O(G)}{O(N(a))}$$

Remark :

Since

$$\begin{aligned} G &= \bigcup_{a \in G} (Cl(a)) \\ O(G) &= \sum_{a \in Z(G)} O(Cl(a)) \\ &= \sum_{a \in Z(G)} O(Cl(a)) + \sum_{a \notin Z(G)} O(Cl(a)) \\ &= Z(G) + \sum_{a \notin Z(G)} O(Cl(a)) \end{aligned}$$

By

$$O(Cl(a)) = 1 \Leftrightarrow a \in Z(G)$$

$$\circ \quad O(G) = O(Z(G)) + \sum_{a \notin Z(G)} O(Cl(a))$$

$$\circ \quad O(G) = O(Z(G)) + \sum_{a \notin Z(G)} \frac{O(G)}{O(N(a))}$$

This equation is called class equation of G .

Sublemma :

$a \in Z$ iff $N(a) = G$. If G is finite $a \in Z$ iff $O(N(a)) = O(G)$.

Proof :

If $a \in Z$, $xa = ax \forall x \in G$ when $N(a) = G$.

Conversely,

$$N(a) = G$$

$$xa = ax \quad \forall x \in G$$

so that $a \in Z$

If G is finite

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

is equivalent to $N(a) = G$

Theorem :

The number of conjugate class of S_n is $p(n)$.

Proof :

Any partition of n is a sequence $n_1 \leq n_2 \leq \dots \leq n_k$ with $n_1 + n_2 + \dots + n_k = n$.

Any permutation $\sigma \in S_n$ can be represented uniquely as a product of disjoint cycles.

Say of length $n_1, n_2, \dots, n_k$ where

$n_1 \leq n_2 \leq \dots \leq n_k$ and $n_1 + n_2 + \dots + n_k = n$

Every permutation thus gives a partition of n .

If $\theta^{-1}\sigma\theta$ is conjugate to σ .

We calculate $\theta^{-1}\sigma\theta$ by replacing each symbol in σ .

By its image under θ .

$\theta^{-1}\sigma\theta$ will also be a product of disjoint cycles of lengths $n_1, n_2, \dots, n_k$ respectively.

The conjugate of σ also gives rise to the same partition of n .

Let $\sigma_1 = (a_1 a_2 \dots a_{n_1})(b_1 b_2 \dots b_{n_2}) \dots (x_1 \dots x_{n_k})$

$\sigma_2 = (\alpha_1 \alpha_2 \dots \alpha_{n_1})(\beta_1 \beta_2 \dots \beta_{n_2}) \dots (\gamma_1 \gamma_2 \dots \gamma_{n_k})$

be two permutation giving rise to be same partition n , namely

$n_1 \leq n_2 \leq \dots \leq n_k$

$n_1 + n_2 + \dots + n_k = n$

Let $\theta = \begin{pmatrix} a_1 \dots a_{n_1} b_1 b_2 \dots b_{n_2} \dots x_1 x_2 \dots x_{n_k} \\ \alpha_1 \dots \alpha_{n_1} \beta_1 \beta_2 \dots \beta_{n_2} \dots \gamma_1 \gamma_2 \dots \gamma_{n_k} \end{pmatrix}$

$\theta^{-1}\sigma_1\theta = \sigma_2$.

Thus σ_1 and σ_2 are conjugate

∴ The number of partition of n = number of conjugate.

2) Finde all the permutation in S_n commuting with (12)

Solution :

Number of elements conjugate to (12) in S_n = Number of 2 cycles in S_n .

$$nc_2 = \frac{n(n-1)}{2}$$

$$= \text{Index of } N_{S_n} \{(1,2)\}$$

$$= \frac{O(S_n)}{O(N(1,2))} = \frac{\angle n}{O(N(1,2))}$$

$$O(N(1,2)) = 2 \angle n - 2 \dots\dots (1)$$

$$\text{Let } T = \{\sigma \in S_n \mid \sigma \text{ leaves 1 and 2 fixed}\}$$

$$\text{Then } O(T) = \angle n - 2$$

Every element of commute with (12)

$$T \subset N \{(12)\}$$

$$\text{If } \ell \in T \quad ((12)\ell) \quad (12)$$

$$= \ell.$$

$$(12) [(12)\ell] = \ell.$$

∴ (12) commutes with every element of the form (12)ℓ, ℓ ∈ T

$$(12)\ell \in N \{(12)\}, \forall \ell \in T$$

$$(12)T \subset N \{(12)\}$$

$$T \cup (12)T$$

$$\subset N \{(12)\}$$

$$O(T \cup (12)T) = O(T) + O\{(12)T\}$$

$$= \angle n - 2 + \angle n - 2 = 2\angle n - 2 \dots\dots\dots (2)$$

From (1),

$$O(N(12)) = 2\angle n - 2$$

$$N \{(12)\} = T \cup (12)T$$

$$N \{(12)\} = \{(12)j\ell\}$$

3) Find all the elements of S_n commuting with (12.....n)

Solution :

Number of elements conjugates of (12.....n) = Number of n cycles in S_n .

$$= \angle n - 1$$

$$\angle n - 1 = i N_{S_n} \{(12.....n)\}$$

$$= \frac{O(S_n)}{O(N\{(12\ldots n)\})} = \frac{\angle n}{O(N\{(12\ldots n)\})}$$

$$O(N\{(12\ldots n)\}) = n$$

The n powers of the n cycles.

$(12\ldots n)$ commute with $(12\ldots n)$ and hence belong to $N\{(12\ldots n)\}$.

$N\{(12\ldots n)\} =$ cyclic subgroup of S_n generated by $(12\ldots n)$

Cauchy's thm for non-abelian group :

Let G be a group and P is a prime dividing $O(G)$. $\exists a \in G, a \neq e, a^P = e$.

Proof :

The proof is by induction on $O(G)$

If $O(G) = 1, G = \{e\}$

The thm is vacuously true.

Induction hypothesis :

Assume the result to be true for all groups whose order $< O(G)$. If G has a subgroup such that $P \nmid O(T)$

$\exists a \in T, a \neq e$ s.t $a^P = e$.

$a \in T \Rightarrow a \in G$

The proof is complete in this case. If P does not divide the order of any proper subgroup of G .

The class equation of G as follows.

$O(G) = \sum \frac{O(G)}{O(N(a))}$ where the summation ranges over one element from each.

Conjugate class of G .

Let z be the centre of G .

$$O(G) = \sum_{a \in Z} \frac{O(G)}{O(N(a))} + \sum_{a \notin Z} \frac{O(G)}{O(N(a))}$$

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

$$O(G) - \sum_{N(a) \neq G} \frac{O(G)}{O(N(a))} = O(z)$$

Given that $P \mid O(G)$

If $N(a) \neq G, P \nmid O(N(a))$

If $N(a) \neq G, P \mid \frac{O(G)}{O(N(a))}$

$$\circ \quad P \mid \sum_{N(a) \neq G} \frac{O(G)}{O(N(a))}$$

$$\circ \quad P \mid O(G) - \sum_{N(a) \neq G} \frac{O(G)}{O(N(a))}$$

$$\circ \quad P \mid O(z).$$

$\circ$ z is not a proper subgroup

$\Rightarrow G = z \Rightarrow G$ is abelian.

$\circ \exists a \in G, a \neq e$ s.t. $a^p = e$.

$\circ$ This complete the proof of the thm.

P - Groups :

Definition :

A groups G is said to be a P -group if its order is a power of P .

Theorem :

A group G is a P -group iff every element in G has an order equal to a power of P .

Proof :

If $O(G) = P^n$

If $a \in G$, (By langramge thm)

$$\circ O(a) \mid O(G) = P^n.$$

$$\circ O(a) = P^\alpha \text{ (for some } 0 \leq \alpha \leq n)$$

Conversely,

If every element in G has an order equal to a power of P .

To P.T. G is a group.

Let q be a prime different from P dividing $O(G)$.

$\frac{q}{O(G)} \Rightarrow G$ has an element of order q . (By Cauchy's theorem)

This contradicts our hypothesis,

$\therefore O(G) = P^n$ for some $n \in \mathbb{Z}^+$.

$\therefore G$ is a P -group.

Theorem :

Every P -group has non-trivial centre.

Proof :

Let G be a group of order P^n .

The class equation of G as follows.

$$O(G) = \sum \frac{O(G)}{O(N(a))}$$

where the summation ranges over one element from each conjugate class of G .

Let z be the centre of G .

$$O(G) = \sum_{a \in Z} \frac{O(G)}{O(N(a))} + \sum_{a \notin Z} \frac{O(G)}{O(N(a))}$$

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

$$\therefore O(G) - \sum_{N(a) \neq G} \frac{O(G)}{O(N(a))} = O(Z).$$

If $N(a) \neq G$, $O(N(a)) = P^{n_1}$, where $0 \leq n_1 < n$

$$\frac{O(G)}{O(N(a))} = \frac{P^n}{P^{n_1}} = P^{n-n_1} \text{ where } n-n_1 > 0$$

$$\therefore \text{If } N(a) \neq G \quad P \mid \frac{O(G)}{O(N(a))}$$

$$\therefore P \mid \sum_{N(a) \neq G} \frac{O(G)}{O(N(a))}$$

$$\circ P / O(G) - \sum_{N(a) \neq G} \frac{O(G)}{O(N(a))} = O(z)$$

$$\circ \Rightarrow P / O(z)$$

$$\circ z \neq \{e\}$$

$\circ G$ has a non-trivial centre.

Cor :

A group of order P^2 is abelian.

Proof :

Let G be a group of order P^2 .

If z is the centre of G .

$$z \neq \{e\}$$

By langange's thm $O(z)/O(G) = P^2$.

$$\circ O(z) = P \text{ or } O(z) = P^2.$$

$$\text{If } O(z) = P^2 = O(G) \Rightarrow G = z$$

$\Rightarrow G$ is abelian.

$$\text{If } O(z) = P$$

$$\text{Let } a \in z, a \notin z$$

$$\circ N(a) \neq z$$

$$\circ O(N(a)) = P^2 = O(G)$$

$$\Rightarrow N(a) = G \Rightarrow a \in z$$

This is a contradiction.

$$\circ O(z) = P^2 = O(G)$$

$$\Rightarrow G = z$$

$\Rightarrow G$ is abelian.

Theorem

A group of order P^n has a normal subgroup of order P^{n-1} .

Proof

The proof is by induction of n . If $n=1$, If G is a group of order P^1 . $\{e\}$ is a normal subgroup of G of order P^0 . The thm is true for $n=1$.

Induction

Let us Assume that the thm is true for all groups whose order is P^α with $\alpha < n$.

If G is a group of order P^n .

If z is the centre of G .

$$\% z \neq \{e\}$$

$$\% O(z) = P^\alpha \text{ where } 0 < \alpha < n$$

$$\% P/O(z)$$

By cauchy's thm, $a \in z$, $a \neq e$, $a^p = e$

Let H be the cyclic subgroup generated by a .

$$H = \langle a \rangle$$

$$O(H) = P$$

If $x \in G$, $h \in H$

$$\% h = a^r \text{ for some } r \in \mathbb{Z}$$

$$a \in z, h = a^r \in z$$

$$xhx^{-1} = h(xx^{-1}) = h \in H$$

$\Rightarrow H$ is a normal subgroup of G .

Consider the canonical homomorphism

$$\phi : G \rightarrow G/H$$

$$O(G/H) = \frac{O(G)}{O(H)} = \frac{P^n}{P} = P^{n-1}$$

By the induction hypothesis G/H has a normal subgroup $\bar{N}$ of order P^{n-2} .

$$\text{Let } N = \phi^{-1}(\bar{N})$$

N is a normal subgroup of G .

By the second law of homomorphism.

$$G/N \approx \frac{(G/H)}{\bar{N}}$$

$$O(G/N) = \frac{O(G/H)}{O(N)} = \frac{p^{n-1}}{p^{n-2}}$$

$$\therefore O(G/N) = P \Rightarrow O(N) = p^{n-1}.$$

$\therefore N$ is the required normal subgroup of G is order P^{n-1} .

This complete the proof of the thm.

Sylow's Theorem :

In this chapter we study groups of order P^n ($p = \text{prime}$) and three theorems due to sylow called sylow's theorems. The ideas developed are so useful that plenty can be known about the nature of a group by knowing only its order.

Definition :

A P -group is group in which every element has order P^r where $P = \text{Prime}$. Here P is a same for all elements and r may vary.

The group $K_4 = \{I, (12)(34), (13)(24), (14)(23)\}$

and the quaternion group are examples of finite P -groups.

Here $P=2$. For example of an infinite P -group,

$\therefore S_3$ is not a P -group.

Theorem :

Let G be a finite group. Then G is a P -group if and only if $O(G) = P^n$.

Proof :

Suppose G is a P -group

Let q be a prime dividing $O(G)$.

By cauchy's theorem.

$$\exists x \in G \text{ s.t. } O(x) = q.$$

But $O(x) = P^r$ as G is a P -group.

$$\therefore q = P^r \Rightarrow q = P$$

So, P is the only prime dividing $O(G)$

$$\text{Thus } O(G) = P^n$$

Conversely,

Let $O(G) = P^n$ (P =prime)

Let $x \in G$

Then $O(x)/O(G) = P^n \Rightarrow O(x) = P^r$

∴ Every element of G has order which is some power of P .

∴ G is a P -group.

Sylow P -subgroups :

Let P be a prime s.t P^n divides order of a group G and P^{n+1} does not divide it. Then a subgroup H of G s.t. $O(H) = P^n$ is called a sylow P -subgroup of G or P -sylow subgroup of G .

We now discuss three theorems due to sylow called sylow's theorems. First theorem shows the existence of a sylow P -subgroup of G for every prime P dividing $P(G)$ while second theorem shows that any two sylow P -subgroups of G are conjugate. The third theorem gives the number of sylow P -subgroups of G .

Theorem : (Sylow's first theorem)

If P is a prime and if G is a finite group s.t. $P^\alpha | O(G)$. Then G has a subgroup of order P^α .

Proof :

$P^\alpha | O(G)$

$O(G) = P^\alpha m$

Let r be such that $P^r | m$, $P^{r+1} \nmid m$

Let $m =$ collection of all subsets of G of order P^α .

$O(m) = P^\alpha m C_{P^\alpha}$.

$$\therefore n C_r = \frac{n!}{r!(n-r)!}$$

$$\therefore P^\alpha m C_{P^\alpha} = \frac{(P^\alpha m)!}{P^\alpha! (P^\alpha m - P^\alpha)!}$$

$$P^\alpha m C_{P^\alpha} = \frac{P^\alpha m}{P^\alpha m - P^\alpha} P^\alpha$$

$$= \frac{(P^\alpha m)(P^\alpha m - 1)(P^\alpha m - 2) \dots (P^\alpha m - i) \dots (P^\alpha m - p^\alpha + 1)}{P^\alpha (P^\alpha - 1)(P^\alpha - 2) \dots (P^\alpha - i) \dots (P^\alpha - P^\alpha + 1)}$$

$$(P^\alpha m - i) - (P^\alpha - i) = P^\alpha (m - 1)$$

$$\circ \circ \quad P^\alpha m - i \equiv P^\alpha - i \pmod{P^\alpha}$$

$\circ$ The power of P dividing $P^\alpha m - i$ is the same as the power of P dividing $P^\alpha - i$.

The power of P dividing m is the same as the power of P dividing $P^\alpha m C_p \alpha$.

Since $P^r/m, P^{r+i} \times m$

$$\circ \circ \quad P^r / P^\alpha m C_p \alpha, P^{r+1} \times P^\alpha m C_p \alpha.$$

$$\circ \circ \quad P^r/O(m), P^{r+1} \times O(m) \dots \dots \dots (1)$$

If $A, B \in m$, we say that $A \sim B$ if,

$$B = Ax \text{ (for some } x \in G)$$

Since $A = Ae$, for every $A \in m$

$$\circ \circ \quad A \sim A$$

$\circ$ is reflexive.

If $A \sim B$, then $B = Ax$ for $x \in G$

$$\circ \circ \quad Bx^{-1} = A$$

$$\circ \circ \quad B \sim A$$

$\circ \sim$ is symmetric.

If $A \sim B$ and $B \sim C$.

Then $B = Ax$ and $C = By$ (for some $x, y \in G$)

$$\begin{aligned} C &= BY = (AX)y \\ &= A(xy) \end{aligned}$$

$$\circ \circ \quad A \sim C$$

$\circ \sim$ is transitive.

This therefore defines an equivalence relation in the collection m .

This relation partitions the collection m into disjoint equivalence classes.

since $P^{r+1} \times O(m)$ [from equation (1)]

$\exists$ at least one equivalence class.

$$\text{say } C = \{M_1, M_2, \dots, M_n\}$$

s.t. $P^{r+1} X_n$

Define $H = \{x \in G; M_1 x = M_1\}$

To verify that H is a subgroup G .

Let $x, y \in H$

$$M_1 x = M_1$$

$$M_1 y = M_1$$

$$M_1(xy) = (M_1 x)y$$

$$= M_1 y$$

$$= M_1$$

$$\Rightarrow xy \in H$$

$\Rightarrow H$ is a subgroup of G .

Let $y \in Hx$

$$y = hx \text{ (for some } h \in H)$$

$$M_1 y = M_1(hx)$$

$$= (M_1 h)x$$

$$= M_1 x$$

$$\Rightarrow M_1 y = M_1 x$$

Two elements belonging to the same right coset of H in G . Give rise to the same element in the equivalence class.

Define a mapping :

$$\emptyset: G/H \rightarrow C \text{ as follows}$$

$$\emptyset(Hx) = M_1 x$$

$\emptyset$ is well defined.

To P.T $\emptyset$ is one-to-one

$$\emptyset(Hx) = \emptyset(Hy)$$

$$\Rightarrow M_1 x = M_1 y$$

post multiply by y^{-1}

$$M_1 x y^{-1} = M_1 \Rightarrow M_1(x y^{-1}) = M_1$$

$$\circledast xy^{-1} \in H$$

$$\circledast xy^{-1} = h \in H$$

$$\circledast x = hy \in Hy$$

$$\circledast x \in Hy \Rightarrow Hx = Hy.$$

$\circledast$ is one to one.

Any element of C will be of the form M_1x for some $x \in G$

$$M_1x = \emptyset(Hx)$$

$\Rightarrow \emptyset$ is onto

$\circledast \emptyset$ is one to one correspondance between G/H and C .

$$\circledast O(G/H) = O(C) = n$$

$$\Rightarrow O(G) = n.O(H)$$

$$P^\alpha m = n.O(H)$$

Since

$$P^\alpha / M_1, P^{r+\alpha} / P^\alpha.m$$

$$P^{r+\alpha} / n.O(H)$$

$$\circledast P^{\alpha+1} \times O(H)$$

$$\Rightarrow P^\alpha / O(H)$$

$$\Rightarrow O(H) \geq P^\alpha \quad \dots\dots\dots (1)$$

If $x, y \in H$

$$M_1x = M_1, M_1y = M_1$$

If $m \in M_1, \forall mx, my \in M_1$

$$\circledast m_1x = m_1y$$

$$\Rightarrow x = y$$

If $x, y \in H$

$$x \neq y$$

Then $mx \neq my$

$$O(M_1) \geq O(H)$$

since $O(M_1) = P^\alpha \quad (\circledast M_1 \in n)$

$$\frac{|G|}{|H|} \geq \frac{|G|}{|H|} \dots\dots\dots (2)$$

From (1) & (2)

$$|G| = |H| \cdot \frac{|G|}{|H|}$$

∴ H is the required subgroup of G of order P^α .

Hence the proof.

Cor :

If $P^n \nmid |G|$, $P^{n+1} \mid |G|$ then G has a subgroup of order P^n .

Proof :

Take $\alpha = n$ and use the above theorem.

Second proof of sylow's theorem :

G has a P-sylow subgroup for every prime P dividing $|G|$.

Proof :

The proof is by induction on $|G|$ If $|G| = 2$.

2 is the only prime dividing $|G|$.

∴ G itself is the required 2 sylow subgroup of G.

The theorem is trivially true in this case.

Induction hypothesis :

Assume the result for all groups whose order is less than $|G|$

Given that $P^n \nmid |G|$

but $P^{n+1} \mid |G|$

If G has a proper subgroup H such that $P^n \mid |H|$

By induction hypothesis,

H has a subgroup of order P^n . P is a subgroup of H and H is a subgroup of G.

∴ P is the required subgroup of order P^n .

If P^n does not divide the order of any proper subgroup of G.

The class equation of G is as follows.

$$O(G) = \sum \frac{O(G)}{O(N(a))} \text{ where the summation ranges over one element.}$$

From each conjugate class of G .

$$O(G) = \sum_{a \in Z} \frac{O(G)}{O(N(a))} + \sum_{a \notin Z} \frac{O(G)}{O(N(a))}$$

Let z be the centre of G .

$$a \in Z \text{ iff } O(N(a)) = O(G)$$

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

$$\Rightarrow O(Z) = O(G) - \sum_{N(a) \neq G} \frac{O(G)}{O(N(a))}$$

$$\text{If } N(a) \neq G, P^n \times O(N(a))$$

$$\text{But } P^n / O(G)$$

$$\therefore P / \frac{O(G)}{O(N(a))}$$

$$\therefore P / \sum_{N(a) \neq G} \frac{O(G)}{O(N(a))}$$

$$\therefore P / O(G) - \sum_{N(a) \neq G} \frac{O(G)}{O(N(a))} = O(Z)$$

$$\therefore P / O(Z)$$

By Cauchy's theorem, $\exists a \in Z, a \neq e$ s.t. $a^p = e$

Let $H = \langle a \rangle$, the cyclic subgroup generated by a .

$$O(H) = P$$

If $x \in G, h \in H, h = a^r$ for some $r \in Z$

$$xhx^{-1} = xax^{-1}$$

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

$$= (xx^{-1})a = a \in H$$

$$\therefore xhx^{-1} \in H, \forall x \in G, \forall h \in H$$

∴ H is a normal subgroup of G.

$$\therefore O(G/H) = \frac{O(G)}{O(H)} = \frac{O(G)}{P} < O(G)$$

$$\therefore P^{n-1} / O(G/H), P^n \times O(G/H)$$

By induction hypothesis,

G/H has a subgroup $\bar{P}$ of order P^{n-1} .

Let $\phi: G \rightarrow G/H$ be the natural homomorphism of G onto G/H.

$P = \phi^{-1}(\bar{P})$ is subgroup of G

Containing H.

$$\therefore P/H \approx \bar{P}$$

$$\therefore O(\bar{P}) = O(P/H)$$

$$P^{n-1} = O(P/H)$$

$$\Rightarrow O(P/H) = P^{n-1} \Rightarrow O(P) = P^n$$

∴ P is required P-sylow subgroup of G of order P^n .

The proof by induction is complete.

If P is a P-sylow subgroup of G,

$$O(P) = P^n.$$

$$O(xpx^{-1}) = O(P) = P^n$$

∴ xpx^{-1} is also a P-sylow subgroup.

The conjugate of a P-sylow subgroup is again a P-sylow subgroup.

Double Caset :

Let A, B be two subgroups of G. Define a relation $\sim$ in G as follows.

$$x \sim y$$

$$\text{If } y = axb \text{ [for some } a \in A, b \in B]$$

$$\text{Since } exe = x, \forall x \in G$$

$$x \sim x$$

∴ $\sim$ is reflexive

$$\text{If } x \sim y, \text{ then } y = axb \text{ where } a \in A, b \in A$$

$$y = axb$$

$$x = a^{-1}yb^{-1} [\because a^{-1} \in A, b^{-1} \in A]$$

∴

$$y \sim x$$

∴ $\sim$ is symmetric

If

$$x \sim y \text{ and } y \sim z$$

$$y = a_1xb_1, z = a_2yb_2. \quad (a_1, a_2 \in A, b_1, b_2 \in B)$$

$$\begin{aligned} z &= a_2(a_1xb_1)b_2 \\ &= (a_2a_1)x(b_1b_2) \end{aligned}$$

∴

$$x \sim z.$$

∴ $\sim$ is transitive.

This defines an equivalence relation in G.

∴ This partition G into disjoint equivalence classes.

$$\begin{aligned} [x] &= \{y, x \sim y\} \\ &= \{axb; a \in A, b \in B\} \\ &= AxB \end{aligned}$$

This is called the double coset of A with respect to A and B.

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

Lemma :

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

Proof :

Define $\emptyset: AxB \rightarrow AxBx^{-1}$ as follows.

$$\emptyset(axb) = axbx^{-1} \text{ (where } a \in A, b \in B)$$

To prove $\emptyset$ is one to one.

$$\text{If } (a_1xb_1) = \emptyset(a_2xb_2)$$

$$a_1xb_1x^{-1} = a_2xb_2x^{-1}$$

post multiply by x.

$$\Rightarrow a_1 x b_1 = a_2 x b_2$$

$\Rightarrow \emptyset$ is one to one.

Any element of $AxBx^{-1}$ will be of the form $axbx^{-1} = \emptyset(axb)$ [where $a \in A, b \in B$]

$\therefore \emptyset$ is onto

$\therefore \emptyset$ is a one to one correspondence between AxB and $AxBx^{-1}$.

$$\therefore O(AxB) = O(AxBx^{-1})$$

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

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

Hence the proof.

Second part of sylow's theorem :

If G is a finite group P is a prime such that $P^n \mid O(G)$, $P^{n+1} \nmid O(G)$. Any two subgroups of order P^n are conjugate to each other.

Proof :

Let A, B be two subgroups of G of order P^n .

Decompose G into the double cosets of A and B .

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

where the summation ranges over one element from each double coset.

To prove that

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

If the result is not true.

$$A \neq xBx^{-1} \text{ for any } x \in G.$$

$$A \cap xBx^{-1} \text{ is a proper subgroup of } A.$$

$$O(A) = P^n$$

$$\therefore O(A \cap xBx^{-1}) = P^\alpha \text{ where } \alpha < n.$$

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

$$\Rightarrow O(AxB) = \frac{p^n p^n}{p^\alpha} = p^{n+(n-\alpha)}$$

$$\Rightarrow O(AxB) = p^{n+(n-\alpha)}$$

[where $n-\alpha \geq 1$]

$$\therefore p^{n+1} / O(AxB)$$

$\therefore p^{n+1}$ divides the order of every double coset in G .

$$p^{n+1}/O(G) = \sum O(AxB)$$

This contradicts hypothesis that

$$p^{n+1} \nmid O(G)$$

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

Hence the proof.

Lemma :

The number of P-sylow's subgroup of a group $G = \text{Index of } N(P)$ where P is any P-sylow subgroup. The number of P-sylow subgroup is a divisor of $O(G)$.

Proof :

$$\text{Let } C = \{x^{-1}Px; x \in G\}$$

$C = \text{set of conjugate subgroups of } P$.

$$\text{Number of P-sylow subgroups} = O(C).$$

Define $\emptyset: \frac{G}{N(P)} \rightarrow C$ as follows.

$$\emptyset(N(P)x) = x^{-1}Px.$$

If $y \in N(P)x, y = nx$ where $n \in N(P)$

$$y^{-1}py = (nx)^{-1}P(nx)$$

$$= x^{-1}n^{-1}Pnx$$

$$= x^{-1}(n^{-1}Pn)x \quad [\because n \in N(P)]$$

$$\Rightarrow y^{-1}py = x^{-1}px$$

$\therefore \emptyset$ is well defined.

Any element of C will be of the form $x^{-1}px$ (for some $x \in G$)

$$x^{-1}px = \emptyset (N(P)x)$$

The mapping $\emptyset$ is onto

$$\text{If } \emptyset (N(P)x) = \emptyset (N(P)y)$$

$$\text{Then } x^{-1}Px = y^{-1}Py$$

$$\Rightarrow (yx^{-1})P(xy^{-1}) = P$$

$$\Rightarrow (xy^{-1})^{-1}P(xy^{-1}) = P$$

$$\Rightarrow xy^{-1} \in N(P)$$

$$\circ \circ xy^{-1} = n \in N(P)$$

$$\circ \circ x = nyN(P)y$$

$$\circ \circ N(P)x = N(P)y$$

$$\Rightarrow \emptyset \text{ is one to one}$$

$\circ \circ \emptyset$ is one one correspondence between $G/N(P)$ and C .

$$\circ \circ O\left(\frac{G}{N(P)}\right) = O(C)$$

Number of P sylow subgroups = Index of $N(P)$ in G .

Hence the thm.

Third part of sylow's theorem :

If P be a prime dividing the order of a finite group G . Then the number of P -sylow subgroups of G is of the form $KP+1$ where K is the integer. $KP+1 \equiv 1 \pmod{P}$ (The number of P -sylow subgroups of G is congruent to 1 modulo P).

Proof :

Let P be the P -sylow subgroup of G .

Let $O(P) = P^n$

Then $P^n / O(G)$. $P^{n+1} \times O(G)$

Decompose G into the double cosets of G with respect to p and P .

$O(G) = \sum O(pxP)$ where the summation ranges over one element from each double coset in G .

$$O(G) = \sum_{x \in N(P)} O(pxP) + \sum_{x \notin N(P)} O(pxP) \dots\dots\dots (1)$$

If $x \in N(P), xpx^{-1} = P$

$$xP = px.$$

$$pxP = P(xP) = P(px) = (pp)x = px$$

[double coset = right coset]

$$\sum_{x \in N(P)} O(pxP) = \sum_{x \in N(P)} O(px) = O(N(P)) \dots\dots\dots (2)$$

If $x \notin N(P), xpx^{-1} \neq P$

∴ $P \cap xPx^{-1}$ is a proper subgroup of P .

$$O(P \cap xPx^{-1}) = P^\alpha, [0 \leq \alpha < n]$$

$$O(PxP) = \frac{O(P) \cdot O(P)}{O(P \cap xPx^{-1})} = \frac{p^n \cdot p^n}{p^\alpha} = p^{n+(n-\alpha)}$$

where $n - \alpha \geq 1$

∴ $p^{n+1} / O(pxP)$

∴ $p^{n+1} / \sum_{x \notin N(P)} O(pxP)$

$$\sum_{x \notin N(P)} O(pxP) = p^{n+1} u \dots\dots (3) \text{ (where } u \text{ is an integer)}$$

Sub (2) & (3) in (1)

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

$$\frac{O(G)}{O(N(P))} = 1 + \frac{p^{n+1} u}{O(N(P))}$$

∴ $\frac{O(G)}{O(N(P))} = \text{index of the normalizer of } P.$

Number of P-sylow subgroups of G .

$$S_p = i(N(P)) = \frac{O(G)}{O(N(P))} = 1 + \frac{p^{n+1} u}{O(N(P))}$$

$$\therefore S_p = 1 + \frac{p^{n+1}u}{O(N(P))}$$

Since $P^{n+1} \times O(G) \cap N(P)$ is a subgroup of G .

$$\therefore P^{n+1} \times O(N(P))$$

$$\frac{p^{n+1}u}{O(N(P))} = PK$$

$$\therefore S_p = 1 + KP \text{ (where } K \text{ is an integer)}$$

$$\therefore \text{Number of } P\text{-sylow subgroups} = 1 + KP.$$

Hence the proof.

Problems

1) Determine the number of the 5-sylow subgroups and the 3-sylow subgroups of a group of order 30.

Solution

Let G be a group of order 30.

$$O(G) = 30 = 2 \times 3 \times 5$$

$$S_5 = \text{Number of 5-sylow subgroups.}$$

$$= 1 + 5k$$

$$S_5 / O(G) \Rightarrow 1 + 5k / 30 = 2 \times 3 \times 5$$

$$\Rightarrow 1 + 5k / 2 \times 3$$

$$\Rightarrow 1 + 5k = 1 \text{ possible}$$

$$1 + 5k = 2 \text{ not possible}$$

$$1 + 5k = 3 \text{ not possible}$$

$$1 + 5k = 6 \text{ possible}$$

Either G has 1 5-sylow subgroup or 6 5-sylow subgroups.

If G has only one 5-sylow subgroup, then that subgroup is normal in G .

$$S_3 = \text{Number of 3 - sylow subgroups}$$

$$= 1 + 3k$$

$$S_3/O(G) \Rightarrow 1+3k / 5 \times 3 \times 2$$

$$\Rightarrow 1+3k / 5 \times 2$$

$$\Rightarrow 1 + 3k = 1 \text{ possible}$$

$$1 + 3k = 2 \text{ not possible}$$

$$1 + 3k = 5 \text{ not possible}$$

$$1 + 3k = 10 \text{ possible}$$

Either G has 1 3-sylow subgroup or 10 3-sylow subgroup.

If G has only one 3 - sylow subgroup, then that subgroup is normal in G.

If G has 6 5-sylow subgroups

say $H_1, H_2, \dots, H_6$

$$O(H_i) = 5 (\forall i = 1, 2, \dots, 6)$$

$$H_1 \cap H_2 \neq H_1$$

$$\% H_1 \cap H_2 = \{e\}$$

$$H_i \cap H_j = \{e\} \text{ for } i \neq j \quad (\forall i, j = 1, 2, \dots, 6)$$

Each H_i contains 4 elements of order 5.

$$\% G \text{ contains } 6 \times 4 = 24$$

elements of order 5.

$$\% \text{ Only } 30 - 24 = 6 \text{ elements are not of order 5.}$$

% G can have only one 3-sylow subgroup of G.

which will be a normal subgroup of G.

% Either the 3-sylow subgroup or the 5-sylow subgroup is normal in G.

1) G has 1 5-sylow subgroup, say H

1 3-sylow subgroup, say K

$$\% H \cap K = \{e\}$$

G will have a normal subgroup of order 15.

% G will then have 15, 1 2-sylow subgroups.

2) G has 1 5-sylow subgroup, 10 3-sylow subgroups.

In this case G will have 5, 2-sylow subgroups.

3) G has 6, 5-sylow subgroups, 1-3 sylow subgroups.

G has 3, 2-sylow subgroups.

Hence the solution.

Problem : 2

P.T in a group of order 231, the 11-sylow subgroup has in the centre of G.

Proof :

Let G be a group of order $231 = 11 \times 7 \times 3$

$$S_{11} = \text{Number of 11 - sylow subgroups}$$

$$= 1 + 11K$$

$$S_{11}/O(G) \Rightarrow 1 + 11K / 11 \times 7 \times 3$$

$$\Rightarrow 1 + 11K / 7 \times 3$$

$$1 + 11K = 1 \text{ possible}$$

$$1 + 11K = 3 \text{ Impossible}$$

$$1 + 11K = 7 \text{ Impossible}$$

$$1 + 11K = 2 \text{ Impossible}$$

G has exactly 1, 11-sylow subgroup say 11.

$$O(H) = 11.$$

H is cyclic, say $H = \langle a \rangle$ and H is abelian.

$$S_7 = \text{Number of 7-sylow subgroups}$$

$$= 1 + 7K$$

$$S_7/O(G) \Rightarrow 1 + 7K / 11 \times 7 \times 3$$

$$\Rightarrow 1 + 7K / 11 \times 3$$

$$\Rightarrow 1 + 7K = 1 \text{ possible}$$

$$1 + 7K = 3 \text{ Impossible}$$

$$1 + 7K = 11 \text{ Impossible}$$

$$1 + 7K = 33 \text{ Impossible}$$

G has exactly 1, 7-sylow subgroup say K.

$$O(K) = 7.$$

K is cyclic say $K = \langle 1 \rangle$ and K is abelian. H and K are both in G.

$$H \cap K = \{e\}$$

Every element of H commutes with every element of K.

HK is a normal subgroup of G.

$$O(HK) = \frac{O(H)O(K)}{O(H \cap K)} = \frac{11 \times 7}{1} = 77.$$

S_3 = Number of 3-sylow subgroups

$$= 1 + 3K$$

$$S_3 / O(G) \Rightarrow 1 + 3K / 11 \times 7 \times 3$$

$$\Rightarrow 1 + 3K / 11 \times 7$$

$$\Rightarrow 1 + 3K = 1 \text{ possible}$$

$$1 + 3K = 7 \text{ possible}$$

$$1 + 3K = 11 \text{ not possible}$$

$$1 + 3K = 77 \text{ not possible}$$

G has either only one 1, 3-sylow subgroups or 7, 3-sylow subgroup.

Case (i)

G has only one 1, 3-sylow subgroup say L

$$O(L) = 3. L \text{ is cyclic and abelian.}$$

Let L be generated by G.

$$\text{i.e.) } L = \langle G \rangle$$

∴ L is normal in G.

$$H \cap L = \{e\}, K \cap L = \{e\}$$

Every element of L commutes with every element of H and with every element of K.

$$O(HK \cap L) / O(HK) = 77$$

$$\Rightarrow O(HK \cap L) / O(L) = 3$$

$$\Rightarrow HK \cap L = \{e\}$$

$$\begin{aligned} O(HKL) &= O(HK).O(L) \Rightarrow 77 \times 3 \\ &= 231 = O(G) \end{aligned}$$

$$\Rightarrow HKL = G$$

Let $h \in H$, Let $x \in G = HKL$

$$x = h_1 k_1 l_1$$

where $h_1 \in H, k_1 \in K, l_1 \in L$

$$hx = (h_1 k_1 l_1)$$

$$= (hh_1) k_1 l_1$$

$$= (hh_1)(k_1 l_1)$$

$$\Rightarrow hx = h_1(hk_1)l_1$$

$$= h_1(k_1 h)l_1$$

$$= (h_1 k_1)(h_1 l_1)$$

$$= (h_1 k_1)(l_1 h)$$

$$= (h_1 k_1 l_1) h = x h$$

$$\therefore H \subset \text{centre of } G.$$

Case (ii) :

G has 7, 3-sylow subgroups. Let L_1 be one of them.

$$S_3 = iN(L_1) = 7$$

$$O(N(L_1)) = \frac{O(G)}{7} = 33 = 3 \times 11$$

$N(L_1)$ has a subgroup of order 11.

$$\therefore H \subset N(L_1)$$

L_1 is a normal subgroup of $N(L_1)$

H is a normal subgroup of $N(L_1)$

$$H \cap L_1 = \{e\}$$

Every element of H commutes with every element of L_1 .

$$HK \cap L_1 = \{e\}$$

$$O(HK \cap L_1) = O(HK).O(L_1) = 77 \times 3 = 231 = O(G)$$

$$G = HKL_1$$

Let $x \in G, h \in H$

$$x \in G = HKL_1$$

$$x = h_1 k_1 l_1 \quad \text{where } h_1 \in H, k_1 \in K, l_1 \in L_1.$$

$$hx = h(h_1 k_1 l_1)$$

$$= (h_1 h)(k_1 l_1)$$

$$= h_1 (h k_1) l_1$$

$$= h_1 (k_1 h) l_1$$

$$= (h_1 k_1)(h l_1)$$

$$= (h_1 k_1)(l_1 h)$$

$$\Rightarrow hx = (h_1 k_1 l_1) h = xh$$

$$\therefore H \subset \text{centre of } G.$$

$\therefore$ The centre of G contains the H -syllow subgroup of G .

Problem :

The above problem is the same as $O(G) = 385$, 7-syllow subgroup centre of G .

Problem 3 :

P.T a group of order 48 contains a normal subgroup of order $2k$ where $k \geq 3$.

Solution :

Let G be a group of order

$$48 = 2^4 \times 3^1.$$

$$S_2 = \text{Number of 2-syllow subgroup}$$

$$= 1 + 2K$$

$$S_2/O(G) \Rightarrow 1 + 2K / 2^4, 3$$

$$\Rightarrow 1 + 2K/3$$

$$\therefore S_2 = 1 + 2K = 1 \text{ possible}$$

$$= 1 + 2K = 3 \text{ possible}$$

$\therefore G$ has either 1, 2-syllow subgroup or 3, 2-syllow subgroup.

Case (i) :

G has either 1, 2-sylow subgroup say H.

$$O(H) = 2^4$$

H is normal in G.

Case (ii) :

G has 3, 2-sylow subgroup say k_1, k_2, k_3 .

$$O(k_1 k_2) = \frac{O(K_1)O(K_2)}{O(K_1 \cap K_2)} = \frac{2^4 \cdot 2^4}{O(K_1 \cap K_2)} \leq 48$$

$$\Rightarrow O(K_1 \cap K_2) \geq \frac{2^4 \cdot 2^4}{48} = \frac{16}{3}$$

$$\Rightarrow O(K_1 \cap K_2) = 8$$

$$i_{k_1}(K_1 \cap K_2) = \frac{O(K_1)}{O(K_1 \cap K_2)} = \frac{16}{8} = 2$$

∴ $K_1 \cap K_2$ is normal in K_1 .

$K_1 \cap K_2$ is normal in K_2 .

∴ $K_1 \cap N(K_1 \cap K_2)$

$K_2 \subset N(K_1 \cap K_2)$

∴ $K_1 K_2 \subset N(K_1 \cap K_2)$

$$O(K_1 K_2) \leq O(N(K_1 \cap K_2))$$

$$\Rightarrow \frac{O(K_1)O(K_2)}{O(K_1 \cap K_2)} \leq O(N(K_1 \cap K_2))$$

$$\Rightarrow \frac{16 \times 16}{8} \leq O(N(K_1 \cap K_2))$$

$$O(N(K_1 \cap K_2)) \geq 32$$

$$O(N(K_1 \cap K_2)) / O(G) = 48$$

$$\therefore O(N(K_1 \cap K_2)) = 48 = O(G)$$

$$\therefore N(K_1 \cap K_2) = G$$

∴ $K_1 \cap K_2$ in the required normal subgroup of order 2^3 .

Hence the solution.

SOLVABLE GROUPS

Defintion :

A group G is said to be solvable if there exists a sequence of subgroups.

$$G = G_0 \supset G_1 \supset G_2 \dots \dots \dots \supset G_k = \{e\}$$

s.t. G_i is a normal in G_{i-1} and

$$\frac{G_i - 1}{G_i} \text{ is abelian.}$$

The series is called a solvable series for G .

Any abelian group is solvable.

If G is an abelian group.

$G \supset \{e\}$ is a solvable series for G .

$$S_1 = \{i\}, S_2 = \{i, (1, 2)\}$$

$$S_3 \supset A_3 \supset \{e\}$$

$$O\left(\frac{S_3}{A_3}\right) = Z \quad \& \quad \frac{S_3}{A_3} \text{ is abelian.}$$

$$O\left(\frac{A_3}{\{e\}}\right) = O(A_3) = 3.$$

$$\frac{A_3}{\{e\}} \text{ is abelina.}$$

$S_3 \supset A_3 \supset \{e\}$ is a solvable series for S_3 .

$\& S_3$ is solvable.

A_4 is a normal subgroup of s_4 .

$$O\left(\frac{S_4}{A_4}\right) = 2 \Rightarrow \frac{S_4}{A_4} \text{ is abelian.}$$

$$H = \{(12)(34), (13)(24), (14)(23), i\}$$

H is a normal subgroup of A_4 .

$$o\left(\frac{A_4}{H}\right) = 3 \Rightarrow \frac{A_4}{H} \text{ is abelian.}$$

$$\frac{H}{\{e\}} = H \text{ is abelian.}$$

∴ $S_4 \supset A_4 \supset H \supset \{e\}$ is a solvable series for S_4 .

∴ S_4 is solvable.

For $n \geq 5$, the only normal subgroups of S_n are S_n , A_n and $\{e\}$

$S_n \supset A_n \supset \{e\}$ is not solvable.

∴ S_n is not solvable, for $n \geq 5$

Lemma :

A group of order pq where p, q are distinct primes is solvable.

Proof :

Without loss of generality, Assume $p > q$.

Let G be a group of order pq ,

$O(G)$

By Cauchy's thm, $\exists a \in G, a \neq e, a^p = e$.

Let $H = \langle a \rangle$ be the cyclic subgroup generated by a .

$O(H) = P$.

H is therefore cyclic and hence abelian.

$$i(H) = \frac{O(G)}{O(H)} = \frac{pq}{p} = q$$

∴ $O(G) \times \angle i(H)$

∴ G has a proper normal subgroup inside H .

But $O(H) = P$.

H has no nontrivial subgroups.

∴ H is the normal subgroup of G .

$$O\left(\frac{G}{H}\right) = q \Rightarrow \frac{G}{H} \text{ is abelian.}$$

$G \supset H \supset \{e\}$ is a solvable series for G .

$\therefore G$ is solvable.

Lemma :

A subgroup of a solvable group is solvable.

Proof :

Let H be a subgroup of a solvable group G .

G has a solvable series

$$G = G_0 \supset G_1 \supset G_2 \supset \dots \supset G_k = \{e\}$$

s.t. G_i is normal in G_{i-1} .

and $\frac{G_{i-1}}{G_i}$ is abelian.

consider the series

$$G \cap H = H = H_0 \supset G_1 \cap H = H_1 \supset G_2 \cap H = H_2 \supset \dots \supset G_k \cap H = \{e\} = H_k.$$

Since G_i is normal in G_{i-1} .

$G_i \cap H$ is normal in $G_{i-1} \cap H$.

i.e.) H_i is normal in H_{i-1}

$$\begin{aligned} \text{Let } X, Y &\in \frac{H_{i-1}}{H_i} \\ &= \frac{G_{i-1} \cap H}{G_i \cap H} \end{aligned}$$

$$X = H_i x, Y = H_i y.$$

$$\text{where } x, y \in H_{i-1}.$$

$$= G_{i-1} \cap H.$$

$$x, y \in G_{i-1}.$$

we know that

$$\frac{G_{i-1}}{G_i} \text{ is abelian.}$$

$$(G_i x) (G_i y) = (G_i y) (G_i x)$$

$$G_i (xy) = G_i (yx)$$

$$\Rightarrow xy \in G_i (yx) = xy = gyx$$

$$\text{where } g \in G_i.$$

$$\Rightarrow xy = gyx$$

$$\Rightarrow xyx^{-1}y^{-1} = g \in G_i$$

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

$$xyx^{-1}y^{-1} = g \in G_i \cap H.$$

$$\Rightarrow xy = g(yx) \in (G_i \cap H)$$

$$\Rightarrow xy \in H_i (yx)$$

$$\Rightarrow H_i(xy) = H_i(yx)$$

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

$$\Rightarrow xy = yx$$

$$\text{where } x, y \in \frac{H_{i-1}}{H_i}$$

$$\circ \frac{H_{i-1}}{H_i} \text{ is abelian.}$$

$$\circ H = H_0 \supset H_1 \supset H_2 \supset \dots \supset H_k = \{e\}$$

is a solvable series for H.

$\circ$ H is solvable.

Lemma :

The homomorphic image of a solvable group is solvable.

Proof :

Let f be a homomorphism of a solvable group G onto a group $\bar{G}$.

To P.T $\bar{G}$ is solvable.

Since G is solvable, G has a solvable series.

$$\begin{aligned} G &= G_0 \supset G_1 \supset G_2 \supset \dots \supset G_k = \{e\} \\ f(G_0) &= f(G) \supset f(G_1) \supset f(G_2) \dots \supset f(G_k) \\ \bar{G} &\supset f(G_1) \supset f(G_2) \dots \supset \{e\} \end{aligned}$$

To show that $f(G_i)$ is normal in $f(G_{i-1})$

Let $\bar{x} \in f(G_{i-1}), \bar{y} \in f(G_i)$

$\circ$ $\bar{x} = f(x), \bar{y} = f(y)$

where $x \in G_{i-1}, y \in G_i$.

Since G_i is normal in G_{i-1} .

$$\begin{aligned} \bar{x}^{-1} y x &\in G_i \\ \Rightarrow f(\bar{x}^{-1} y x) &\in f(G_i) \\ \Rightarrow [f(x)]^{-1} f(y) f(x) &\in f(G_i) \quad [\circ f \text{ is homomorphism}] \\ \Rightarrow (\bar{x})^{-1} \bar{y} \bar{x} &\in f(G_i) \\ \Rightarrow f(G_i) &\text{ is normal in } f(G_{i-1}) \end{aligned}$$

Let $x, y \in \frac{f(G_{i-1})}{f(G_i)}$

$$\begin{aligned} X &= f(G_i) \bar{x}, Y = f(G_i) \bar{y}, \bar{x}, \bar{y} \in f(G_{i-1}) \\ \bar{x} &= f(x), \bar{y} = f(y) \end{aligned}$$

where $x, y \in G_{i-1}$.

Since $\frac{G_{i-1}}{G_i}$ is abelian.

$$\begin{aligned} (G_i x) (G_i y) &= (G_i y) (G_i x) \\ \Rightarrow G_i(xy) &= G_i(yx) \\ \Rightarrow xyx^{-1}y^{-1} &\in G_i \\ \Rightarrow f(xyx^{-1}y^{-1}) &\in f(G_i) \end{aligned}$$

$$\Rightarrow \bar{x}.\bar{y}.\bar{x}^{-1}.\bar{y}^{-1} \in f(G_i)$$

$$\Rightarrow f(G_i)(\bar{xy}) = f(G_i)(\bar{yx})$$

$$\Rightarrow [f(G_i)\bar{x}][f(G_i)\bar{y}] = [f(G_i)\bar{y}][f(G_i)\bar{x}]$$

$$\Rightarrow xy = yx \text{ for } x, y \in \frac{f(G_{i-1})}{f(G_i)}$$

∴ $\frac{f(G_{i-1})}{f(G_i)}$ is abelian.

$$\circ \bar{G} \supset f(G_i) \supset f(G_2) \supset \dots \supset \{e\}$$

is a solvable series for $f(G)$

∴ $f(G)$ is solvable.

Lemma :

The quotient group of a solvable series is solvable.

Proof :

Let N be a normal subgroup of a solvable group G .

Let $\phi: G \rightarrow G/N$

be the natural homomorphism of G onto G/N .

$$\phi(x) = Nx \quad (\forall x \in G)$$

∴ G/N is therefore a homomorphic image of G .

Lemma :

A normal subgroup of G/N will be of the form H/N is a normal subgroup of G .

Proof :

Let $\phi: G \rightarrow G/N$ be the natural homomorphism of G onto G/N .

Kernal of $\phi = N$.

Let $\bar{H}$ be a normal subgroup of G/H .

$H = \phi^{-1}(\bar{H})$ is a normal subgroup of G containing N .

$$\begin{aligned}\bar{H} &= \{\bar{0}(x); x \in H\} \\ &= \{Nx; x \in H\} \\ &= H/N\end{aligned}$$

$$\circ \quad \bar{H} = H/N \text{ where } H \text{ is a normal subgroup of } G \text{ containing } N.$$

Theorem :

If N is a normal subgroup of G and if N and G/N are both solvable then G is solvable.

Proof :

Since N is solvable, N has a solvable series.

$$N = N_0 \supset N_1 \supset N_2 \supset \dots \supset N_k = \{e\}$$

since G/N is solvable. G/N has a solvable series.

$$G/N \supset \frac{H_1}{N} \supset \frac{H_2}{N} \supset \frac{H_3}{N} \dots \supset \frac{H_r}{N} = N$$

where H_1 is normal in G , H_2 is normal in H_1 .

H_1 is normal in H_{i-1} .

$\circ$

$$\frac{\frac{H_{i-1}}{N}}{\frac{H_i}{N}} \text{ is abelian.}$$

By the second law of homomorphism.

$$\frac{\frac{H_{i-1}}{N}}{\frac{H_i}{N}} \approx \frac{H_{i-1}}{H_i}$$

$\circ$

$$\frac{H_{i-1}}{H_i} \text{ is abelian}$$

$$G \supset H_1 \supset H_2 \dots \supset H_r = N \supset N_1 \supset \dots \supset N_k = \{e\}$$

is a solvable series for G .

$\circ$ G is solvable.

This proves the thm.

Lemma :

If A is solvable of G and N is a normal sub group of G. If A and N are both solvable, then AN is solvable.

Proof :

Since A is solvable.

$A \cap N$ is solvable.

$\therefore \frac{A}{A \cap N}$ is solvable.

By the third law of homomorphism.

$$\frac{AN}{N} \approx \frac{A}{A \cap N}$$

$\therefore \frac{AN}{N}$ is solvable and N is solvable.

$\Rightarrow AN$ is solvable.

Hence the lemma.

Lemma :

If N is a normal subgroup of G and if G/N is abelian. Then N containing G^1 .

Proof :

Let $a, b \in G$

$Na, Nb \in G/N$ and G/N is abelian.

$$(Na)(Nb) = (Nb)(Na)$$

$$N(ab) = N(ba)$$

$$\Rightarrow ab \in N(ba)$$

$$\Rightarrow ab = n(ba) \quad \text{where } n \in N$$

Post multiply by a^{-1} and b^{-1}

$$aba^{-1}b^{-1} = n \in N$$

$$\therefore G^1 \subset N$$

Hence the lemma.

For a group G , we define the upper central series as follows.

$G^{(1)} = G^1$, the commutator subgroup of G .

$G^{(2)} =$ Commutator subgroup of $G^{(1)}$

$G^{(i)} =$ Commutator subgroup of $G^{(i-1)}$

Commutator subgroup of $S_3 = A_3$.

$G^{(1)} = A_3$

$G^{(2)} = \{e\}$, for $n \geq 2$, $G^{(n)} = \{e\}$

For $n \geq 5$, $G = S_n$, $G^{(1)} = A_n$

A_n is simple for $n \geq 5$

$G^{(1)} = G^{(2)} = A_n$

$G^{(3)} = A_n$

Lemma :

Let $G \supset G^{(1)} \supset G^{(2)} \supset \dots$ be the upper central series for G .

Proof :

$G^{(i)}$ is a normal subgroup of G . The proof is by induction on i . $[\forall i \geq 1]$

For $i = 1$

$G^{(1)} =$ Commutator subgroup of G .

If $x \in G^{(1)}$

$x = x_1 x_2 \dots x_r$

(where $x_j = a_j b_j a_j^{-1} b_j^{-1}$)

Let $g \in G$

$$\begin{aligned} g x_j g^{-1} &= g(a_j b_j a_j^{-1} b_j^{-1}) g^{-1} \\ &= (g a_j g^{-1})(g b_j g^{-1})(g a_j^{-1} g^{-1})(g b_j^{-1} g^{-1}) \\ &= a_j^1 b_j^1 (a_j^1)^{-1} (b_j^1)^{-1} \quad [\forall j = 1, 2, \dots, r] \end{aligned}$$

$$g x g^{-1} = (g x^1 g^{-1})(g x^2 g^{-1}) \dots (g x^r g^{-1}) \in G^{(i)}$$

$$\Rightarrow g x g^{-1} \in G^{(i)}, \forall g \in G, x \in G^{(i)}$$

$G^{(i)}$ is a normal subgroup of G .

Induction hypothesis; Assume $G^{(i-1)}$ is a normal subgroup of G .

To prove that

$G^{(1)}$ is a normal subgroup of G .

Let $x \in G^{(i)}, g \in G$

$$x = x_1 x_2 \dots x_r$$

where

$$x_j = a_j b_j a_j^{-1} b_j^{-1}$$

where $a_j, b_j \in G^{(i-1)}$

$[\forall j=1, \dots, r]$

$$g x_j g^{-1} = (g a_j g^{-1}) (g b_j g^{-1}) (g a_j^{-1} g^{-1}) (g b_j^{-1} g^{-1})$$

$$a_j^{-1} = g a_j g^{-1} \in G^{(i-1)} \quad [\because G^{(i-1)} \text{ is normal in } G]$$

|||ly

$$b_j^{-1} = g b_j g^{-1} \in G^{(i-1)}$$

$$\therefore g x_j g^{-1} = a_j^{-1} b_j^{-1} (a_j^{-1})^{-1} (b_j^{-1})^{-1} \in G^{(i)}$$

$$\therefore g x g^{-1} = (g x_1 g^{-1}) (g x_2 g^{-1}) \dots (g x_r g^{-1}) \in G^{(i)}$$

$$\therefore (g x g^{-1}) \in G^{(i)}$$

where $g \in G, x \in G^{(i)}$

$\therefore G^{(i)}$ is a normal subgroup of G

This complete the proof by induction.

Theorem :

A group G is solvable iff $G^{(k)} = \{e\}$ for some (+ve) integer k .

Proof :

Let $G^{(k)} = \{e\}$ for some (+ve) integer k . Then $G \supset G^{(1)} \supset G^{(2)} \dots G^{(k)} = \{e\}$ is a solvable series for G .

because $G^{(i)} =$ commutator subgroup of $G^{(i-1)}$.

$\therefore G^{(i)}$ is a normal subgroup of $G^{(i-1)}$ and $\frac{G^{(i-1)}}{G^{(i)}}$ is abelian.

$\therefore G$ is solvable.

Conversely,

If G is solvable, G has a solvable series, say

$$G \supset G_1 \supset G_2 \supset \dots \supset G_k = \{e\}$$

Each G_i is a normal in G_{i-1} and $\frac{G_{i-1}}{G_i}$ is abelian.

$\frac{G}{G_1}$ is abelian $G^{(1)} \subset G$.

Induction hypothesis $G^{(1)} \subset G$

To P.T

$$G^{(i+1)} \subset G_{i+1}$$

Let $x \in G^{(i+1)}$

$$x = x_1, x_2, \dots, x_r$$

where each

$$x_j = a_j b_j a_j^{-1} b_j^{-1}$$

where

$$a_j, b_j \in G^{(i)} \subset G_i \quad [\forall j=1, 2, \dots, r]$$

$\frac{G_i}{G_{i+1}}$ is abelian.

G_{i+1} contains the commutator

subgroup of G_i .

$$\Rightarrow x_j = a_j b_j a_j^{-1} b_j^{-1} G_i^{-1}, [j = 1 \dots r]$$

$$x = x_1, x_2, \dots, x_r \in G_{i+1}$$

$$\therefore G^{(i+1)} \subset G_{i+1}$$

The proof by induction is complete

$$G^{(i)} \subset G_i \quad [\forall i \geq 1]$$

In particular

$$G^{(k)} \subset G_{(k)} = \{e\}$$

$$\therefore G^{(k)} = \{e\}$$

Lemma :

A solvable group always contains an abelian normal subgroup

Proof :

If G is solvable

$G^{(k)} = \{e\}$ for some (+ve) integer k .

$G^{(k)} =$ Commutator subgroup of $G^{(k-1)}$

∴ $G^{(k-1)}$ is abelian.

$G^{(k-1)}$ is the required abelian normal subgroup of G .

The lower central series for G is defined as follows :

$G_{(1)} = G^{(1)} =$ Commutator subgroup of G .

$G_{(2)} =$ subgroup generated by $\{aba^{-1}b^{-1}; a \in G, b \in G_{(1)}\}$

$G_{(i)} =$ subgroup generated by $\{aba^{-1}b^{-1}; a \in G, b \in G_{(i-1)}\}$

Induction hypothesis; Assume $G^{(1)} \subset G_{(1)}$

To P.T. $G^{(i+1)} \subset G_{(i+1)}$

Let $x \in G^{(i+1)}$

$$x = x_1 x_2 \dots x_r$$

where each $x_j = a_j b_j a_j^{-1} b_j^{-1}$

$$a_j b_j \in G^{(i)}.$$

The result is true $j = 1, 2, \dots, r$.

$$a_j b_j \in G^{(1)} \subset G_{(1)} \quad (\text{By Induction hypothesis})$$

$$x_j = a_j b_j a_j^{-1} b_j^{-1} \in G_{(i+1)}$$

$$x = x_1 x_2 \dots x_r \in G_{(i+1)}$$

$$G^{(i+1)} \subset G_{(i+1)}$$

The proof by induction is complete.

To P.T. each $G_{(i)}$ is normal subgroup of G .

Proof :

$G_{(1)} =$ Commutator subgroup of G .

$G_{(1)}$ is normal in G .

Induction hypothesis; Assume $G_{(1)}$ is normal in G .

To P.T. $G_{(i+1)}$ is normal in G .

Let $g \in G, x \in G_{(i+1)}$

$$x = x_1, x_2, \dots, x_r$$

where

$$x_j = a_j b_j a_j^{-1} b_j^{-1}$$

where

$$a_j \in G, b_j \in G_{(i)}$$

$$gx_j g^{-1} = (ga_j g^{-1})(gb_j g^{-1})(ga_j^{-1} g^{-1})(gb_j^{-1} g^{-1})$$

$$a_j^{-1} = ga_j g^{-1} \in G$$

[$\because b_j \in G_{(i)}$ and $G_{(i)}$ is a normal in G]

$$gx_j g^{-1} = a_j^{-1} b_j^{-1} (a_j^{-1})^{-1} (b_j)^{-1} \in G_{(i+1)} \quad [j=1, 2, \dots, r]$$

$$gxg^{-1} = (gx_1 g^{-1})(gx_2 g^{-1}) \dots (gx_r g^{-1}) \in G_{(i+1)}$$

$\therefore$

$$gxg^{-1} \in G_{(i+1)}$$

where

$$x \in G_{(i+1)} \text{ and } g \in G$$

$\Rightarrow G_{(i+1)}$ is a normal subgroup of G .

Nilpotent :

Definition :

A group G is said to be nilpotent if $G_{(k)} = \{e\}$ for some (+ve) k .

If G is abelian $G_{(1)} = \{e\}$

$\Rightarrow G$ is nilpotent.

A nilpotent group is solvable.

If G is nilpotent $G_{(k)} = \{e\}$

[for some (+ve) integer $k = \{e\}$]

$$G^{(k)} \subset G_{(k)} = G^{(i)} = \{e\}$$

$\therefore G$ is solvable.

The converse is not true.

$$S_3 \supset A_3 \supset \{e\} \text{ is a solvable series for } A_3.$$

Proof :

$$G_{(1)} = A_3$$

$$G_{(2)} = \text{subgroup generated by } \{\sigma\ell\sigma^{-1}\ell^{-1}; \sigma \in S_3; \ell \in G_1 = A_3\}$$

$$(12)(123)(12)(132) \in G_{(2)}$$

$$(213)(132) \in G_{(2)}$$

$$\circ \quad (123) \in G_{(2)}$$

$$\Rightarrow G_{(2)} = A_3 = G_{(1)}$$

$$\Rightarrow G_{(3)} = G_{(2)} = G_{(1)} = A_3$$

$$\Rightarrow G_{(n)} = A_3 \quad [\forall n \geq 1]$$

$\circ S_3$ is not nilpotent, even though it is solvable.

Theorem :

A group of order p^n is nilpotent where p is a prime.

Proof :

The proof is by induction on n . If $n=1$, and if G is a group of order p^1 .

G is abelian and hence nilpotent.

Induction hypothesis ;

Assume the result for all groups of order p^α .

where $0 \leq \alpha < n$

Let G be a group of order p^n .

If z is the centre of G .

$$z \neq \{e\}$$

$$O(z) = p^\alpha, 0 \leq \alpha \leq n$$

$$P/O(z) \Rightarrow \exists a \in z, a \neq e, \text{ s.t. } a^p = e \quad (\text{cauchy thm})$$

Let $H = \langle a \rangle$, the cyclic subgroup generated by a .

$$\circ O(H) = P.$$

H is normal in G , because if $x \in G, h \in H$

$$h = a^r \in z$$

$$xhx^{-1} = xa^r x^{-1}$$

$$= a^r = h \in H$$

$$O(G/H) = \frac{O(G)}{O(H)} = \frac{p^n}{p} = p^{n-1}$$

By induction hypothesis G/H is nilpotent.

$(G/H)_{(k)} = \{H\}$ for some positive integer k .

Theorem :

A subgroup of a nilpotent group is nilpotent.

Proof :

Let H be a subgroup of a nilpotent group G .

G is nilpotent $G_{(k)} = \{e\}$

(for some (+ve) integer k)

$H_{(1)} =$ subgroup generated by $(aba^{-1}b^{-1}; a, b \in H)$

$G_{(1)} =$ subgroup generated by $(aba^{-1}b^{-1}; ab \in G)$

∴

$$H_{(1)} \subset G_{(1)}$$

Induction hypothesis; Assume that

$$H_{(i-1)} \subset G_{(i-1)}$$

To P.T. $H_{(i)} \subset G_{(i)}$

$H_{(i)} =$ Subgroup generated by $\{aba^{-1}b^{-1}; a \in H, b \in H_{(-i)}\}$

$G_{(i)} =$ Subgroup generated by $\{aba^{-1}b^{-1}; a \in G, b \in G_{(-i)}\}$

∴

$$H_{(i)} \subset G_{(i)} \quad [\forall i \geq 1]$$

∴

$$H_k \subset G_{(k)} = \{e\}$$

⇒

$$H_{(k)} = \{e\}$$

⇒

H is nilpotent.

This proves the thm.

Theorem :

The homomorphic image of a nilpotent group is nilpotent.

Proof :

Let f be a homomorphism of a nilpotent group G onto a group $\bar{G}$

To P.T. $\bar{G}$ is nilpotent.

G is nilpotent $\Rightarrow G_{(k)} = \{e\}$ (for some (+ve) integer k)

Let $\bar{x} \in \bar{G}_{(1)}$

$$\bar{x} = \overline{x_1 x_2 \dots x_r}$$

where

$$\bar{x}_j = \overline{a_j b_j (a_j)^{-1} (b_j)^{-1}} \text{ \& } \overline{a_j}, \overline{b_j} \in \bar{G}$$

since

$$f : G \rightarrow \bar{G} \text{ is onto } \exists a_j, b_j \in G$$

s.t.

$$f(a_j) = \overline{a_j}, f(b_j) = \overline{b_j}$$

$$\bar{x}_j = f(a_j) f(b_j) [f(a_j)]^{-1} [f(b_j)]^{-1}$$

$$= f(a_j b_j a_j^{-1} b_j^{-1})$$

$$\in f(G_{(1)}) \quad (\forall j=1, \dots, r)$$

$$\bar{x} = \overline{x_1 x_2 \dots x_r} \in f(G_{(1)})$$

$$\bar{G}_{(1)} \subset f(G_{(1)})$$

Induction hypothesis :

Assume

$$\bar{G}_{(i-1)} \subset f(G_{(i-1)})$$

To. P.t.

$$\bar{G}_{(i)} \subset f(G_{(i)})$$

Let

$$\bar{x} \in \bar{G}_{(i)}$$

$$\bar{x} = \overline{x_1, x_2, \dots, x_r}$$

where

$$\bar{x}_j = \overline{a_j b_j a_j^{-1} b_j^{-1}}$$

where

$$\overline{a_j} \in \bar{G}, \overline{b_j} \in \bar{G}_{(i-1)} \subset f(G_{(i-1)})$$

$\exists$

$$a_j \in G \text{ s.t. } f(a_j) = \overline{a_j}$$

$$\overline{b_j} \in f(G_{(i-1)}) \Rightarrow \overline{b_j} = f(b_j) \text{ for } b_j \in G_{(i-1)}$$

$$\bar{x}_j = f(a_j)f(b_j)[f(a_j)]^{-1}[f(b_j)]^{-1}$$

$$= f(a_j b_j a_j^{-1} b_j^{-1})$$

$$\in f(G_{(i)}) \quad [\forall j=1, \dots, r]$$

$$\bar{x} = \bar{x}_1, \bar{x}_2, \dots, \bar{x}_r \in f(G_{(i)})$$

$$\circ \quad \bar{G}_{(i)} \subset f(G_{(i)}) \quad [\forall i \geq 1]$$

In particular

$$\bar{G}_{(k)} \subset f(G_{(k)}) = f(e) = \{e\}$$

$$\Rightarrow \bar{G}_{(k)} = \{e\}$$

$\circ \quad \bar{G}$ is nilpotent.

This proves the thm.

The quotient group of G is nilpotent group is nilpotent.

Because the quotient group is a homomorphic image of nilpotent.

Lemma :

A nilpotent group has a non-trivial centre.

Proof :

Let G be a nilpotent group.

$$G_{(k)} = \{e\} \text{ (for some +ve integer } k)$$

Let k be (+ve) first integer s.t. $G_{(k)} = \{e\}$

$$G_{(k-1)} \neq \{e\}$$

$$\text{If } b \in G_{(k-1)}$$

$$\text{If } a \in G.$$

$$aba^{-1}b^{-1} \in G_k = \{e\}$$

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

$$\circ \quad ab = ba, \quad \forall a \in G$$

$$\Rightarrow b \in \text{centre of } G.$$

$$G_{(k-1)} \subset \text{centre of } G.$$

∴ The centre of G is nontrivial.

Lemma :

A homomorphic image of a nilpotent group different from identity has a non-trivial centre.

Proof :

Let $\bar{G}$ be the homomorphic image of a nilpotent group G .

$$\bar{G} \neq \{e\}$$

∴ $\bar{G}$ is nilpotent and hence has a nontrivial centre.

Lemma :

If H is subgroup of a nilpotent group G , then $N(H) \neq H$

Proof :

$$N(H) = \{x \in G; xHx^{-1} = H\}$$

$$N(H) = G \text{ iff } H \text{ is normal in } G.$$

Since G is nilpotent $G_{(k)} = \{e\}$ for some (+ve) integer k .

Consider the lower central series.

$$G \supset G_{(1)} \supset G_{(2)} \supset \dots \supset G_{(k)} = \{e\}$$

$$\exists G_{(i)} \text{ s.t. } G_{(i)} \not\subset H \text{ is not contained in } H.$$

$$G_{(i)} \subset H$$

$$\text{then } \exists x \in G_{(i-1)}, x \notin H$$

$$\text{Let } h \in H$$

$$xhx^{-1}h^{-1} \in G_{(i)} \subset H$$

$$\Rightarrow (xhx^{-1}h^{-1})h \in H$$

$$\Rightarrow xhx^{-1} \in H \quad \forall h \in H$$

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

$$\Rightarrow x \in N(H), x \notin H$$

$$\therefore N(H) \neq H$$

Definition : (Composition Series)

A series of subgroups $G = G_0 \supset G_1 \supset \dots \supset G_k = \{e\}$ is said to be a composition series for G if G_i is normal in G_{i-1} and $\frac{G_{i-1}}{G_i}$ is simple.

It $S_3 \supset A_3 \supset \{e\}$

$$0\left(\frac{S_3}{A_3}\right) = 2 \Rightarrow \frac{S_3}{A_3} \text{ is simple.}$$

$$0\left(\frac{A_3}{\{e\}}\right) = 3 \Rightarrow \frac{A_3}{\{e\}} \text{ is simple.}$$

The length of the above composition series is said to be k . The quotient groups $\frac{G_{i-1}}{G_i}$ are called the factors of the composition series.

Theorem :

Every finite group has a composition series.

Proof :

The proof is by induction on the order of the groups.

If $0(G) = 1$

$G = \{e\}$

This is the only composition series for G . Induction hypothesis. Assume take every group whose order K less than $o(G)$ has a composition series.

If G is simple.

$G \supset \{e\}$ is the only composition series for G .

If G is not simple.

Let M be the normal subgroup in G of maximum order in G . By induction hypothesis, N has a composition series.

$N = N_0 \supset N_1 \supset N_2 \supset \dots \supset N_k = \{e\}$

If G/N has a proper normal subgroup H/N .

Then H will be a proper normal subgroup of G containing N .

Induction hypothesis :

This contradicts our choice of N

∴ G/N is simple.

$$G \supset N \supset N_1 \supset N_2 \supset \dots \supset N_k = \{e\}$$

This is the required composition series for G.

The proof by induction is complete.

Let G be a cyclic group of order 12 generated by a $G = \langle a \rangle$,

$$H_1 = \langle a^2 \rangle = \{a^2, a^4, a^6, a^8, a^{10}, a^{12} = e\}$$

G/H is simple.

$$\begin{aligned} H^2 &= \langle a^4 \rangle \\ &= \{a^4, a^8, a^{12} = e\} \end{aligned}$$

$$O\left(\frac{H_1}{H_2}\right) = \frac{6}{3} = 2 \Rightarrow \frac{H_1}{H_2} \text{ is simple.}$$

$\frac{H_3}{\{e\}}$ is simple

$$G \supset H_1 \supset H_2 \supset H_3 = \{e\}$$

Is a composition series for G with length 3.

The composition factors are

$$G/H_1, H_1/H_2, H_2/H_3$$

there are orders 2, 2, 3

$$\begin{aligned} \text{Let } K_1 &= \langle a^3 \rangle \\ &= \{a^3, a^6, a^9, a^{12} = e\} \end{aligned}$$

$$O\left(\frac{G}{K_1}\right) = \frac{12}{4} = 3 \Rightarrow \frac{G}{K_1} \text{ is simple.}$$

$$\begin{aligned} \text{Let } k_2 &= \langle a^6 \rangle \\ &= \{a^6, a^{12} = e\} \end{aligned}$$

$$O\left(\frac{k_1}{k_2}\right) = \frac{4}{2} = 2$$

$\Rightarrow \frac{k_1}{k_2}$ is simple.

Another composition series for G .

$G \supset k_1 \supset k_2 \supset k_3 = \{e\}$ is another composition series for G of length 3.

The Composition factors are

$$\frac{G}{k_1}, \frac{G}{k_2}, k_2$$

There are orders of 3, 2, 2

$$\frac{G_1}{H_1} \approx \frac{k_1}{k_2}$$

$$\frac{H_1}{H_2} \approx \frac{k_2}{\{e\}}$$

$$\frac{H_2}{\{e\}} \approx \frac{G}{k_1}$$

Jordan Holder Theorem :

Any two composition series for a group have the same length. The composition factors of both the series can be paired off so that paired factors are isomorphic.

Proof :

The proof is by induction of the order of G .

If $0(G) = 1 \Rightarrow G = \{e\}$

Is the only composition series for G . Assume $0(G) > 1$.

If $G = G_0 \supset G_1 \supset G_2 \supset \dots \supset G_k = \{e\}$ (1)

and

$G = H_0 \supset H_1 \supset H_2 \supset \dots \supset H_l = \{e\}$ (2)

are two composition series for G .

If $k = 1$, G is simple, then $l = 1$. The thm is trivially true in this case. Assume that both k and l are greater than 1.

Induction hypothesis :

Assume the result to be true for all groups whose order is less than $0(G)$.

Case (i) :

$$G_1 = H_1$$

$$G = G_1 \supset G_2 \supset \dots \supset G_k = \{e\} \dots \dots (3)$$

$$G_1 = H_1 \supset H_2 \supset \dots \supset H_l = \{e\} \dots \dots (4)$$

are two composition series for G_1 .

Since $0(G_1) < 0(G)$

By the induction hypothesis (3) and (4), have the same length and the composition factors of (3) and (4) can be paired off so that the paired factors are isomorphic.

$$\therefore k-1 = l-1 \Rightarrow k = l.$$

The composition factor of (1) are the same as those of (3) along with G/G_1 .

The composition factors of (2) are the same as those of (4) along with $G/H_1 = G/G_1$.

The composition factors of (1) can be paired off with the composition factors of (2). So that the paired factors are isomorphic.

This complete the proof of the thm in this case.

Case (ii) :

$$G_1 \neq H_1$$

G_1 and H_1 are both normal subgroup of G .

G_1H_1 and $G_1 \cap H_1$ are normal subgroup of G .

$$\text{Let } F = G_1 \cap H_1$$

Let $F = F_0 \supset F_1 \supset F_2 \dots \supset F_r = \{e\} \dots \dots (5)$ be a composition of F .

$\frac{G_1H_1}{G_1}$ is a normal subgroup of G/G_1 . Since (1) is composition series for G . G/G_1 is

simple.

$$\therefore \frac{G_1H_1}{G_1} = \frac{G}{G_1} \quad [\therefore G_1H_1 \neq G_1]$$

$$\Rightarrow G_1 H_1 = G$$

$$\circ \quad \frac{G}{H_1} = \frac{G_1 H_1}{H_1} \approx \frac{G_1}{G_1 \cap H_1} = \frac{G_1}{F} \quad (\text{third law homomorphism})$$

$\Rightarrow G/H_1$ is simple $\Rightarrow G_1/F$ is simple.

$$\circ \quad \frac{G}{G_1} = \frac{G_1 H_1}{G_1} \approx \frac{H_1}{G_1 \cap H_1} = \frac{H_1}{F}$$

$$\circ \quad \frac{G_1}{F} \text{ and } \frac{H_1}{F} \text{ are simple.}$$

$$\text{and } \frac{G_1}{F} \approx \frac{G}{H_1} \text{ and } \frac{H_1}{F} \approx \frac{G}{G_1}$$

$$\circ \quad G \supset G_1 \supset F \supset F_1 \supset F_2 \dots \dots \supset F_r = \{e\} \quad \dots \dots (6)$$

and

$$G \supset H_1 \supset F \supset F_1 \dots \dots \supset F_r = \{e\} \quad \dots \dots (7)$$

are two composition series for G of the same length.

The composition factors of (6) and (7) can be paired off so that the paired factors are isomorphic.

Comparing (1) and (6), we see by case (i) that both of them should have the same length. ie) $k = r+2$, and the composition factors of (1) and (6) can be paired off so that the paired factors are isomorphic.

Comparing composition series (2) and (7) by case (i) we see that they should have the same length, ie) $l = r+2$ and the composition factors of (2) and (7) can be paired off so that the paired factors are isomorphic, $k = r+2 = l$.

$\circ$ (1) and (2) have the same length and the composition factors of (1) and (2) can be paired off so that the paired factors are isomorphic.

$\circ$ This completes the proof of the Jordan Holder thm.

Lemma :

Converse of the Jordan holder is not true.

Proof :

$$G_1 = S_3$$

$$S_3 A_3 \supset \{i\}$$

$$0\left(\frac{S_3}{A_3}\right) = 2, 0\left(\frac{A_3}{\{i\}}\right) = 3$$

∴ S_3 is non abelian.

Let G_2 be the cyclic group of order 6. G_2 is abelian G_1 is not isomorphic to G_2 .

$$H = (a^2) = (a^2, a^4, a^6 = e)$$

$$G_2 \supset H \supset \{e\}$$

$$0\left(\frac{G_2}{H}\right) = 2, 0\left(\frac{H}{\{e\}}\right) = 3 \text{ is a composition series for } G_2.$$

$$\frac{S_3}{A_3} \approx \frac{G_2}{H}$$

$$\frac{A_3}{\{i\}} \approx \frac{H}{\{e\}}$$

∴ The converse of Jordan holder thm.

isomorphic is not true.

Division Ring :

Definition : (Associative ring)

Field :

$a + b$ is in R .

A field is a commutative division ring.

$a + b = b + a$

Euclidean ring :

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

There is an element $0 \in R$ such that

An integral domain R is said to be an Euclidean ring if there is a function $f: R \setminus \{0\} \rightarrow \mathbb{N}$ such that

(i) $\forall a, b \in R, b \neq 0, \exists q, r \in R$ such that $a = bq + r$ and $f(r) < f(b)$

There exists an element $-a \in R$

(ii) For any $a, b \in R$ both non-zero, $\exists t, r \in R$ such that $a = bt + r$ and $f(r) < f(b)$

such that $a + (-a) = 0$

$f(b) < f(r)$

$a.b$ is in R .

$a.(b.c) = (a.b).c$

RING THEORY

Introduction :

Groups were studied in the previous chapter, and the definition of a group involves a single binary operation. We know that there are two binary operations, viz, addition and multiplication on the number systems such as integers, rational, real or complex numbers, and with respect to addition they form a group. Also the non-zero rational, real or complex numbers form a group for multiplication. Many of the properties of numbers depend simultaneously on both operations of addition and multiplication. The two operations are interrelated. This leads us to the study of algebraic systems with two binary operations. In this chapter we shall study one such algebraic system. It has two binary operations subject to axioms similar to the properties satisfied by addition and multiplication in $\mathbb{Z}$. Such an algebraic system will be called a ring. We shall give an axiomatic definition of a ring and study some of its elementary properties. These results will then be applied to particular types of rings such as Euclidean rings, principal ideal rings and unique factorisation rings. We shall then study the interrelation between these rings and apply the results to the special case of the polynomial ring.

Rings :**Definition : (Associative ring)**

A non-empty set R is said to be an associative ring if in R . There are defined two operations, denoted by '+' and '.' respectively, such that for all $a, b, c \in R$.

1. $a + b$ is in R .
2. $a + b = b + a$
3. $(a + b) + c = a + (b + c)$
4. There is an element $0 \in R$ such that
 $a + 0 = a$ (for every $a \in R$)
5. There exists an element $-a \in R$
such that $a + (-a) = 0$.
6. $a.b$ is in R .
7. $a.(b.c) = (a.b).c$

8. $a.(b+c) = a.b+a.c$ and

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

The axioms 1–5 state that '+' is an abelian group. Condition 6 says R is closed under multiplication. Condition 7 shows that multiplication is associative in R.

Ring with unit element (or) identity element :

If there is an element $1 \in R$ s.t. $a.1=1.a=a, \forall a \in R$. Then R is said to be a ring with unit element (or) identity element.

Commutative ring :

If the multiplication of R is such that $a.b=b.a, \forall a,b \in R$ then R is said to be a commutative ring.

Zero Divisor :

If R is a commutative ring, then $a \neq 0 \in R$ is said to be a zero divisor.

if there exists $a,b \in R, b \neq 0$ s.t. $a.b = 0$

Integral Domain :

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

Division Ring :

A ring is said to be a division ring if its non-zero elements form a group under multiplication.

Field :

A field is a commutative division ring.

Eudidean ring :

An integral domain R is said to be an Eudidean ring if $\forall a \neq 0 \in R$. There is defined a non-negative integer $d(a)$ such that

(i) $\forall a,b \in R$, both non-zero $d(a) \leq d(ab)$

(ii) For any $a,b \in R$ both non-zero, $\exists t,r \in R$ such that $a = tb+r$ where either $r=0$ or $d(r) < d(b)$.

Ideal :

Let R be a ring. I is said to be an ideal of R if,

(i) $a-b \in I, \quad \forall a, b \in I$

(ii) when $a \in I, r \in R, ar, ra \in I$

Greatest Common divisor :

If $a, b \in R$ then $d \in R$ is the greatest common divisor of a and b if

(i) d/a & d/b .

(ii) whenever c/a & c/b then c/d .

The notation used is $(a, b) = d$

Associates :

In a ring R , if a/b & b/a then a and b are called associates.

Ex ample :

- (i) $R = \mathbb{Z}$, the ring of integers, is a ring for the usual addition and multiplication. It has 1 as unit element, and is commutative.
- 2) $R = 2\mathbb{Z}$ the ring of even integers, is also a ring for the usual addition and multiplication. It has no unit element, but is commutative.

Properties :

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

(i) $a0 = 0a = 0$

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

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

If, in addition, R has a unit element 1, then

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

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

(vi) $a(b-c) = ab-ac$

Proof :

To P.T.

$$\begin{aligned}
 (i) \quad & a \cdot 0 = 0 \cdot a = 0 \\
 \text{consider} \quad & a \cdot 0 = a \cdot (0+0) \\
 \Rightarrow \quad & a \cdot 0 = a \cdot 0 + a \cdot 0 \quad (\text{By distributive law}) \\
 \Rightarrow \quad & a \cdot 0 + 0 = a \cdot 0 + a \cdot 0 \\
 \Rightarrow \quad & 0 = a \cdot 0 \quad (\text{by cancellation law})
 \end{aligned}$$

$$\begin{aligned}
 \text{III}^{\text{ly}} \quad & 0 \cdot a = (0+0) \cdot a \\
 & = 0 \cdot a + 0 \cdot a \quad (\text{by distributive law}) \\
 & 0 = 0 \cdot a \quad (\text{By cancellation law})
 \end{aligned}$$

$$\text{Hence} \quad a \cdot 0 = 0 \cdot a = 0$$

$$(ii) \quad \text{To P.T. } a(-b) = (-a) \cdot b = -(ab) \quad \forall a, b \in R.$$

$$\begin{aligned}
 \circ \quad & a \cdot 0 = 0 \\
 & a(-b+b) = 0 \\
 & a(-b)+ab = 0 \\
 & a(-b) = -(ab)
 \end{aligned}$$

$$\text{III}^{\text{ly}} \quad 0 \cdot b = 0$$

$$\begin{aligned}
 \Rightarrow \quad & (-a+b) \cdot b = 0 \\
 \Rightarrow \quad & (-a)b+ab = 0 \\
 \Rightarrow \quad & (-a)b+ab = 0 \\
 \Rightarrow \quad & (-a)b = -(ab)
 \end{aligned}$$

$$\circ \quad a(-b) = (-a)b = -(ab), \quad \forall a, b \in R$$

$$\begin{aligned}
 (iii) \quad \text{To P.T.} \quad & (-a)(-b) = ab \\
 & (-a)(-b) = -[a(-b)] \quad [\text{by (ii)}]
 \end{aligned}$$

$$\begin{aligned}
 \Rightarrow \quad & (-a)(-b) = -[-ab] \\
 \Rightarrow \quad & (-a)(-b) = ab
 \end{aligned}$$

$$(iv) \quad \text{Suppose that } R \text{ has a unit elements } 1$$

$$\begin{aligned}
 \text{Then} \quad & a+(-1) \cdot a = 1 \cdot a+(-1)a \\
 & = (1+(-1)) \cdot a
 \end{aligned}$$

$$= 0.a = 0 \quad 0 = a.0 = 0.a \quad (i)$$

$$a+(-1).a = 0 \quad (0+0).a = 0.a \quad \text{consider}$$

$$\circ \quad a+(-1).a = 0 \quad (By distributive law) \quad a.0 + a.0 = 0.a \quad \Rightarrow$$

$$\Rightarrow (-1).a = -a \quad a.0 + 0.a = 0 + 0.a \quad \Rightarrow$$

$$(v) \text{ To P.T } (-1)(-1) = 1 \quad (by cancellation law) \quad 0.a = 0 \quad \Rightarrow$$

$$\text{we know that } (-1).a = -a \quad a.(0+0) = a.0 \quad \text{Hence}$$

$$\text{If } a = -1 \quad (by distributive law) \quad a.0 + a.0 = 0.a + 0.a = 0 \quad \Rightarrow$$

$$(-1)(-1) = -(-1) \quad (By cancellation law) \quad 0.a = 0 \quad \Rightarrow$$

$$= 1 \quad 0.a = 0 \quad \Rightarrow$$

$$\Rightarrow (-1)(-1) = 1 \quad \text{P.T. } a(-b) = (-a).b = -(ab) \quad \text{To (ii)}$$

$$(vi) \text{ To P.T } \quad 0.a = 0 \quad \circ$$

$$a(b-c) = ab - ac \quad 0 = (d+b).a \quad \Rightarrow$$

$$a(b-c) = a(b+(-c)) \quad 0 = a(-b)+ab = 0 \quad \Rightarrow$$

$$= ab+a(-c) \quad (a(-b)) = (-a).b = -(ab) \quad \Rightarrow$$

$$\Rightarrow a(b-c) = ab - ac \quad \text{Hence}$$

This proves the properties.

Theorem :

Every field is an integral domain

Proof :

Let R be a field

Suppose $a \in R, b \in R, a \neq 0, b \neq 0$ and $ab = 0$

Since R is a field.

And $b \neq 0$

And b has an inverse b^1 .

$$bb^1 = b^1b = 1 \quad (iv) \text{ Suppose that R has a unit element 1}$$

$$\text{Now } (ab)b^1 = 0(b^1) = 0 \quad \text{Then } a+(-1).a = 1.a+(-1).a$$

$$\text{but } (ab)b^1 = a(bb^1) = a.1 = a \quad (1+(-1)).a = 0$$

Hence $a = 0$

which is $a \Rightarrow \Leftarrow$

Thus $ab \neq 0$

∴ R is an integral domain

Cor :

If R is a ring with unit element, and $b \in R$, which is regular, then b is not a zero divisor.

Cor :

z_n is not a field, when n is not a prime.

Proof :

If n is not a prime

∴ $n = m_1 \cdot m_2$ where m_1, m_2 are proper divisors.

Hence

$$\overline{m_1 \cdot m_2} = \overline{m_1 m_2} = \overline{n} = \overline{0}$$

$$\therefore \overline{m_1} \neq \overline{0}, \overline{m_2} \neq \overline{0}$$

Hence z_n is not an integral domain.

Hence it is not a field.

The converse of every field is an integral domain is not true.

because z is an integral domain which is not a field.

Lemma :

Let R be a finite integral domain. Then R is a field.

Proof :

Let $R = \{a_1, a_2, \dots, a_n\}$ be a finite

non-zero integral domain. Let $0 \neq a \in R$ be any element.

Then $aa_1, aa_2, \dots, aa_n$ are all in R .

If $aa_i = aa_j$ for some $i \neq j$

(by cancellation law)

$$a_i = a_j$$

which is not true.

Hence $aa_1, aa_2, \dots, aa_n$ are distinct member of R .

Since $a \in R$, $a = aa_i$ for some i

Let $x \in R$ be any element,

$$\text{then } x = aa_j \text{ for some } j$$

$$\circ x = a_i x$$

Hence using commutativity we find,

$$x = a_i x = x a_i$$

(or) that a_i is unity of R .

$$\text{Let } a_i = 1$$

Thus for $1 \in R$

$$\circ 1 = aa_k \text{ for some } k$$

we find a_k is multiplicative inverse of a .

Hence any non-zero element of R has

multiplicative inverse (or) that R is a field.

Hence the lemma.

Corollary :

For any prime p , $\mathbb{Z}_p$ is a field.

Proof :

$\mathbb{Z}_p$ is an integral domain.

$$\text{If } \overline{a}\overline{b} = \overline{0}$$

$$\circ \overline{a}\overline{b} = \overline{0}$$

then $p|ab$.

Since p is a prime, $p|a$ or $p|b$

$$\circledast \bar{a} = \bar{0} \text{ or } \bar{b} = \bar{0}$$

Hence Z_p is an integral domain, and since it is a finite ring.

$\circledast Z_p$ is a field.

Definition :

Let R be a ring. The characteristic of R is the smallest positive integer n if it exists such that $na=0 \forall a \in R$.

If no such integer exists, the characteristic of R is said to be zero.

We use the abbreviation ch to denote the characteristic of R .

Example :

- 1) If R is the field of rational, real or complex numbers, then $chR = 0$
- 2) $ch Z_n = n$, because $\overline{na} = \bar{0} \forall a \in Z_n$ and n is the smallest (+ve) integer with this property.

Lemma :

Let R be a ring with unit element e . Then (i) $chR = n$, if n is the smallest (+ve) integer such that $ne = 0$

(ii) $chR = 0$ if no such n exists.

Proof :

(i) Suppose n is the smallest (+ve) integer such that $ne = 0 = 0 \cdot e$

Then for any $a \in R$,

$$\begin{aligned} na &= a+a+\dots+a \text{ (n times)} \\ &= a\ell+a\ell+\dots+a\ell \text{ (n times)} \\ &= a(\ell+\ell+\dots+\ell) \\ &= a(n\ell) \\ &= a \cdot 0 \\ &= 0 \end{aligned}$$

Also for $0 < m < n$, $me \neq 0$

Hence $chR = n$

(ii) Suppose no such n exists,

then $\text{ch}R = 0$

Then $\exists$ some $m > 0$, with $ma = 0 \forall a \in R$

In particular $m1 = 0$, $m > 0$

which is impossible.

Lemma :

Let R be an integral domain. Then $\text{Ch}R = 0$ or a prime.

Proof :

Suppose $\text{Ch}R = n \neq 0$

Suppose n is not a prime.

Then $n = m_1 m_2$

where m_1 and m_2 are proper divisors of n .

For any $a \in R$, $a \neq 0$

we have

$$0 = na^2 = (m_1 m_2) a^2 = (m_1 a)(m_2 a)$$

Since R is an integral domain.

$$m_1 a = 0 \text{ (or) } m_2 a = 0$$

Suppose $m_1 a = 0$

Then we show that $m_1 x = 0$ for any $x \in R$

$$\text{now } m_1(xa) = (m_1 x)a = x(m_1 a) = x \cdot 0 = 0$$

since $a \neq 0$, and R is an integral domain $m_1 x = 0$

$$\text{Thus } m_1 x = 0 \forall x, m_1 < n$$

This is $\Rightarrow \Leftarrow$

The assumption that $\text{Ch}R = n$

Hence n is a prime

Hence the Lemma.

Definition :

A ring R is called a Booleam ring if $x^2 = x \quad \forall x \in R$

Problem :

Show that a Booleam ring is commutative.

Solution :

Let $a, b \in R$ be any elements

Then $a+b \in R$ (closure)

By given condition

$$(a+b)^2 = a+b$$

$$\Rightarrow a^2 + b^2 + ab + ba = a+b$$

$$\Rightarrow a + b + ab + ba = a+b$$

$$\Rightarrow ab + ba = 0$$

$$\Rightarrow ab = -ba$$

$$\Rightarrow a(ab) = a(-ba)$$

$$\Rightarrow a^2b = -aba$$

$$\Rightarrow ab = -aba \quad \dots\dots\dots (2)$$

Again (1) gives

$$(ab)a = -(ba).a$$

$$\Rightarrow aba = -ba^2 = -ba \quad \dots\dots\dots (3)$$

(2) & (3)

$$ab = ba (= -aba)$$

(or) $\circ R$ is Commutative

Homomorphism and Isomorphism

Definition :

A mapping ϕ from the ring R into the ring R^1 is said to be a homomorphism if

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

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

$$\forall a, b \in R$$

Lemma :

If $\theta: R \rightarrow R^1$ be a homomorphism, then

- (i) $\theta(0) = 0^1$
- (ii) $\theta(-a) = -\theta(a)$

where 0 and 0^1 are zeros of the rings R and R^1 respectively.

Proof :

$$\begin{aligned}
 \text{(i)} \quad & \text{Since } 0 + 0 = 0 \\
 & \therefore \theta(0+0) = \theta(0) \\
 \Rightarrow & \theta(0) + \theta(0) = \theta(0) + 0^1 \\
 \Rightarrow & \theta(0) = 0^1.
 \end{aligned}$$

(ii) Again,

$$\begin{aligned}
 \text{As } & a + (-a) = 0 \\
 \Rightarrow & \theta(a + (-a)) = \theta(0) \\
 \Rightarrow & \theta(a) + \theta(-a) = \theta(0) = 0 \\
 \Rightarrow & -\theta(a) = \theta(-a) \\
 \Rightarrow & -\theta(a) = \theta(-a)
 \end{aligned}$$

Hence the lemma.

Definition :

If θ is a homomorphism of R into R^1 , then the kernel of θ , $I(\theta)$, is the set of all elements $a \in R$ such that $\theta(a) = 0$ the zero-element of R^1 .

Example :

Consider the map $f: c \rightarrow c$, s.t $f(a+ib) = a-ib$ then f is a homomorphism, where $c = \text{complex numbers}$,

$$\begin{aligned}
 f[(a+ib)+(c+id)] &= f((a+c)+i(b+d)) \\
 &= (a+c) - i(b+d) \\
 &= (a-ib) + (c-id) \\
 &= f(a+ib) + f(c+id)
 \end{aligned}$$

And

$$\begin{aligned} f[(a+ib) + (c+id)] &= f((ac-bd)+i(ad+bc)) \\ &= (ac-bd)-i(ad+bc) \\ &= (a-ib)c - id(a-ib) \\ &= (a-ib)(c-id) \\ &= f(a+ib) f(c+id) \end{aligned}$$

Definition : (isomorphism)

Let R and R^1 be rings. A mapping $f: R \rightarrow R^1$ is called an isomorphism if

- (i) f is (1,1) and 'onto'
- (ii) $f(a+b) = f(a) + f(b)$, $a, b \in R$
- (iii) $f(ab) = f(a) f(b)$, $a, b \in R$

Lemma :

Let Q be the field of rational numbers. Then the only isomorphism of Q onto Q is the identity mapping I_Q .

Proof :

Let $f: Q \rightarrow Q$ be an isomorphism of Q onto Q . Then $f(1) = 1$

Hence for any $n > 0$

$$\begin{aligned} f(n) &= f(1 + \dots + 1) \text{ (n times)} \\ &= f(1) + \dots + f(1) \text{ (n times)} \\ &= n \cdot f(1) \\ &= n \cdot 1 = n \end{aligned}$$

$$\Rightarrow f(n) = n.$$

$$\text{if } n = -m, m > 0$$

$$\text{then } f(n) = f(-m) = -f(m) = -m = n$$

$$\text{thus } f(a) = a \quad \forall \text{ integers } a.$$

$$\text{Let } a/b \in Q, b > 0$$

$$\text{Then } a = f(a) = f(a/b + a/b + \dots + a/b) \text{ (b times)}$$

$$= f(a/b) + f(a/b) + \dots + f(a/b) \text{ (b times)}$$

$$= b f(a/b)$$

$$\circ \quad f(a/b) = a/b$$

$$\circ \quad f = I_Q. \text{ This proves the lemma.}$$

Lemma :

Let R be a field of real numbers then the only isomorphism of R onto R is the identity mapping I_R .

Proof :

Let $f: R \rightarrow R$ be an isomorphism of R onto R . we have already seen that $f(a) = a$ for any $a \in Q$

Let $x \in R$ s.t. $x > 0$.

$$\text{then } f(x) = f(\sqrt{x})^2 = f(\sqrt{x}) \cdot f(\sqrt{x})$$

$$= f(\sqrt{x})^2 > 0. \text{ Thus } f(x) > 0 \text{ whenever } x > 0.$$

$$\Rightarrow f(\alpha) > f(\beta) \text{ whenever } \alpha > \beta, \alpha, \beta \in R.$$

for any real x ,

choose $\alpha, \beta \in Q$ s.t. $\alpha < x < \beta$.

$$\text{then } f(\alpha) < f(x) < f(\beta)$$

$$\circ \quad < f(x) < \beta.$$

$$\circ \quad \alpha < x < \beta, \alpha, \beta \in Q.$$

It follows that $\alpha < f(x) < \beta$.

$$\Rightarrow f(x) = x.$$

This proves the lemma.

Theorem :

Let C be the field of complex numbers. Then the only isomorphism of C onto C which maps reals to reals is the identity I_C or the conjugation map.

Proof :

Let $f: C \rightarrow C$ be an isomorphism of C onto C .

we have already seen that $f(a) = a$ (for any real a)

Let $z = a+ib \in \mathbb{C}$

Then $f(z) = f(a+ib) = f(a) + f(i).f(b)$

If $f(i) = t$

then $t^2 = \{f(i)\}^2 = f(i^2) = f(-1) = -1$

Thus $t^2 = -1$

$\therefore t = \pm i$

If $t = i$

then $f(a+ib) = a+ib$

$\therefore f = I_{\mathbb{C}}$

If $t = -i$

then $f(a+ib) = f(a) + f(i).f(b)$

$$= a-ib$$

$\therefore f$ is the conjugation map.

This proves the Lemma.

Lemma :

Let $f: R \rightarrow R^1$ be a homomorphism of R in R^1 . Then f is a $(1,1)$ map if and only if $\ker f = 0$

Proof :

Suppose f is $(1,1)$ mapping

Let $K = \ker f$

If $a \in K$, then $f(a) = 0 = f(0)$

Since f is $(1,1)$ mapping

$a = 0$.

Hence $K = 0$.

Conversely,

suppose $K = 0$.

Let $f(a) = f(b), a, b \in R$

then $f(a-b) = f(a) + f(-b)$
 $= f(a) - f(b) = 0$

Hence $a-b \in k$

but $a-b = 0 [\because k=0]$

Hence $a = b$

$\therefore f$ is a (1,1) mapping.

Definition :

Let R be a ring $S \subset R$. S is called a subring of R if (i) S is a sub group of the abelian group R .

i.e.) $a-b \in S$ whenever $a \in S$ & $b \in S$

(ii) S is closed for multiplication

i.e.) $ab \in S$ whenever $a \in S$ & $b \in S$

Example :

1) Let $R=Q$ and $S=Z$ Then S is a subring of R .

2) The ring S of all 2×2 matrices of the type $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ is a subring of the ring of all 2×2 matrices.

Lemma :

Let $f: R \rightarrow R^1$ be a homomorphism of R in R^1 . Then (i) $k = \ker f$ is a subring of R & (ii) $f(R) = \{b/b = f(a)/a \in R\}$ is a subring of R^1 .

Proof :

(i) Let $a \in k, b \in k$

$$f(a) = f(b) = 0$$

Then $f(a-b) = f(a) - f(b) = 0 - 0 = 0$

$\Rightarrow a-b \in k.$

$\therefore f(ab) = f(a).f(b) = 0.0 = 0$

$$\Rightarrow ab \in k$$

Thus k is a subring of R .

$$(ii) \text{ Let } S^1 = f(R) = \{b/b = f(a), a \in R\}$$

$$\text{Let } b, b^1 \in S$$

$$\circ f(a) = b, f(a^1) = b^1, \forall a, b \in R$$

$$b - b^1 = f(a) - f(a^1)$$

$$\circ b - b^1 = f(a - a^1) S^1$$

$$\circ bb^1 = f(a) \cdot f(a^1)$$

$$= f(aa^1) \in S^1$$

$\circ S^1$ is subring of R^1 .

Lemma :

Let R be a ring with unit element 1. Then R is isomorphic to a subring of the ring of endomorphisms of the obelian group R .

Proof :

Let R^1 be the ring of endomorphisms of the obelian grou R .

Define :

$$f: R \rightarrow R^1$$

by $f(a) = f_a$ where f_a is the endomorphism of R .

defined by $f_a(x) = ax, \forall x \in R$

$$\circ a(x+y) = ax + ay \text{ (distributive property in } R)$$

$$\circ f_a \text{ is an endomorphism of the abelian group } R.$$

Hence f is a ring homomorphism

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

$$= ax + bx$$

$$= (a+b)x$$

$$= f_{a+b}(x) \forall x \in R$$

Thus

$$f_a + f_b = f_{a+b}$$

Also

$$\begin{aligned}(f_a \cdot f_b)(x) &= f_a(f_b(x)) \\ &= f_a(bx) = a(bx) \\ &= (ab)x = f_{ab}(x)\end{aligned}$$

$$\Rightarrow f_a \cdot f_b = f_{ab} \quad \forall x \in R$$

These two relations show that f is a ring homomorphism

$$\text{Let } k = \ker f$$

$$\text{Then } a \in k \text{ if and only if } f_a = 0$$

$$f_a(x) = ax = 0 \quad \forall x \in R$$

In particular

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

$$\text{Thus } k = 0$$

Hence f is an isomorphism of R onto R^1 .

Definition :

Let R and R^1 be two rings. R is said to be embedded in R^1 if there exists an isomorphism $f: R \rightarrow R^1$ of R into R^1 . f is called the embedding.

Quotient Fields

In this section we investigate conditions under which a ring R can be embedded in a field. Since a subring of an integral domain is an integral domain, a necessary condition for this to be possible is that R should be an integral domain. We shall show that this condition is also sufficient ie) every integral domain R can be embedded in a field. We shall also find a smallest field in which R can be embedded and show that it is unique up to isomorphism. The construction of this field is similar to the construction of the field Q of rational numbers from the ring Z of integers.

Definition :

Let R and R^1 be two rings. A one-one homomorphism θ from R to R^1 is called an imbedding (embedding) mapping and in that case R^1 is called extension ring or over ring of R .

Theorem :

Every integral domain can be imbedded in a field.

Proof :

Let D be an integral domain

$$\text{Let } S = \{(a,b)/a,b \in D, b \neq 0\}$$

Define a relation $\sim$ on S by

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

It is easy to see that $\sim$ is an equivalence relation. Thus it partitions S into equivalence classes. Let equivalence class of (a,b) be denoted by $[a,b]$. Let F be the set of all these equivalence classes. We show F forms a field under addition and multiplication defined by

$$[a,b] + [c,d] = [ad+bc, bd]$$

$$[a,b].[c,d] = [ac,bd]$$

Addition is well - defined

$$\text{Let } [a,b] = [a^1,b^1] \text{ and } [c,d] = [c^1,d^1]$$

$$\text{Then } (a,b) \sim (a^1,b^1) \text{ and } (c,d) \sim (c^1,d^1)$$

$$\Rightarrow ab^1 = ba^1 \text{ and } cd^1 = dc^1$$

$$\Rightarrow (ab^1)dd^1 = (ba^1)dd^1 \text{ and } (cd^1)bb^1 = (dc^1)bb^1 \dots\dots\dots (1)$$

We want to show that

$$[ad+bc,bd] = [a^1d^1+b^1c^1, b^1d^1]$$

which will hold if

$$(ad+bc, bd) \sim (a^1d^1+b^1c^1, b^1d^1)$$

$$\text{or if } (ad+bc)b^1d^1 = bd(a^1d^1+b^1c^1)$$

$$\text{or if } ab^1dd^1+bb^1cd^1 = ba^1dd^1+bb^1dc^1$$

which is true if we add equations (1) above

Hence addition is well defined

To verify that multiplication is well defined.

$$\text{Let } [a,b] = [a^1,b^1] \text{ and } [c,d] = [c^1,d^1]$$

then

$$\begin{aligned} ab^1 &= ba^1 \text{ and } cd^1 = dc^1 \\ ab^1cd^1 &= ba^1dc^1 \end{aligned} \quad \dots\dots\dots (2)$$

now

$$[a,b].[c,d] = [a^1,b^1][c^1,d^1]$$

$$\text{If } [ac, bd] = [a^1c^1, b^1d^1]$$

$$\text{or if } (ac, bd) \sim (a^1c^1, b^1d^1)$$

$$\text{or if } acb^1d^1 = bda^1c^1$$

which is true by (2)

That addition is commutative and associative will be a routing affaire to prove.

Existence of zero element

Let $[a,b] \in F$ be any element.

$$\text{Then } [a,b] + [0,b] = [ab+b0, b^2]$$

$$\Rightarrow [ab, b^2] = [a,b]$$

$$\Leftrightarrow (ab, b^2) \sim (a, b)$$

$$\Leftrightarrow abb = b^2a$$

$$\Leftrightarrow ab^2 = ab^2$$

Thus $[0,b]$ will be zero of F .

One might notice here that $[0,x] = [0,y]$

for any non-zero, $x, y \in D$

$$\text{As } (0,x) \sim (0,y) \quad 0.y \Leftrightarrow 0.x$$

Existence of additive inverse

For any $[a,b] \in F$

$[a,b]$ will be its additive inverse.

$$\text{As } [a,b] + [-a,b] = [ab-ba, b^2]$$

$$= [0, b^2] = [0, b]$$

Thus $\langle F, + \rangle$ forms an abelian group. We leave it to the reader to verify that multiplication is commutative, associative and is distributive over addition.

Again, since for any $0 \neq x \in D$

And for any $[a, b] \in F$

$$[a, b][x, x] = [ax, bx] = [a, b]$$

we notice $[x, x]$ will act as unity in F . Let now $[a, b]$ be any non-zero element of F .

then $a \neq 0$ (b , of course is non-zero)

So we can talk of $[b, a] \in F$

As $[a, b][b, a] = [ab, ba]$

$$= [ab, ab] = [x, x]$$

We find every non-zero element of F has multiplicative inverse.

Hence F is a field.

We show that D can be imbedded into F .

Define a mapping

$\varphi : D \rightarrow F$ s.t.

$$\varphi(a) = [ax, x] \text{ where } 0 \neq x \in D$$

φ is well defined.

Let $a = b$

Then $ax = bx$

$$\Rightarrow ax, x = bxx$$

$$\Rightarrow (ax, x) \sim (bx, x)$$

$$\Rightarrow [ax, x] = [bx, x]$$

$$\Rightarrow \varphi(a) = \varphi(b)$$

φ is 1-1

Let $\varphi(a) = \varphi(b)$

Then $[ax, x] = [bx, x]$

$$\Rightarrow (ax, x) \sim (bx, x)$$

$$\Rightarrow ax, x = bx, x$$

$$\Rightarrow x^2(a-b) = 0$$

$$\Rightarrow a-b = 0 \text{ as } x^2 \neq 0$$

$$\Rightarrow a = b$$

ϕ is a homomorphism

$$\phi(a+b) = [(a+b)x, x]$$

$$= [ax+bx, x]$$

$$\Rightarrow \phi(a)+\phi(b) = [ax, x] + [bx, x]$$

$$= [axx+xbx, x^2]$$

$$= [ax^2+bx^2, x^2]$$

$$= [ax+bx, x]$$

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

Also $\phi(ab) = [abx, x]$

$$\phi(a)\phi(b) = [ax, x][bx, x]$$

$$= [abx^2, x^2]$$

$$= [abx, x]$$

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

Hence ϕ is 1-1 homomorphism and is the required imbedding mapping.

This proves the thm.

Remark :

The above field F is called the field of quotients or the quotient field of D . The reader is, however, cautioned not to confuse it with R/I .

We also sometimes use the notation a/b to denote $[a, b]$. The logic behind this notation is clear if we consider imbedding of Z into Q .

In fact, at times this notation looks more natural and convenient.

For instance,

$$[a, b] + [c, d] = [ad+bc, bd]$$

$$\text{would read as } a/b + c/d = (ad+bc)/(bd)$$

$$\text{or } [a, b] = [c, d] \text{ would mean } a/b = c/d$$

(or)

$$ad = bc$$

We say that any integral domain D can be enlarged to a field F .

So that each element of F can be expressed as a quotient of two elements of D .

Lemma :

Prove that if k is any field which contains D then k contains a subfield isomorphic to F , where F is the field of quotients of the integral domain D . (In this sense F is the smallest field containing D)

Proof :

Define a map $\varphi : F \rightarrow k$ s.t.

$$\varphi([a,b]) = ab^{-1}$$

Since $a, b \in D \subseteq K, b \neq 0$,

$\therefore b^{-1}$ exists in k .

φ is well-defined, 1-1 map as

$$[a_1, b_1] = [a_2, b_2]$$

$$\Leftrightarrow (a_1, b_1) \sim (a_2, b_2)$$

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

$$\Leftrightarrow \varphi([a_1, b_1]) = \varphi([a_2, b_2])$$

Again

$$\varphi([a_1, b_1] + [a_2, b_2]) = \varphi([a_1 b_2 + b_1 a_2, b_1 b_2])$$

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

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

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

$$= \varphi([a_1, b_1]) + \varphi([a_2, b_2])$$

And

$$\varphi([a_1, b_1][a_2, b_2]) = \varphi([a_1 a_2, b_1 b_2])$$

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

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

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

$$= \varphi([a_1, b_1])\varphi([a_2, b_2])$$

∴ ϕ is a homomorphism

Thus F will be isomorphic to $\phi(F)$ which will be a subfield of k .

Thus quotient field is the smallest field containing D .

Problem :

If D_1 and D_2 be two isomorphic integral domains then show that their respective fields of quotients F_1 and F_2 are also isomorphic.

Solution :

Let $f: D_1 \rightarrow D_2$ be the given isomorphism. The fields of quotients F_1 & F_2 are given by

$$F_1 = \{[a,b]/a,b \in D_1, b \neq 0\}$$

$$F_2 = \{[x,y]/x,y \in D_2, y \neq 0\}$$

Define a map $\phi: F_1 \rightarrow F_2$ s.t.

$$\phi([a,b]) = [f(a), f(b)]$$

$$[a,b] \in F_1 \Rightarrow a,b \in D, b \neq 0$$

$$\Rightarrow f(a), f(b) \in D_2, \text{ and } f(b) \neq 0$$

$$\Rightarrow [f(a), f(b)] \in F_2.$$

ϕ is then well defined and one-one.

$$\phi([a,b]) = \phi([a^1, b^1])$$

$$\Leftrightarrow [f(a), f(b)] = [f(a^1), f(b^1)]$$

$$\Leftrightarrow (f(a), f(b)) \sim (f(a^1), f(b^1))$$

$$\Leftrightarrow f(a) f(b^1) \sim f(b) f(a^1)$$

$$\Leftrightarrow f(ab^1) = f(ba^1)$$

$$\Leftrightarrow ab^1 = ba^1$$

$$\Leftrightarrow (a,b) \sim (a^1, b^1) \Leftrightarrow [a,b] = [a^1, b^1]$$

ϕ is onto, so for any $[x,y] \in F_2$

$$x,y \in D_2 \Rightarrow \exists a,b \in D, \text{ s.t.}$$

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

Also

then $\varphi([a,b]) = [f(a), f(b)] = [x,y]$

φ is a homomorphism

$$\varphi([a,b] + [a^1,b^1]) = \varphi([ab^1+ba^1, bb^1])$$

$$= [f(ab^1+ba^1), f(bb^1)]$$

$$\varphi([a,b]) + \varphi([a^1,b^1]) = [f(a), f(b)] + [f(a^1), f(b^1)]$$

$$= [f(a)f(b^1) + f(b)f(a^1), f(b)f(b^1)]$$

$$= [f(ab^1+ba^1), f(bb^1)]$$

Again,

$$\varphi([a,b][a^1b^1]) = \varphi([aa^1, bb^1])$$

$$= [f(aa^1), f(bb^1)]$$

$$= [f(a)f(a^1), f(b)f(b^1)]$$

$$= [f(a), f(b)][f(a^1), f(b^1)]$$

$$= \varphi([a,b]) \varphi([a^1,b^1])$$

Hence φ is an isomorphism.

Ideals

Definition :

Let R be a ring and $I \subset R$. Then I is called an ideal if :

- (i) I is an additive subgroup of R .
- (ie) $a-b \in I$ whenever $a \in I$ and $b \in I$
- (ii) For any $a \in I, x \in R$ we have both $xa \in I$ and $ax \in I$

It is clear from the definition that every ideal is a subring, but a subring may not always be an ideal. For instance $\mathbb{Z} \subset \mathbb{Q}$ is a subring which is not an ideal.

The following are some examples of ideals.

Example :

- 1) For any ring, $\{0\}$ and R are ideals in R . These are called improper ideals and any other ideal is called a proper ideal.
- 2) If $R = \mathbb{Z}$, then $I = m\mathbb{Z}, m \geq 0$ is an ideal in R .

Lemma :

Let $f: R \rightarrow R^1$ be a homomorphism of R in R^1 . Then $k = \ker f$ is an ideal in R .

Solution :

Let $a \in k$ and $b \in k$

Then $f(a) = 0$ and $f(b) = 0$

Now

$$\begin{aligned} f(a-b) &= f(a) - f(b) \\ &= 0 - 0 = 0 \end{aligned}$$

$\Rightarrow a-b \in k$

Also for any $x \in R$

$$f(xa) = f(x) \cdot f(a)$$

$$\Rightarrow f(xa) = f(x) \cdot 0 = 0$$

Similarly

$$f(ax) = f(a) \cdot f(x)$$

$$\Rightarrow f(ax) = 0 \cdot f(x)$$

$$\Rightarrow f(ax) = 0.$$

Then $xa \in k$ and $ax \in k$

Hence k is an ideal.

Definition :

A ring R with nontrivial multiplication is called a simple ring if it has no proper ideals.

Lemma :

Any field is a simple ring

Proof :

Let R be a field.

we have to show that the only ideals of R are 0 and R .

Let I be a non-zero ideal of R .

Choose $a \in I$, $a \neq 0$

Since R is a field.

Then $\exists a^1 \in R$ s.t. $aa^1 = a^1a = 1$

Since I is an ideal and $a \in I$

we have $1 = a^1a \in I$

now for any $x \in R$

$x = x \cdot 1 \in I$

Hence $I = R$.

Lemma :

Let R be a commutative ring with 1 which is a simple ring. Then R is a field.

Proof :

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

consider $I = Ra = \{xa/x \in R\}$

we shall show that I is an ideal in R .

If $xa \in I$ and $ya \in I$

then $xa - ya = (x - y)a \in I$.

Also for any $z \in R$,

$$(xa)z = z(xa) = (zx)a \in I$$

Since $a = 1.a \in I$ we have $I \neq 0$.

The only ideals of R are 0 and R

We must have $I = R$

In particular $1 \in I$

$\therefore 1 = a^1a = aa^1$ for some $a^1 \in R$

Thus every non-zero element of R has an inverse showing that R is a field.

Definition :

Let A and B be two ideals of a ring R . We define $A+B$ to be the set $\{a+b/a \in A, b \in B\}$ called sum of the ideals A and B .

Let A, B be two ideals of a ring R . We define the product AB of A & B by

$AB = \{\sum a_i b_i / a_i \in A, b_i \in B\}$ where the summation is finite.

Theorem :

If A and B are two ideals of R, then $A+B$ is an ideal of R, containing both A and B.

Proof :

$$A+B \neq \emptyset \text{ as } 0 = 0+0 \in A+B$$

Again, $x, y \in A+B$

$$\Rightarrow x = a_1 + b_1$$

$$y = a_2 + b_2 \text{ for some } a_1, a_2 \in A, b_1, b_2 \in B.$$

since $x-y = (a_1+b_1) - (a_2+b_2)$

$$= (a_1-a_2) + (b_1-b_2)$$

$$x-y \in A+B.$$

Let $x = a+b \in A+B, r \in R$ be any elements then

$$xr = (a+b)r = ar+br \in A+B$$

As A, B are ideals.

$$rs = r(a+b) = ra+rb \in A+B$$

Thus $A+B$ is an ideal of R.

Again for any $a \in A$

Since $a = a+0 \in A+B$ and for any $b \in B$ Since $b = 0+b \in A+B$

$$\therefore A \subseteq A+B$$

$$B \subseteq A+B$$

Theorem :

The product AB of any two ideals A and B of a ring R is an ideal of R.

Proof :

$$AB \neq \emptyset \text{ as } 0 = 0.0 \in AB$$

Let $x, y \in AB$ be any two members.

Then $x = a_1 b_1 + a_2 b_2 + \dots + a_n b_n$

$$y = a_1' b_1' + \dots + a_m' b_m'$$

for some $a_i, a_j' \in A, b_i, b_j' \in B.$

$$x-y = (a_1b_1 + \dots + a_nb_n) - (a_1^1b_1^1 + \dots + a_m^1b_m^1)$$

which clearly belongs to AB.

The R.H.S can be written as

$$x_1y_1 + x_2y_2 + \dots + x_ky_k \quad [k=n+m]$$

where $x_i \in A, y_i \in B$.

Again,

$$x = a_1b_1 + \dots + a_nb_n \in AB \text{ and } r \in R.$$

$$rx = r(a_1b_1 + \dots + a_nb_n)$$

$$= (ra_1)b_1 + (ra_2)b_2 + \dots + (ra_n)b_n \in AB$$

because $ra_i \in A$ as $a_i \in A, r \in R$ and

A is an ideal.

$$\text{III}^{\text{ly}} \quad xr \in AB.$$

$\therefore AB$ is an ideal of R .

Quotient rings :

Definition :

Let R be a ring and I an ideal in R . The ring R/I with addition and multiplication defined as $(a+I) + (b+I) = (a+b) + I$

$(a+I)(b+I) = ab+I$ is called the quotient ring of R by the ideal I .

Example :

1) If $R = \mathbb{Z}$ and $I = n\mathbb{Z}, n > 0$ then the quotient ring R/I is the ring $\mathbb{Z}_n$ of residue classes modulo n .

2) For any ring $R, R/I = R$ when $I = 0$.

III^{ly} R/R is the zero ring.

Theorem : (First isomorphism thm)

Let $f: R \rightarrow R^1$ be a homomorphism of R onto R^1 and let $I = \ker f$. Then I is an ideal in R , and $R/I \approx R^1$

Proof :

We have that I is an ideal in R .

Defin $\phi: R/I \rightarrow R^1$ s.t. $\phi(I+r) = (r)$

Claim (i) :

ϕ is well defined

ie) To prove, If $r_1 = I + r_2$.

Then $\phi(I+r_1) = \phi(I+r_2)$

Then to prove $f(r_1) = f(r_2)$

$$I + r_1 = I + r_2$$

$$\Rightarrow r_1 \in (I+r_2)$$

$$\Rightarrow r_1 = i+r_2 \text{ where } i \in I.$$

$$\Rightarrow r_1 - r_2 = i$$

$$\Rightarrow r_1 - r_2 \in I \in \text{Kernal}$$

$$\Rightarrow f(r_1 - r_2) = 0$$

$$\Rightarrow f(r_1) - f(r_2) = 0$$

$$\Rightarrow f(r_1) = f(r_2)$$

$$\Rightarrow \phi(I+r_1) = \phi(I+r_2)$$

$\therefore \phi$ is well defined.

Claim 2 :

ϕ is homomorphism

Let $I + r_1, I + r_2 \in R/I$.

Then

$$\phi[(I+r_1)+(I+r_2)] = \phi[I+r_1+r_2] \text{ [by defn]}$$

$$= f(r_1+r_2)$$

$$= f(r_1)+f(r_2)$$

$$= \phi(I+r_1) + \phi(I+r_2)$$

$$\Rightarrow \phi[(I+r_1)+(I+r_2)] = \phi[I+r_1+r_2]$$

$$= f(r_1 r_2)$$

$$= f(r_1) \cdot f(r_2)$$

$$= \phi(I+r_1) \cdot \phi(I+r_2)$$

$\therefore \phi$ is a homomorphism

Calim (iii) :

ϕ is 1-1

$$\phi(I+r_1) = \phi(I+r_2)$$

$$\Rightarrow f(r_1) = f(r_2)$$

$$\Rightarrow f(r_1) - f(r_2) = 0$$

$$\Rightarrow f(r_1 - r_2) = 0 \text{ [}\because f \text{ is homo]}$$

$$\Rightarrow r_1 - r_2 \in \ker f = I$$

$$\Rightarrow r_1 = I + r_2$$

$$\Rightarrow r_1 \in I + r_2$$

$$\Rightarrow I + r_1 = I + r_2$$

$\therefore \phi$ is 1-1

Claim (iv) :

ϕ is on to

Let $r^1 \in R^1$. Then $\exists r \in R$ s.t $f(r) = r^1$.

(ie) $r^1 \in R^1$ and $I+r \in R/I$

$$\therefore \phi(I+r) = r^1$$

$\therefore \phi$ is onto

From (i) (ii) (iii) (iv)

$\therefore \phi$ is an isomorphism.

$$\therefore R/I \cong R^1.$$

Lemma :

Let I be an ideal in a ring R , and $P: R \rightarrow R/I$ the projection mapping. Then any $J \subset I$ is an ideal in R if and only if $P(J) = J/I$ is an ideal in R/I .

Proof :

Let $J \subset I$ be an ideal in R .

$$\therefore J^1 = P(J)$$

Then J^1 is clearly a subgroup of $R^1 = R/I$

now, Let $a+I \in J^1$ with $a \in J$ and $x+I \in R^1$.

$$\text{Then } (x+I)(a+I) = xa + I \in J^1$$

Hence $xa \in J$.

$$\text{III}^{\text{ly}} (a+I)(x+I) = ax + I \in J^1$$

Hence $ax \in J$.

Thus J' is an ideal in R^1 .

Conversely,

Assume that $J' = \{a+I/a \in J\}$ is an ideal in R' .

Then $J = P^{-1}(J')$ is an abelian subgroup of R .

Also, for any $x \in R$, $a \in J$.

$$(x+I)(a+I) = xa + I \in J^1$$

So that $xa \in J$.

$$\text{III}^{\text{ly}} ax \in J.$$

Showing that J is an ideal in R .

Prime and maximal ideals

Definition :

An ideal P in a ring R is said to be a prime ideal if whenever $ab \in P$, then either $a \in P$ or $b \in P$, $P \neq R$.

Example :

1) Let $R = \mathbb{Z}$ and $P = p\mathbb{Z}$ where p is a prime. Then p is a prime ideal because if $ab \in p\mathbb{Z}$, then $ab = pk$ for $k \in \mathbb{Z}$, ie) p divides ab .

Since p is a prime, we have $p|a$ or $p|b$.

$$\therefore a \in p\mathbb{Z} \text{ or } b \in p\mathbb{Z}$$

Hence p is a prime ideal.

2) If R is an integral domain, $p = \{0\}$ is a prime ideal in R for if $ab \in p = \{0\}$

$$\text{then } ab = 0$$

$$a = 0 \text{ or } b = 0$$

ie) $a \in p$ or $b \in p$

Hence p is a prime ideal.

Theorem :

Let R be a commutative ring. An ideal p of R is prime iff R/p is an integral domain

Proof :

Let P be prime ideal of R .

$$\text{Let } (a+P)(b+P) = 0+P$$

$$\text{Then } ab+P = P$$

$$\Rightarrow ab \in P$$

$$\Rightarrow ab \in P \text{ or } b \in P$$

$$\Rightarrow a+P = P \text{ or } b+P = P$$

Thus R/P is an integral domain.

Conversely,

Let R/P be an integral domain

$$\text{Let } ab \in p \text{ then } ab+P = P$$

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

$$\Rightarrow a+P = P \text{ or } b+P = P$$

(R/p is an integral domain)

$$\Rightarrow a \in p \text{ (or) } b \in p$$

Hence p is a prime ideal.

Hence the result.

Definition :

An ideal M in a ring is called a maximal ideal. If $M \neq R$, and if for any ideal I of R such that $M \subset I \subset R$, we have $I = M$ or $I = R$.

Examples :

- 1) Let $R = \mathbb{Z}$ and $M = p\mathbb{Z}$ where p is a prime. Then M is a maximal ideal of R . Let I be any ideal containing M .

Then $I = mZ$ and since $I \subset M$, $P \in I$

$\therefore P = mK$ for some K .

$\Rightarrow m/p$ since p is a prime $m = 1$ or $m = p$

$\therefore I = R$ or $I = M$

Thus M is a maximal of R .

Lemma :

An ideal M in Z is a maximal ideal iff $M = pz$ where p is a prime.

Proof :

We have seen that $M = pz$ where p is a prime is a maximal ideal of z . Let I be any maximal ideal of z .

where $I = mz$

suppose m is not prime

It has a proper divisor K .

ie) $m = kl$, $1 < K < M$, $1 < l < m$

consider the ideal $J = kz$.

Since k/m we have $m \in J$

Hence $I \subset J$.

This inclusion is proper, because $k \in J$ and $k \notin I$ as k is a proper divisor of m . Moreover $J \neq R$. because $k > 1$.

Thus there is a proper ideal J containing I properly contradicting the maximality of I .

Hence m is a prime.

$\therefore I$ is of the form pz where P is a prime.

Hence the lemma.

Theorem :

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

Proof :

Let M be maximal ideal of R . Since R is commutative ring with unity. R/M is also a commutative ring with unity.

Thus all that we need prove is that non-zero elements of R/M have multiplication inverse.

Let $x+M \in R/M$ be any non-zero element.

Then $x+M \neq M \Rightarrow x \notin M$.

Let $xR = \{xr/r \in R\}$

It is easy to verify that xR is an ideal of R .

Since sum of two ideals is an ideal, $M+xR$ will be an ideal of R .

Again, $x = 0+x, 1 \in M+xR$ and $x \notin M$

we find

$$M \subset M+xR \subseteq R$$

$$M, \text{ maximal} \Rightarrow M+xR = R$$

$$\text{Thus } 1 \in R \Rightarrow 1 \in M+xR$$

$$\Rightarrow 1 = m+xr \text{ for some } m \in M, r \in R.$$

$$\begin{aligned} \Rightarrow 1+M &= (m+xr)+M \\ &= (m+M) + (xr+M) = xr+M \\ &= (x+M)(r+M) \end{aligned}$$

$$\Rightarrow (r+M) \text{ is multiplicative inverse of } x+M.$$

Hence R/M is a field.

Conversely,

Let R/M be a field.

Let I be any ideal of R s.t

$$M \subset I \subseteq R.$$

Then some $a \in I$, s.t. $a \notin M$.

Now

$a \notin M \Rightarrow a+M \neq M \Rightarrow a+M$ is a non-zero element of R/M .

which being a field, means $a + M$ has multiplicative inverse.

Let $b + M$ be its inverse.

Then

$$\begin{aligned}(a + M)(b + M) &= 1 + M \\ \Rightarrow ab + M &= 1 + M \\ \Rightarrow ab - 1 &\in M \\ \Rightarrow ab - 1 &\in M \\ \Rightarrow ab - 1 &= m \text{ for some } m \in M. \\ \Rightarrow 1 &= ab - m \in I \text{ (by defn. of ideal)} \\ \Rightarrow I &= R \text{ (ideal containing unity, equals the ring)}\end{aligned}$$

Hence M is maximal ideal of R .

Problem :

1) Let R be a commutative ring with unity, if every ideal of R is prime show R is a field.

Solution :

To show that R is a field, we need show that every non-zero element of R has multiplicative inverse.

We first show that R is an integral domain.

$$\begin{aligned}\Rightarrow a \in \{0\} \text{ or } b \in \{0\} \\ \therefore a = 0 \text{ or } b = 0\end{aligned}$$

this R is an integral domain.

Let now $a \in R$ be any non-zero element.

$$\text{Let } a^2R = \{a^2r/r \in R\}$$

then a^2R is an ideal of R .

$$\text{now } a.a = a^2 = a^2.1 \in a^2R$$

$$\Rightarrow a \in a^2R$$

$$\Rightarrow a = a^2b \text{ for some } b \in R$$

$$\Rightarrow a(1-ab) = 0$$

$$\Rightarrow 1-ab = 0 \text{ as } a \neq 0$$

$\Rightarrow b$ is multiplicative of a

Hence R is a field.

Problem 2 :

Let R be a commutative ring with unity. Show that every maximal ideal of R is prime.

Solution :

We know that an ideal M of R is maximal iff R/M is field.

This if M is maximal then R/M is a field and hence an integral domain.

$\Rightarrow M$ is a prime ideal (by problem 1)

Factorisation

Definition :

Let $a \in R$ and $b \in R$, $a \neq 0$, a is said to divide b if there exist $C \in R$ such that $b = ac$.

Lemma :

Let a and b be non-zero elements of R . If a/b and b/a then $b = au$ for some unit u (regular element) in R and conversely.

Proof :

Since a/b , we have $b = ac$, $c \in R$,

and since b/a , we have $b = ad$, $d \in R$

$$\% \quad a = bd = acd$$

$$\Rightarrow a - acd = 0$$

$$\Rightarrow a(1-cd) = 0$$

$$\text{Since } a \neq 0.$$

$\% R$ is an integral domain

$$\% \quad 1-cd = 0.$$

$\% c$ and d are units.

Then $b = ac$ where c is a unit.

Conversely,

If $b = au$ where u is a unit

then clearly a/b .

Also if $uv = 1 \forall v \in R$.

then $a = auv = bv$

ie) b/a .

Hence the proof.

Definition:

Two non-zero elements a and b are said to be associates of each other if a/b and b/a .

Example :

1) In $R = \mathbb{Z}$, $a = 5$ and $b = -5$ are

associates $-5 = (-1).5$

Definition :

If $a \in R$ is called an irreducible element if (i) a is not a unit & (ii) the only divisors of a are units and associates of a .

Example :

i) Let $R = \mathbb{Z}$ and $n \in \mathbb{Z}_n > 1$. Then n is irreducible iff if the only divisors of n are ± 1 (units) and $\pm n$ (associates of n) thus n is a prime integer.

Definition :

Let $P \in R$ which is not a unit. p is called a prime element if it has the property that whenever p/ab we have that p/a or p/b .

Lemma :

Every prime element is irreducible.

Proof :

Suppose P is prime. Let a be any divisor of p .

$$\because p = ab$$

$$\text{now } p/p = ab.$$

$\because p$ is a prime p/a or p/b .

If p/a

Since a/p we have that a is an associated of p and b is a unit.

III^{ly}

If p/b

then b is an associate of p and a is a unit.

Thus the only divisors of p are units and associates of p .

Hence p is irreducible.

Definition :

Let $a \in R$ and $b \in R$. An element $d \in R$ is called a greatest common divisor (gcd) of a and b if

(i) d/a and d/b .

(ii) whenever d_1/a and d_1/b then d_1/d .

Lemma :

An element $P \in R$ is prime iff the ideal $P = RP = \{xp/x \in R\}$ is a prime ideal.

Proof :

Suppose P is a prime element.

Let $ab \in p$.

Then $ab = cp$ for some $c \in R$.

$\because p/ab$

$\because p$ is a prime, p/a or p/b

$\because a \in p$ or $b \in p$.

Hence P is a prime ideal.

Coversely,

Let P be a prime ideal and let p/ab .

Then $ab = cp \in p$

$\therefore p$ is a prime ideal, $a \in p$ or $b \in p$

$\therefore p/a$ or p/b . Hence p is a prime element.

Definition :

If $a, b \in R$, then a and b are said to be relatively prime if their gcd is a unit.

Theorem :

Let R be an integral domain with unity. If $d_1 = \text{g.c.d.}(a, b)$ in R then $d_2 = \text{g.c.d.}(a, b)$ iff d_1 and d_2 are associates.

Proof :

Let d_1 and d_2 be both g.c.d (a, b)

Then $d_1/a, d_1/b$ &

$d_1/a, d_2/b$.

By definition we get d_1/d_2 and d_2/d_1

$\Rightarrow d_1$ and d_2 are associates.

Conversely,

Let $d_1 = \text{g.c.d.}(a, b)$ and

d_2 be an associates of d_1

Then $ud_2 = d_1$ for some unit u .

$\Rightarrow d_2/d_1$ and $d_1/a, d_1/b$

$\Rightarrow d_2/a$ & d_2/b .

Let $x/a, x/b$ this x/d_1

As d_1 is g.c.d (a, b)

Also $d_2 = d_1 u^{-1}$
 d_1/d_2

Thus x/d_2

$\Rightarrow d_2 = \text{g.c.d.}(a, b)$

Lemma :

Let R be an integral domain with unity. If $\text{g.c.d}(a, b) = d$ for $a, b \in R$ then cd and $\text{g.c.d}(ca, cb)$ are associates.

Solution :

$$\text{Let } \text{g.c.d}(ca, cb) = d^1$$

$$d/a, a = dk$$

$$\Rightarrow ac = dkc = cdk$$

$$\Rightarrow cd / ca$$

$$\text{III}^{\text{ly}} \quad cd / cb \Rightarrow cd / d^1 \Rightarrow d^1 = cdt$$

$$\text{Again } d^1/ca \Rightarrow ca = d^1s$$

$$\Rightarrow ca = d^1s = cdt$$

$$\Rightarrow a = (dt)s \Rightarrow dt/a$$

$$\text{III}^{\text{ly}} \quad dt / b \Rightarrow dt / d \Rightarrow d = dtp \Rightarrow d(1-tp) = 0$$

$$\Rightarrow 1 = tp \Rightarrow t \text{ is a unit}$$

$$\Rightarrow \text{g.c.d}(ca, cb) = d^1 = cdt$$

$\therefore cd$ and d^1 are associates.

EUCLIDEAN RINGS

Definition :

An integral domain R is said to be a 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 $t, r \in R$ such that $a = tb + r$ where either $r = 0$ (or) $d(r) < d(b)$.

Theorem (1) :

Let R be a Euclidean ring and let A be an ideal of R . Then there exists an element $a_0 \in A$ s.t $A = \{a_0 x / x \in R\}$.

Proof :

Case (i) :

Let A consists of the element 0. If we put $a_0 = 0$. The theorem is trivially true.

Case (ii) :

Let $A \neq \{0\}$

Then $\exists$ an $a \in A$, $a \neq 0$

choose an element $a_0 \in A$ s.t. $d(a_0)$ is minimum.

[since the d value is a non-negative integer such a choice of a_0 is possible]

suppose $a \in A$

By the properties of the Euclidean ring. There exists $t, r \in R$ s.t. $a = ta_0 + r$

where either $r = 0$ (or) $d(r) < d(a_0)$

$$\Rightarrow r = a - ta_0$$

now,

$$a_0 \in A, t \in R \Rightarrow ta_0 \in A$$

[A is an ideal of R]

$$a \in A, ta_0 \in A \Rightarrow a - ta_0 \in A$$

(ie) $r \in A$

If $d(r) < d(a_0)$

which is $\Rightarrow \Leftarrow$

The choice of a_0 whose d value is minimum.

Hence $r = 0$

(ie) $a = ta_0$

(ie) $A = \{a_0x/x \in R\}$

Every ideal of a Euclidean ring is a principal ideal.

Hence the theorem.

Definition :

An integral domain R with unit element is a principal ideal ring if every ideal A is of the form $A=(a)$ for some $a \in R$.

Theorem (2) :

Every Euclidean ring possesses a unit element.

Proof :

Let R be an Euclidean ring. Then R be an ideal of R .

By the previous theorem.

$R=(u_0)$ (for some $u_0 \in R$)

Every element of R is a multiple of u_0 .

Hence in particular,

$u_0 = u_0c$ (for some $c \in R$)

consider an arbitrary element $a \in R$.

then

$$a = xu_0 \text{ (for some } x \in R)$$

$$\circ \quad ac = (xu_0)c$$

$$\Rightarrow \quad ac = x(u_0c)$$

$$\Rightarrow \quad ac = xu_0$$

$$\Rightarrow \quad ac = a$$

$$\Rightarrow \quad ac = a \Rightarrow c \text{ is a required unit element.}$$

Theorem (1) & (2) we conclude that Every Euclidean ring is a principal ideal ring.

Definition :

If $a \neq 0$ and b are in a commutative ring R then a is said to divide b if there exists $ac \in R$ such that $b=ac$. We shall use the symbol a/b to represent the fact that a divides b and $a \times b$ to mean that a does not divide b .

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 (g.c.d) :

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

- 1) d/a and d/b .
- 2) whenever c/a and c/b then c/d .

We shall use the notation $d = (a, b)$ to denote that d is a greatest common divisor of a and b .

Lemma (1) :

Let R be a Euclidean ring. Then any two elements a and b in R have a greatest common divisor R . Moreover $d = \lambda a + \mu b$ for some $\lambda, \mu \in R$

Proof :

$$\text{Let } A = \{sa + tb, s, t \in R\}$$

Claim :

A is an ideal of R .

$$\text{Let } x, y \in A$$

$$\text{Then } x = s_1 a + t_1 b, \quad s_1, t_1 \in R$$

$$y = s_2 a + t_2 b, \quad s_2, t_2 \in R$$

$$x-y = (s_1-s_2)a + (t_1-t_2)b$$

$$s_1, s_2 \in R \Rightarrow (s_1-s_2) \in R$$

$$t_1, t_2 \in R \Rightarrow (t_1-t_2) \in R$$

$$x-y \in A$$

$$\text{Let } r \in R \text{ \& } x \in A$$

$$rx = r(s_1a + t_1b)$$

$$rx = r(s_1a) + r(t_1b) \quad s_1 \in R, r \in R$$

$$= (rs_1)a + (rt_1)b \Rightarrow rs_1 \in R$$

$$\in R \quad rt_1 \in R$$

$$\text{ie) } rx, xr \in R$$

% A is an ideal of R.

% R is an Euclidean ring every ideal of R is a principal ideal.

Hence $\exists$ an element $d \in A$ such that every element of A is a multiple of d.

$$d \in A \Rightarrow d = \lambda a + \mu b, \lambda, \mu \in R$$

Claim :

$$d = (a, b)$$

since R is an Euclidean ring

$$1 \in R$$

$$a = 1.a + 0.b$$

$$b = 0.a + 1.b$$

$$\text{ie) } a, b \in A.$$

$$\text{ie) } a \text{ and } b \text{ are multiple of } d.$$

$$\% d/a \text{ and } d/b.$$

Suppose c/a and c/b

$$c/a \Rightarrow c/\lambda a, c/b \Rightarrow c/\mu b$$

$$c/\lambda a, c/\mu b \Rightarrow c/\lambda a + \mu b \Rightarrow c/d$$

$$\% d = (a, b)$$

Hence the proof.

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. A unit in a ring is an element whose inverse is also in the ring.

Lemma (2) :

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

Proof :

Given $a/b \Rightarrow b = ax$ for some $x \in R$.

Give $b/a \Rightarrow a = by$ for some $y \in R$.

$$\circledast \quad a = by$$

$$\Rightarrow a = (ax)y$$

$$\Rightarrow a = a(xy)$$

$$\Rightarrow xy = 1$$

$\Rightarrow x$ is a unit (or) y is a unit.

$$\circledast \quad a = by \Rightarrow y \text{ is a unit}$$

$$\circledast \quad a = ub \text{ where } u \text{ is a unit in } R.$$

Defintion :

Let R be a commutative ring with unit element. Two elements a and b in R are said to be associates if $b = ua$ for some unit $u \in R$.

Lemma (3) :

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

Proof :

Given b is not a unit in R .

To prove that $d(a) < d(ab)$

If possible

$$\text{Let } d(a) = d(ab)$$

$$\text{Let } A = \{ax, x \in R\} = (a)$$

$$\circledast A = (a) \Rightarrow d(a) \text{ is minimum in } A.$$

$$\text{Now } ab \in A$$

If $d(a) = d(ab)$, then d value of ab is minimum.

Hence every element of A can be written as a multiple of ab .

$$\circledast a \in A.$$

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

$$\Rightarrow 1 = bx$$

$$\Rightarrow b \text{ is a unit in } R$$

$$\Rightarrow$$

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

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

If b is not a unit in R .

Lemma (4) :

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 a finite number of prime elements of R .

Proof :

Given R is an Euclidean ring.

Let $a \in R$ be arbitrary.

We prove the theorem by induction on $d(a)$.

$$\text{If } d(a) = d(1)$$

Then a is a unit in R .

We assume the theorem to be true for every element $x \in R$. Then $d(x) < d(a)$.

Let we prove the theorem for $d(a)$.

If a is a prime element, then the result holds.

If a is not a prime element, then $a=bc$ where neither b nor c is a unit. By induction hypothesis,

$$b = \pi_1, \pi_2, \dots, \pi_n.$$

$$c = \pi_1^1, \pi_2^1, \dots, \pi_m^1 \text{ where } \pi_i \text{ \& } \pi_j^1$$

are prime elements of R .

∴

$$a = bc$$

⇒

$$a = (\pi_1, \pi_2, \dots, \pi_n) (\pi_1^1, \pi_2^1, \dots, \pi_m^1)$$

∴ a can be written as a product of finite number of prime element of R .

Since $a \in R$ is arbitrary, a is a unit in R or a can be written as a product of finite number of prime elements of R .

Definition :

In the Euclidean ring R , and b in R are said to be relatively prime if their greatest common divisor is a unit of R .

Since any associate of a greatest common divisor is a greatest common divisor and since 1 is an associate of any unit, if a and b are relatively prime we may assume that $(a,b) = 1$.

Lemma (5) :

Let R be a Euclidean ring. Suppose that for $a, b, c \in R$, a/bc but $(a, b)=1$, then a/c .

Proof :

$$\text{Given } (a, b) = 1$$

By Lemma (1),

$$1 = \lambda a + \mu b.$$

Multiplying throughout by c ,

$$\therefore c = \lambda ac + \mu bc$$

$$a/c \Rightarrow a/\lambda ac$$

$$a/bc \Rightarrow a/\mu bc$$

$$\therefore a/\lambda ac \text{ \& } a/\mu bc \Rightarrow a/\lambda ac + \mu bc \Rightarrow a/c$$

Hence the lemma.

Lemma (6) :

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

Proof :

Suppose that π/a .

Since π is a prime element $(\pi, a) = 1$

$$\circ \quad \lambda\pi + \mu a = 1$$

Throughout multiply by b .

$$\Rightarrow \quad \lambda\pi b + \mu ab = b.$$

$$\text{Given} \quad \pi/ab \Rightarrow \pi/\mu ab \text{ \& } \pi/\pi b \Rightarrow \pi/\lambda\pi b$$

$$\pi/\lambda\pi b + \mu ab$$

$$\Rightarrow \pi/b$$

$\circ$ If π/a then π/b .

Theorem : (unique factorization theorem)

Let R be an Euclidean ring and $a \neq 0$ a non-unit in R . Suppose that $a = \pi_1 \pi_2 \dots \pi_n = \pi_1^1 \pi_2^1 \dots \pi_m^1$ where the π_i & π_j^1 are prime elements of R . Then $n=m$ and each π_i , $1 \leq i \leq n$ is an associate of some π_j^1 , $1 \leq j \leq m$ and conversely each π_k^1 is an associate of some π_q .

Proof :

Let R be an Euclidean ring.

given $a \neq 0$, a non-unit in R .

$$a = \pi_1 \pi_2 \dots \pi_n = \pi_1^1 \pi_2^1 \dots \pi_m^1$$

where the π_i & π_j^1 are prime elements of R .

To prove $n = m$

$$a = \pi_1 \pi_2 \dots \pi_n = \pi_1^1 \pi_2^1 \dots \pi_m^1 \quad \dots \dots \dots (1)$$

$$\circ \quad \pi_1 / \pi_1 \pi_2 \dots \pi_n = \pi_1 / \pi_1^1 \pi_2^1 \dots \pi_m^1$$

without loss of generality

$$\pi_1 / \pi_1^1 \quad [\circ \pi_1 \text{ \& } \pi_1^1 \text{ are prime elements of } R]$$

Also π_1 / π_1^1 must be associates.

$$\circ \quad \pi_1^{-1} = u_1 \pi_1 \text{ where } u_1 \text{ is a unit in } R.$$

$$\begin{aligned} \pi_1 \pi_2 \dots \pi_n &= u_1 \pi_1 \pi_2^{-1} \dots \pi_m^{-1} \\ \Rightarrow \pi_2 \dots \pi_n &= u_1 \pi_2^{-1} \dots \pi_m^{-1} \end{aligned}$$

Let π_2/π_2^{-1}

$$\Rightarrow \pi_2^{-1} = u_2 \pi_2 \text{ where } u_2 \text{ is a unit in } R.$$

$$\circ \quad \pi_2 \pi_3 \dots \pi_n = u_1 u_2 \pi_2 \pi_3^{-1} \dots \pi_m^{-1}$$

$$\Rightarrow \pi_3 \pi_4 \dots \pi_n = u_1 u_2 \pi_3^{-1} \dots \pi_m^{-1}$$

Proceeding like this, we get

$$\text{L.S.H.} = 1$$

$$\circ \quad n \leq m \dots (2)$$

III^{ly}

$$\pi_1^{-1}/\pi_1^{-1} \pi_2^{-1} \dots \pi_m^{-1}$$

$$\Rightarrow \pi_1^{-1}/\pi_1 \pi_2 \dots \pi_n$$

$$\Rightarrow \pi_1^{-1}/\pi_1$$

$$\Rightarrow \pi_1 = u_1^{-1} \pi_1^{-1}$$

$\circ \quad u_1^{-1}$ is a unit in R .

$$\circ \quad u_1^{-1} \pi_1^{-1} \pi_2 \pi_3 \dots \pi_n = \pi_1^{-1} \pi_2^{-1} \dots \pi_m^{-1}$$

$$\Rightarrow u_1^{-1} \pi_2 \pi_3 \dots \pi_n = \pi_2^{-1} \dots \pi_m^{-1}$$

Proceeding like this we get R.H.S. = 1

$$m < n \dots (3)$$

from (2) & (3)

$$m = n$$

This shows that π_i is an associate of some π_j^{-1} and π_k^{-1} is an associate of some π_q .

Lemma :

Let R be an E.R. Let a and b be two non-zero elements in R . Then

- (i) If b is a unit in R , then $d(a) = d(ab)$
- (ii) If b is not a unit in R , then $d(ab) > d(a)$.

Proof :

Given b is a unit.

To prove that $d(a) = d(ab)$
 we have $d(a) \leq d(ab)$ (1)

To prove that $d(a) \geq d(ab)$

∴ $a = (ab)b^{-1}$ [∵ b is a unit, b^{-1} exists]

∴ $d(a) = d(ab) b^{-1}$
 $\geq d(ab)$

∴ $d(a) \geq d(ab)$ (2)

from (1) & (2)

$$\begin{aligned} d(a) &= d(ab) \\ d(ab) &> d(a) \end{aligned}$$

If b is unit

$$d(ab) = d(a)$$

If b is not an unit

$$d(ab) > d(a)$$

Hence the lemma.

Theorem :

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

Proof :

Necessary Part :

Given A is a maximal ideal of R . To prove that a_0 is prime elements of R . If possible,

Let a_0 be not a prime element of R . Then $a_0 = bc$ where neither b nor c is a unit in R .

Let $B = (b)$

$$a_0 = bc \Rightarrow a_0 \in B$$

∴ $A \subseteq B \subseteq R$

Claim :

$$A \neq B, B \neq R$$

$$B = R \Rightarrow 1 \in B$$

$\Rightarrow 1 = bx$ for some $x \in R$
 $\Rightarrow b$ is a unit in R .
 $\Rightarrow \Leftarrow$
 $\% B \neq R$
 $B = A \Rightarrow b \in A$
 $\Rightarrow b = a_0 y$ for some $y \in R$
 $\Rightarrow b = bcy$
 $\Rightarrow 1 = cy$
 $\Rightarrow c$ is a unit in R .
 $\Rightarrow \Leftarrow$
 $\% B \neq A$
 $\% A \subseteq B \subseteq R \Rightarrow B \neq R \text{ \& } A \neq B$.
 $\% A$ is not a maximal ideal of R .
 $\Rightarrow \Leftarrow$
 $\% a_0$ is a prime element of R .

Sufficient Part :

Given a_0 is a prime element of R .

To P.T

$$A = (a_0) \text{ is maximal}$$

Let U be an ideal of R s.t. $A \subseteq U \subseteq R$

then $U = (u_0)$ for some $u_0 \in R$

$$A \subseteq U \Rightarrow a_0 \in U$$

$$\Rightarrow a_0 = u_0 \text{ for some } x \in R$$

since a_0 is a prime element.

either x is a unit or u_0 is a unit.

If u_0 is a unit, u_0^{-1} exist.

$$\% u_0 u_0^{-1} \in U$$

$$\Rightarrow 1 \in U$$

$$\Rightarrow U = R$$

If x is a unit, x^{-1} exist.

$$\begin{aligned} \circ \quad x^{-1} a_0 &= x^{-1} x a_0 \\ &= u_0 \end{aligned}$$

$$\circ \quad u_0 = x^{-1} a_0$$

$$\Rightarrow u_0 \in A$$

$$\Rightarrow U \subseteq A$$

Already we have $A \subseteq U$

$$\circ \quad A = U$$

$$\text{ie) } A \subseteq U \subseteq R \Rightarrow \text{either } U = A \text{ or } R = U$$

$\circ$ A is maximal

Hence the them.

Principal ideal Domain :

Definition :

An integral domain R with unity is called a principal ideal domain. (PID) if every ideal of R is a principal ideal.

Lemma :

Show that in a PID every non-zero prime ideal is maximal.

Proof :

Let $P = (p)$, $p \neq 0$ be a non-zero prime ideal in a PID R .

Suppose $P \subseteq Q = (q) \subseteq R$

then $p \in P \subseteq Q = (q)$

$$\Rightarrow p = qr$$

$$\Rightarrow qr \in p$$

$$\Rightarrow q \in p \text{ or } r \in p$$

$$\text{If } q \in p$$

then all multiples of q

$$p \Rightarrow Q \subseteq P$$

thus $Q = p$.

If $r \in p$ then $r = pt \Rightarrow r = qrt$

$$\Rightarrow r(1-qt) = 0$$

$$\Rightarrow 1 = qt \quad (r \neq 0)$$

But $q \in Q, t \in R \Rightarrow qt \in Q$

$$\Rightarrow 1 \in Q \Rightarrow Q = R$$

note $r = 0$ would mean $p = q \cdot 0 \Rightarrow p = 0 \Rightarrow p = (0)$.

Problem :

Show that $z[i] = \{a+ib/a, b \in z\}$, the ring of Gaussian integers is a Euclidam domain.

Solution :

We know that $z[i]$ is an integral domain.

For any $0 \neq x \in z[i]$,

where $x = a+ib$

define $d(x) = d(a+ib) = a^2 + b^2$

Then $x \neq 0$, either $a \neq 0$ or $b \neq 0$

Thus $d(a+ib) = a^2 + b^2 > 0$

Let $x, y \in z[i]$, s.t $x \neq 0, y \neq 0$ and

Let $x = a+ib, y = c+id$

$$\begin{aligned} \text{then } d(xy) &= d((a+ib)(c+id)) \\ &= d((ac-bd) + i(ad+bc)) \\ &= (ac-bd)^2 + (ad+bc)^2 \\ &= (a^2+b^2)(c^2+d^2) \\ &= d(x)d(y) \end{aligned}$$

since $y \neq 0, d(y) \geq 1$ [$y \neq 0$ means c or d is non-zero]

Thus $d(xy) \geq d(x)$

we now prove the last condition in the definition of a Euclidean domain.

Let $x, y \in z[i]$ be two members.

where x is an ordinary (+ve) integer

$n(x=n+io)$ and $y = a+ib$

By Euclid's division algorithm,

$$a = un + r_1 \quad 0 \leq r_1 < n$$

$$b = vn + r_2 \quad 0 \leq r_2 < n$$

now either $r_1 \leq n/2$ or $r_1 > n/2$.

If $r_1 > n/2$ then $-r_1 < -n/2$.

$$\Rightarrow n - r_1 < n - n/2 = n/2$$

$$\begin{aligned} \text{Thus } a &= un + r_1 = un + n - n + r_1 \\ &= n(u+1) - (n - r_1) \\ &= nq + k_1 \text{ where } k_1 = -(n - r_1) \end{aligned}$$

$$|k_1| = n - r_1 < n/2.$$

Thus whether $r_1 \leq n/2$ or $n/2 < r_1$.

we can express

$$a = nq + k_1 \text{ where } |k_1| \leq n/2.$$

$$\text{III}^{\text{ly}} \quad b = nq + k_2 \text{ where } |k_2| \leq n/2.$$

$$\text{ie) } a+ib = n(q+iq^1) + (k_1+ik_2)$$

$$\text{(or) } y = tn + r \quad [r = q+iq^1, r = k_1+ik_2]$$

$$\text{where either } r = 0 \text{ (} k_1 \text{ \& } k_2 \text{ could be zero)}$$

$$\begin{aligned} \text{(or) } d(r) &= d(k_1+ik_2) \\ &= k_1^2 + k_2^2 \leq n^2/4 + n^2/4 < n^2 = d(n) \end{aligned}$$

Thus, under this particular case.

The result is proved.

Lemma :

Let p be a prime integer and suppose that for some integer c relatively prime to p we can find integers x and y such that $x^2 + y^2 = cp$. Then p can be written as the sum of squares of two integers that is, there exist integers a and b such that $p = a^2 + b^2$.

Proof :

P is not a prime element of $J[i]$ suppose P is a prime element of $J[i]$

Then p/cp

$$\Rightarrow p/x^2+y^2$$

$$\Rightarrow p/(x+iy)(x-iy)$$

$$\Rightarrow P/(x+iy) \text{ or } P/x-iy$$

(or)

If $p/x+iy$

$$x+iy = p(u+iv)$$

$$x-iy = p(u-iv)$$

$$\Rightarrow x^2+y^2 = p^2(u^2+v^2)$$

$$\Rightarrow p^2/x^2+y^2 = p^2/(u^2+v^2)$$

$$\Rightarrow p^2/cp \Rightarrow p/c$$

which is $a \Rightarrow \Leftarrow$

P is a prime to C .

Hence P is not a prime element in $J[i]$.

Let

$$P = (a+ib)(g+id) \text{ where } a+ib \text{ is a unit nor } g+id \text{ is a unit.}$$

$$a^2+b^2 \neq 1, \quad g^2+d^2 \neq 1$$

$$p = (a-ib)(g-id)$$

$$p^2 = (a^2+b^2)(g^2+d^2)$$

$$\Rightarrow (a^2+b^2)/p^2$$

The divisors p^2 are $1, p, p^2$

$$\text{ie) } a^2+b^2 = 1 \text{ (or) } a^2+b^2 = p^2 \text{ (or) } a^2+b^2 = p$$

$$\text{but } a^2+b^2 \neq 1$$

$$a^2+b^2 = p^2 \Rightarrow g^2+d^2 = 1.$$

which is not true.

$$\therefore a^2+b^2 = p$$

Hence the thm.

Lemma (i) :

If P is a prime number of the form $4n+1$. Then we can solve the congruence $x^2 \equiv -1 \pmod{P}$

Proof :

Let $x = 1, 2, \dots, (p-1)/2$

now $P = 4n+1$

$\Rightarrow P-1 = 4n \Rightarrow (p-1)/2 = 2n$

Hence in this product there are even number of terms.

Hence we can write

$$x = (-1)(-2) \dots \dots \dots (-(p-1)/2)$$

$$\% \quad P-k \equiv -k \pmod{p}$$

$$x \equiv (p-1)(p-2) \dots \dots \dots (p-(p-1)/2)$$

$$= (p-1)(p-2) \dots \dots \dots (P+1)/2$$

$$x^2 = 1.2 \dots \dots \dots (p-1)/2 \cdot (p+1)/2 \dots \dots \dots (p-2)(p-1)$$

$$\Rightarrow x^2 = (p-1)!$$

$$\angle p-1 \equiv -1 \pmod{p} \text{ (by wilson's them)}$$

$$x^2 \equiv -1 \pmod{p}$$

Hence the solution for $x^2 \equiv -1 \pmod{p}$ is $1, 2, \dots, (p-1)/2$.

Fermat's thm (ii) :

If P is a prime number of the form $4n+1$, then $p = a^2+b^2$ for some integers a and b .

Proof :

P is an prime number of the form $4n+1$

There exist an x such that $x^2 \equiv -1 \pmod{p}$

This x can be so chosen $|x| \leq P/2$

Even when $x > p$.

we can choose y such that $y = p-x$

$$|y| \leq p/2$$

$$y^2 = (p-x)^2$$

$$= p^2 + x^2 - 2xp$$

$$\equiv -1 \pmod{p}$$

$$\circ \quad x^2 \equiv -1 \pmod{p}$$

Hence there is always possible to choose x such that $|x| < p/2$.

$$\circ \quad x^2 \equiv -1 \pmod{p}$$

$$\Rightarrow \quad x^2 + 1 = cp \text{ for some integer } c.$$

Claim :

c is prime to p .

$$\text{ie) } (c, p) = 1$$

$$cp = x^2 + 1$$

$$\leq (p^2/4) + 1$$

$$\leq p^2$$

$$\Rightarrow \quad c \leq p \text{ and } p \text{ is a prime.}$$

$$\circ \quad (c, p) = 1.$$

Hence by lemma (i)

There are integer a and b

$$\text{such that } p = a^2 + b^2$$

Hence the proof.

Unique factorisation Domain :

Definition :

Let R be an integral domain with unity then R is called a unique factorisation domain (UFD) if

(i) every non-zero, non unit element a of R can be expressed as a product of finite number of irreducible elements of R and

$$\begin{aligned} \text{(ii) If } a &= p_1 p_2 \dots p_m \\ a &= q_1 q_2 \dots q_n \end{aligned}$$

where p_i and q_j are irreducible in R then $m = n$ and each p_i is an associate of some q_j .

Example :

The ring $\langle \mathbb{Z}, +, \cdot \rangle$ of integers is a UFD. We know it is an integral domain with unity. If $n \in \mathbb{Z}$ be any non-zero, non unit element (ie. $n \neq 0, \pm 1$) of $\mathbb{Z}$ then if $n > 0$.

we can write $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$ where p_i are primes.

$$\Rightarrow n = (p_1 p_1 \dots p_1) (p_2 p_2 \dots p_2) \dots (p_r p_r \dots p_r)$$

or that n is a product of prime (and thus irreducible) elements of $\mathbb{Z}$. Again this representation of n is unique (by fundamental thm of Arithmetic)

In case $n < 0$,

Let $n = (-m)$ where $m > 0$ then we can express m as product of primes in $\mathbb{Z}$.

$$\text{say, } m = q_1 q_2 \dots q_k$$

$$\text{then } (-m) = n = (-q_1)(q_2) \dots (q_k)$$

Example :

$\mathbb{Z}[\sqrt{-5}]$ is an integral domain which is not a UFD.

Solution :

$46 \in \mathbb{Z}[\sqrt{-5}]$ is a non unit, non-zero element and we can express it as product of irreducibles in two ways.

$$46 = 2 \cdot 23$$

$$46 = (1+3\sqrt{-5})(1-3\sqrt{-5})$$

But 2 is not an associate of

$$1+3\sqrt{-5} \text{ or } 1-3\sqrt{-5}$$

Hence $\mathbb{Z}[\sqrt{-5}]$ is not a UFD.

Theorem :

In a UFD, R be any two non-zero elements have a g.c.d.

Proof :

Let a, b be any two non-zero elements of R .

Suppose one of them (say a) is a unit then $aa^{-1} = 1$

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

$$\Rightarrow a/b$$

$$\text{Also } a = 1 \cdot a \Rightarrow a/a$$

now if c/a and c/b then as it

means c/a

$$\text{we get } a = \text{g.c.d.}(a, b)$$

III^{ly} if b is a unit, $b = \text{g.c.d.}(a, b)$

Let now a and b be non units.

since R is a UFD.

$$a = P_1^{\alpha_1} P_2^{\alpha_2} \dots P_n^{\alpha_n}$$

$$b = P_1^{\beta_1} P_2^{\beta_2} \dots P_n^{\beta_n}$$

As product of irreducibles

$$\text{Let } s_i = \min(\alpha_i, \beta_i)$$

$$\text{we show } d = P_1^{s_1} P_2^{s_2} \dots P_n^{s_n} \text{ is g.c.d.}(a, b)$$

$$\begin{aligned} a &= (P_1^{s_1} P_2^{s_2} \dots P_n^{s_n}) (P_1^{\alpha_1 - s_1} P_2^{\alpha_2 - s_2} \dots P_n^{\alpha_n - s_n}) \\ &= d (P_1^{\alpha_1 - s_1} P_2^{\alpha_2 - s_2} \dots P_n^{\alpha_n - s_n}) \end{aligned}$$

$$\Rightarrow d/a$$

III^{ly} d/b

Let now c/a and c/b

$$\text{If } C \text{ is a unit, } d = (cc^{-1})d \Rightarrow c/d.$$

If C is not a unit,

we can write

$$c = P_1^{r_1} P_2^{r_2} \dots P_n^{r_n}$$

$$\text{since } c/a, r_i \leq \alpha_i \quad \forall_i$$

$$c/b, r_i \leq \beta_i \quad \forall_i$$

$$\Rightarrow r_i \leq \min(\alpha_i, \beta_i) = s_i \quad \forall_i$$

Thus

$$d = P_1^{s_1} P_2^{s_2} \dots P_n^{s_n} = (P_1^{r_1} P_2^{r_2} \dots P_n^{s_n}) (P_1^{s_1-r_1} \dots P_n^{s_n-r_n})$$

$$\Rightarrow c/d$$

Hence $d = \text{g.c.d.}(a, b)$

which proves our result.

Lemma :

Every non-zero unit element in a PID, R is divisible by an irreducible element.

Proof :

Let $a \in R$, be a non zero,

non unit element.

Let $I_1 = (a)$

If I_1 is maximal ideal, then a is irreducible and as a/a .

Our lemma stands proved. Suppose I_1 is not maximal then f some ideal $I_2 \neq R$, s.t $I_1 \subset I_2 \subset R$.

Let $I_2 = (P_2)$

If I_2 is maximal then P_2 will be irreducible and as P_2/a .

∴ The Lemma is proved.

POLYNOMIAL RINGS

Consider expression of the type x^2-3x+2 (or) $x^3 - 1/2x^2 + 1/4$. These are called polynomial expressions with integer coefficients or rational coefficients. We are familiar with their properties like factorisation, nature of roots, etc. In this section we shall consider polynomial expression with coefficients from any commutative ring R with unit element and investigate how far the usual properties of polynomials with integer or rational coefficients, are valid for the general polynomial expressions. We shall define addition and multiplication of polynomials with coefficients in a ring R and show that they form a ring.

Definition :

A polynomial in x with coefficients from R is an expression of the type $f(x) = a_0 + a_1x + \dots + a_nx^n$ $a_i \in R, n \geq 0$.

Definition :

Two polynomials $f(x) = a_0 + a_1x + \dots + a_nx^n$ and $g(x) = b_0 + b_1x + \dots + b_mx^m$, $a_n b_m \neq 0$ will be equal if and only if $m=n$ and $a_i = b_i \forall i$.

Example :

- 1) $f(x) = x^3 + ix^2 - x (5+7i)$ is a polynomial with coefficients from the ring of Gaussian integers.
- 2) If $R = \{a+b\sqrt{-5} / a, b \in \mathbb{Z}\}$, then

$f(x) = (1+\sqrt{5})x^3 - x^2 + (7+8\sqrt{-5})x + 9$ is a polynomial with coefficient from R .

Definition :

Let $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$ and $g(x) = b_0 + b_1x + \dots + b_mx^m$ be two polynomials over R . Their sum $f+g$ and their product fg are defined as follows.

$$(f+g)(x) = (a_0+b_0) + (a_1+b_1)x + \dots$$

&

$$(fg)(x) = c_0 + c_1x + c_2x^2 + \dots + c_{m+n}x^{m+n}$$

where

$$c_i = a_0b_i + a_1b_{i-1} + a_2b_{i-2} + \dots + a_ib_0.$$

Example :

3) Let $R = \{a+b\sqrt{-5} / a, b \in \mathbb{Z}\}$

$$f(x) = x^2 + (1+\sqrt{-5})x + (2+3\sqrt{-5})$$

and $g(x) = x^3 - (3+7\sqrt{-5})x + (2-3\sqrt{-5})$

Then $(f+g)(x) = x^3 + x^2 - (2+6\sqrt{-5})x + 4$

and $(fg)(x) = x^5 + (1+\sqrt{-5})x^4 - (1+4\sqrt{-5})x^3 + (34-13\sqrt{-5})x^2 + (116-24\sqrt{-5})x + 49$

Definition :

The ring $R[x]$ is called the polynomial ring in x over R .

Lemma :

If R is a commutative ring with unit element, so is $R[x]$. If R is an integral domain then $R[x]$ is also an integral domain.

Proof :

Since R is an integer domain there exist $f, g \in R$ such that $fg = 0$.

To P.T $R[x]$ is non-zero.

$$f(x) + g(x) = [a_0 + a_1x + a_2x^2 + \dots + a_nx^n] + [b_0 + b_1x + \dots + b_nx^n]$$

$$= [(a_0 + b_0) + (a_1 + b_1)x + \dots + (a_n + b_n)x^n]$$

$$a_i, b_i \in R, a_i + b_i \in R$$

$$\therefore f(x) + g(x) \in R[x]$$

$f(x) + g(x)$ is closed and addition of polynomial.

$$h(x) = c_0 + c_1x + \dots + c_nx^n$$

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

$$(a_0 + b_0 + c_0) + (a_1 + b_1 + c_1)x + \dots + (a_n + b_n + c_n)x^n$$

$$= (a_0 + b_0 + c_0) + (a_1 + b_1 + c_1)x + \dots + (a_n + b_n + c_n)x^n$$

$$\therefore (f(x) + g(x)) + h(x) \in R[x]$$

$$\Rightarrow f(x) + (g(x) + h(x)) \in R[x]$$

◦ It is an associative property $f(0)$ is the identity element in $R[x]$.

$$\circ f(x)+f(0) = f(0)+f(x) = f(x)$$

$-f(x)$ is the additive inverse in $R[x]$

$$\circ f(x)+-(f(x)) = -f(x)+f(x) = f(0) \in R[x]$$

◦ $R[x]$ is an abelian group.

$$f(x)+g(x) = g(x)+f(x)$$

$$(a_0+b_0)+(a_1+b_1)x+\dots+(a_n+b_n)x^n = (a_0+b_0)+\dots+(a_n+b_n)x^n$$

$$\begin{aligned} f(x).g(x) &= (a_0+a_1x+\dots+a_nx^n)(b_0+b_1x+\dots+b_nx^n) \\ &= c_0+c_1x+\dots+c_nx^n \end{aligned}$$

$$[f(x).g(x)]h(x) = f(x) [g(x).h(x)]$$

$$(c_0+c_1x+\dots+c_nx^n)(d_0+d_1x+\dots+d_nx^n) = (a_0+a_1x+\dots+a_nx^n)(b_0+b_1x+\dots+b_nx^n)$$

$$f(x).[g(x)+h(x)] = (a_0+a_1x+\dots+a_nx^n)$$

$$[(b_0+c_0)+(b_1+c_1)x+\dots+(b_n+c_n)x^n]$$

$$\begin{aligned} &= a_0(b_0+c_0)+a_0(b_1+c_1)x+\dots+a_0(b_n+c_n)x^n \\ &\quad +\dots+a_n(b_n+c_m)x^n x^m \end{aligned}$$

$$\begin{aligned} f(x).g(x)+f(x).h(x) &= (a_0+a_1x+\dots+a_nx^n).(b_0+b_1x+\dots+b_mx^m) \\ &\quad +(a_0+a_1x+\dots+a_nx^n).(c_0+c_1x+\dots+c_r x^r) \\ &= (a_0b_0+a_0b_1x+\dots+a_0b_nx^n+\dots+a_nx^n b_mx^m) \\ &\quad +(a_0c_0+a_0c_1x+\dots+a_0c_nx^r+\dots+a_n c_r x^n x^r) \\ &= a_0(b_0+c_0)+a_0(b_1+c_1)x+\dots+a_n(b_n+c_n)x^n x^m \end{aligned}$$

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

$R[x]$ is a commutative ring.

To P.T $R[x]$ is an integral domain. We have to prove that no zero divisor.

$f(x), g(x)$ be non zero $a_n \neq 0, b_m \neq 0$

R is an integral domain. $a_n \neq 0, b_m \neq 0 \Rightarrow a_n b_m \neq 0$

now $f(x)g(x) = a_0b_0+(a_0b_1+a_1b_0)x+\dots+a_nb_mx^n x^m$

◦ $a_nb_m \neq 0, f(x)g(x)$ be non zero

polynomial in $R[x]$. ◦ $R[x]$ has no zero divisor. ◦ $R[x]$ is an integral domain.

Cor :

If R is an integral domain $R[x_1, x_2, \dots, x_n]$ is also an integral domain.

Proof :

Let

$$R_1 = R[x_1]$$

$$R_2 = R_1[x_2] = R[x_1, x_2]$$

$$R_3 = R_2[x_3] = R[x_1, x_2, x_3]$$

$$\dots \dots \dots$$

$$R_n = R_{n-1}[x_n] = R[x_1, x_2, \dots, x_n]$$

If R is an integral domain. $R_1 = R[x_1]$ is an integral domain. Let R, R_1 is an integral domain and so on.

Thus R_n is an integral domain.

Theorem :

If F is a field, every ideal in $F[x]$ is principal.

Lemma :

Let R be a commutative ring with unity and $\langle x \rangle$ be a prime ideal of $R[x]$. Show that R must be an integral domain.

Solution :

Let $a, b \in R$ be such that $ab=0$ then the polynomials.

$$(0+1x+0x^2+\dots) + (a+0x+0x^2+\dots) \text{ and}$$

$$(0+1x+0x^2+\dots) + (b+0x+0x^2+\dots) \in R[x]$$

$$\Rightarrow x+a, x+b \in R[x]$$

$$\Rightarrow (x+a)(x+b) \in R[x]$$

$$\Rightarrow x^2+x(a+b)+ab \in R[x]$$

$$\text{since } ab = 0, x^2+x(a+b) = x[x+a+b] \in \langle x \rangle$$

$$\text{Thus } (x+a)(x+b) \in \langle x \rangle$$

$$\Rightarrow (x+a) \in \langle x \rangle \text{ or } (x+b) \in \langle x \rangle$$

as $\langle x \rangle$ is prime ideal.

$$\begin{aligned} \text{now } (x+a) \in \langle x \rangle &\Rightarrow x+a = xf(x) \text{ for some } f(x) \in R[x] \\ &= x(a_0 + a_1x + \dots) \\ \Rightarrow a &= 0 \end{aligned}$$

III^{ly} if $(x+b) \in \langle x \rangle$ then $b=0$

Hence R is an integral domain.

Definition :

Let $f(x) \in R[x], f(x) \neq 0$. Then the largest n such that the coefficient of x^n in $f(x)$ is non-zero is called the degree of $f(x)$.

We use notation $\deg f$ to denote the degree of $f(x)$.

Theorem :

Let R any commutative ring. $f(x), g(x) \in R[x]$. Then $\deg(fg) \leq \deg f + \deg g$ and equality holds when R is an integral domain.

Proof :

$$\text{Let } f(x) = a_0 + a_1x + \dots + a_nx^n, a_n \neq 0$$

$$\text{so that } \deg f = n \text{ \& let}$$

$$g(x) = b_0 + b_1x + \dots + b_mx^m, b_m \neq 0$$

$$\text{with } \deg g = m$$

then

$$f(x)g(x) = a_0b_0 + (a_0b_1 + a_1b_0)x + \dots + a_nb_mx^{m+n}$$

$$\therefore \deg(fg) \leq m+n = \deg f + \deg g$$

$$\Rightarrow \deg(fg) \leq \deg f + \deg g$$

If R is an integral domain.

$$\text{then } a_nb_m \neq 0$$

$$\therefore \deg(fg) = m+n$$

$$\Rightarrow \deg(fg) = \deg f + \deg g$$

Cor :

If F is a field $\deg(fg) = \deg f + \deg g$ and in particular $\deg(fg) \geq \deg f$, as $\deg \geq 0$.

Definition :

If $f(x) \in R[x]$ is such that $\deg f = 0$ it is called a constant polynomial.

If $\deg f = 0$, then $f(x) = a_0 \in R$ and conversely if $a \in R$, then a can be identified with the polynomial $a + 0x + 0x^2 + \dots$ of degree 0. Thus the constant polynomials can be identified with elements of R and under this identification, R is a subring of $R[x]$.

Theorem :

If F is a field, then $F[x]$ is an Euclidean domain.

Proof :

We have seen that $F[x]$ is an integral domain with unity.

For any, $f(x) \in F[x]$, $f(x) \neq 0$

define

$$d(f(x)) = \deg f(x)$$

which is non(-ve) integer.

Since, for any $f(x), g(x) \in F[x]$,

$$f(x), g(x) \neq 0$$

$$\deg(f(x)g(x)) = \deg f(x) + \deg g(x)$$

we get

$$\deg(f(x)) \leq \deg(f(x)g(x))$$

As

$$\deg(g(x)) \geq 0$$

$\therefore$

$$d(f(x)) \leq d(f(x)g(x))$$

we show for any non zero $f(x), g(x) \in F[x]$ if $t(x)$ and $r(x) \in F[x]$

such that

$$f(x) = t(x)g(x) + r(x)$$

where either $r(x)$ is zero or

$$\deg r(x) < \deg g(x)$$

If

$$\deg f(x) < \deg g(x)$$

then

$f(x) = 0 \cdot g(x) + f(x)$ gives the result. Assume now the result is true for all non-zero polynomials in $F[x]$ of deg. less than $\deg f(x)$.

$$\text{Let } f(x) = a_0 + a_1x + \dots + a_mx^m$$

$$g(x) = b_0 + b_1x + \dots + b_nx^n$$

suppose $\deg f(x) \geq \deg g(x)$

Define :

$$f_1(x) = f(x) - a_m b_n^{-1} x^{m-n} g(x)$$

then coefficient of x^m in $f_1(x)$ is

$$a_m - a_m b_n^{-1} \cdot b_n = a_m - a_m = 0$$

$\therefore$ either $f_1(x) = 0$ (zero polynomial)

or $\deg f_1(x) < m$

If $f_1(x) = 0$, then

$$0 = f(x) - a_m b_n^{-1} x^{m-n} g(x)$$

gives $f(x) = a_m b_n^{-1} x^{m-n} g(x) + 0$

By taking

$$t(x) = a_m b_n^{-1} x^{m-n} \text{ and } r(x) = 0$$

we get the required result.

suppose $f_1(x) \neq 0$

then $\deg f_1(x) < m$

$\therefore \deg f_1(x) < \deg f(x)$

By induction hypothesis

$$f_1(x) = t_1(x)g(x) + r(x)$$

where either $r(x) = 0$ or $\deg r(x) < \deg g(x)$

$\therefore f(x) - a_m b_n^{-1} x^{m-n} g(x) = t_1(x)g(x) + r(x)$

or $f(x) = [a_m b_n^{-1} x^{m-n} + t_1(x)]g(x) + r(x)$

$$= t(x)g(x) + r(x)$$

where either

$r=0$ or $\deg r(x) < \deg g(x)$ and hence $F[x]$ is a Euclidean domain. This verifies the division algorithm in all cases, showing that $F[x]$ is a Euclidean domain.

Lemma :

Let R be a commutative integral domain with unit elements. Then the units of $R[x]$ are the same as units of R .

Proof :

Let $f(x) \in R[x]$ be a unit.

so that there exists some $g(x) \in R[x]$

such that $f(x)g(x) = g(x)f(x) = 1$.

now $0 = \deg 1 = \deg (fg) = \deg f + \deg g$

Thus

$\deg f = \deg g = 0$

$\therefore f$ and g are constant polynomials.

The relation $fg = 1 = gb$. shows that f is a unit in R .

Thus the units of $R[x]$ are the units of R and conversely every units of R is also a unit of $R[x]$.

Roots of Polynomials :

In order to define the roots of polynomials with coefficients in any ring R . We consider the following substitution mapping. For any fixed $\alpha \in R$, consider the mapping $S_\alpha : R[x] \rightarrow R$ defined by $S_\alpha (a_0 + a_1x + \dots + a_nx^n) = a_0 + a_1\alpha + \dots + a_n\alpha^n$. The element on the right - hand side is an element of R because, $a_0, a_1, \dots, a_n$ and α are in R , and R is a ring. S_α is clearly a ring homomorphism because let $f(x) = a_0 + a_1x + \dots + a_nx^n \in R[x]$ and $g(x) = b_0 + b_1x + \dots + b_mx^m \in R[x]$.

Then $S_\alpha(f(x)) = a_0 + a_1\alpha + \dots + a_n\alpha^n = f(\alpha)$

say

$S_\alpha(g(x)) = b_0 + b_1\alpha + \dots + b_m\alpha^m = g(\alpha)$

now

$S_\alpha(f(x) + g(x))$

$$= S_{\alpha} \{a_0 + b_0 + (a_1 + b_1)x + (a_2 + b_2)x^2 + \dots\}$$

$$= a_0 + b_0 + (a_1 + b_1)\alpha + (a_2 + b_2)\alpha^2 + \dots$$

$$= (a_0 + a_1\alpha + a_2\alpha^2 + \dots) + (b_0 + b_1\alpha + b_2\alpha^2 + \dots)$$

$$= f(\alpha) + g(\alpha) = S_{\alpha}(f(x)) + S_{\alpha}(g(x))$$

Also

$$S_{\alpha}(f(x) \cdot g(x))$$

$$= S_{\alpha} \{a_0b_0 + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + \dots\}$$

$$= a_0b_0 + (a_0b_1 + a_1b_0)\alpha + (a_0b_2 + a_1b_1 + a_2b_0)\alpha^2 + \dots$$

$$= (a_0 + a_1\alpha + a_2\alpha^2 + \dots)(b_0 + b_1\alpha + b_2\alpha^2 + \dots)$$

$$= f(\alpha)g(\alpha)$$

$$= S_{\alpha}(f(x)) \cdot S_{\alpha}(g(x))$$

Definition :

Let $f(x) \in R[x]$ and $\alpha \in R$. Then α is called a root of $f(x)$ if $S_{\alpha}(f(x)) = 0$. Thus α is a root of $f(x) = a_0 + a_1x + \dots + a_nx^n$ iff $S_{\alpha}(f) = f(\alpha) = a_0 + a_1\alpha + \dots + a_n\alpha^n = 0$.

Example:

1) If $R = \mathbb{Z}$ and $f(x) = x^3 + x^2 + x + 1$, then $\alpha = -1$ is a root of $f(x)$ as

$$f(-1) = -1 + 1 - 1 + 1 = 0.$$

2) If $R = \mathbb{Z} + i\mathbb{Z}$ and $f(x) = x^2 - 3x + 3 - i$, then $\alpha = 1 - i$ is a root of $f(x)$ as $f(1 - i)$

$$= (1 - i)^2 - 3(1 - i) + (3 - i) = 0$$

when R is a field, the division algorithm gives a criterion for α to be a root of $f(x)$.

Proposition :

Let F be a field and $f(x) \in F[x]$. Then $\alpha \in F$ is a root of $f(x)$ iff $(x - \alpha)$ divides $f(x)$.

Proof :

Since $F[x]$ is a Euclidean domain, we can write $f(x) = (x - \alpha)q(x) + r(x)$

where $r = 0$ or $\deg r < \deg(x - \alpha) = 1$

$\therefore r \in F$

Since S_{α} is a ring homomorphism.

$$\begin{aligned} f(\alpha) &= S_{\alpha}(f(x)) \\ &= S_{\alpha}(x-\alpha) S_{\alpha}(q(x)) + S_{\alpha}(r(x)) \end{aligned}$$

$$\circ \circ \quad f(\alpha) = 0 \cdot q(x) + r$$

$$\circ \circ \quad f(\alpha) = r$$

$$\text{Hence} \quad f(x) = (x-\alpha)q(x) + f(\alpha)$$

If α is a root of $f(x)$

then

$$f(\alpha) = 0$$

$$\circ \circ \quad f(x) = (x-\alpha)q(x)$$

Hence $(x-\alpha)/f(x)$

conversely,

If $x-\alpha/f(x)$

$$\circ \circ \quad f(x) = (x-\alpha) q(x)$$

$$\text{where} \quad q(x) \in F[x]$$

Hence

$$S_{\alpha}(f(x)) = S_{\alpha}(x-\alpha) \cdot S_{\alpha}(q(x))$$

$$\circ \circ \quad f(\alpha) = 0, q(\alpha) = 0$$

Hence α is a root of $f(x)$.

Lemma :

Let F be a field and $f(x) \in F[x]$ be a polynomial of $\deg n$. Then $f(x)$ has at most n distinct roots in F .

Proof :

Let $\alpha_1, \alpha_2, \dots, \alpha_m$ be the distinct roots of $f(x) \in F$.

$$\circ \circ \quad x - \alpha_1 / f(x)$$

$$\Rightarrow \quad f(x) = (x - \alpha_1)g(x)$$

$$\text{now} \quad (x - \alpha_2) / f(x)$$

$$\text{since} \quad \alpha_1 \neq \alpha_2$$

∴

$$x - \alpha_2 \mid x - \alpha_1$$

Hence

$$x - \alpha_2 \mid g(x)$$

$$g(x) = (x - \alpha_2)h(x)$$

∴

$$f(x) = (x - \alpha_1)(x - \alpha_2)h(x)$$

containing the argument, we have

$$f(x) = (x - \alpha_1)(x - \alpha_2)\dots(x - \alpha_m)\phi(x)$$

In particular $n = \deg f = m + \deg \phi \geq m$

Thus $f(x)$ has at most n distinct roots in F .

Cor :

Let $f(x) \in F[x]$ be of deg 2 or 3. Then $f(x)$ is reducible iff $f(x)$ has a root in F .

Proof :

If $f(x)$ has a root $\alpha \in F$

then $f(x) = (x - \alpha)g(x)$

∴ $f(x)$ is reducible as $\deg f > 1$.

conversely,

If $f(x)$ is reducible, then

$$f(x) = g(x)h(x) \text{ where } \deg g < \deg f \text{ and } \deg h < \deg f.$$

∴ $\deg f = 2 \text{ or } 3$

either $\deg g = 1 \text{ or } \deg h = 1$

suppose g is of degree 1 then

$$g(x) = a_0 + a_1x$$

then $x + a_1^{-1}a_0 \mid f(x)$

∴ $\alpha = -a_0a_1^{-1}$ is a root of $f(x)$.

Hence the proof

Factorization of Polynomials :

Theorem (Eisentein's Oriterion) :

Let R be a UFD and $f(x) \in R[x]$ where $f(x) = a_0 + a_1x + \dots + a_nx^n$. Suppose there exists an irreducible element $P \in R$ such that $P \nmid a_0, P \nmid a_1, \dots, P \nmid a_{n-1}, P \nmid a_n, P^2 \nmid a_0$ then $f(x)$ is irreducible.

Proof :

Suppose $f(x)$ is reducible

Then $f(x) = g(x)h(x)$ where $\deg g < n$ and $\deg h < n$

Let $g(x) = b_0 + b_1x + \dots + b_r x^r, b_r \neq 0, r < n$

$h(x) = c_0 + c_1x + \dots + c_s x^s, c_s \neq 0, s < n.$

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

we have

$$a_i = b_i c_0 + b_{i-1} c_1 + \dots + b_0 c_i$$

since P/a_0 we have P/b_0 or P/c_0

but not both as $P^2 \nmid a_0$.

suppose P/b_0 and $P \nmid c_0$

Since $P \nmid a_n, P \nmid b_i$ for some i .

Choose least i such that $P \nmid b_i$

$\nmid P \nmid b_i$

but $P/b_{i-1} \dots \dots P/b_0$ ($1 \leq i \leq r \leq n$)

consider

$$a_i = b_i c_0 + b_{i-1} c_1 + \dots + b_0 c_i$$

Since $i < n$, we have P/a_i and $P/b_0 \dots \dots P/b_{i-1}$

Hence $P/b_i c_0$

This is $\Rightarrow \Leftarrow$

Because $P \nmid b_i$ and $P \nmid c_0$

Hence $f(x)$ is irreducible.

Definition :

Let R be a UFD and $f(x) = a_0 + a_1x + \dots + a_n x^n$ in $R[x]$. Then the gcd of the coefficients $a_0, a_1, a_2, \dots, a_n$ is called the content of $f(x)$. It is denoted by $c(f)$.

Example :

1) If $f(x) = 3x^3 - 2x^2 + 9x + 6 \in \mathbb{Z}[x]$

then $c(f) = 1$.

2) If $f(x) = 2x^2 - (1+i)x - 2 \in R[x]$

where $R = \mathbb{Z} + i\mathbb{Z}$, then $c(b) = 1+i$

Definition :

Let $f(x) \in R[x]$ and $\alpha \in R$, α is called a multiple root of multiplicity $k (k \geq 1)$ iff $(x-\alpha)^k \mid f(x)$ but $(x-\alpha)^{k+1} \nmid f(x)$.

Example :

- 1) If $R = \mathbb{Z}$ and $f(x) = x^3 - 5x^2 + 7x - 3$ then $f(x)$ has $\alpha = 1$ as a root of multiplicity 2.
- 2) If $R = \mathbb{Z} + i\mathbb{Z}$ and $f(x) = x^4 - 2ix^3 - 2ix - 1$ then $f(x)$ has $\alpha = i$ as a root of multiplicity 3.

Lemma :

Let F be a field and let $f(x) \in F[x]$ be a polynomial of $\deg n$. Then $f(x)$ has at most n roots in F , where a root of multiplicity k is counted k times.

Proof :

Let $\alpha_1, \alpha_2, \dots, \alpha_m$ be the distinct roots of $f(x)$ with multiplicities $k_1, k_2, \dots, k_m$ respectively.

we shall show that $k_1 + k_2 + \dots + k_m \leq n$ Since α_1 is a root of multiplicity k_1 .

$$f(x) = (x - \alpha_1)^{k_1} g(x)$$

where $(x - \alpha_1) \nmid g(x)$

now,

$$(x - \alpha_2)^{k_2} \mid f(x)$$

and since it is relatively prime to $(x - \alpha_1)^{k_1}$ (as $\alpha_1 \neq \alpha_2$)

$$\therefore (x - \alpha_2)^{k_2} \mid g(x)$$

$$\therefore g(x) = (x - \alpha_2)^{k_2} h(x)$$

$$\text{Thus } f(x) = (x - \alpha_1)^{k_1} (x - \alpha_2)^{k_2} h(x)$$

continuing the argument

we have that

$$f(x) = (x - \alpha_1)^{k_1} (x - \alpha_2)^{k_2} \dots (x - \alpha_m)^{k_m} \phi(x)$$

Hence $n = \deg f = k_1 + k_2 + \dots + k_m \deg \phi \geq k_1 + k_2 + \dots + k_m$.

Thus

If each root α_i of multiplicity k_i is counted k_i times.

The number of roots of $f(x) \in F$ is almost n .

This proves the lemma.

Definition :

Let R be a UFD. Then $f(x)$ is called a primitive polynomial, if $c(f) = 1$

Theorem :

Let R be a UFD. Then the product of two primitive polynomials over R is also a primitive polynomial.

Proof :

Let
$$f(x) = a_0 + a_1x + \dots + a_nx^n$$

$$g(x) = b_0 + b_1x + \dots + b_mx^m$$
 be two

primitive polynomials in $R[x]$

Let P be any irreducible element in R .

Since $f(x)$ and $g(x)$ are primitive polynomials. P does not divide all a_i^s and P does not divide all b_j^s .

Let a_r be the first coefficient of $f(x)$

not divisible by P .

$\therefore P/a_1, P/a_2, \dots, P/a_{r-1}$ and P does not divide a_r (1)

Let b_s be the first coefficient of $g(x)$ not divisible by P .

$\therefore P/b_1, P/b_2, \dots, P/b_{s-1}$ and P does not divide b_s

now the coefficient of x^{r+s} in $f(x)g(x)$ is given by,

$$C_{r+s} = (a_0b_{r+s} + a_1b_{r+s-1} + \dots + a_{r-1}b_{s+1}) + a_rb_s + (a_{r+1}b_{s-1} + \dots + a_{r+s}b_0)$$

from (1) & (2) we get

$$P / (a_0b_{r+s} + a_1b_{r+s-1} + \dots + a_{r-1}b_{s+1})$$

$$P / a_{r+1}b_{s-1} + \dots + a_{r+s}b_0 \text{ and } P \text{ does not divide } a_rb_s.$$

∴ P does not divide C_{r+s} .

Thus for any irreducible element $P \in R$

There exists some coefficient of $f(x) g(x)$ not divisible by P.

Hence $f(x) g(x)$ is primitive.

Lemma:

If R is a UFD. Then so in $R[x]$

Proof :

Let $f(x)$ be any arbitrary

Polynomial in $R[x]$

Then $f(x) = c f_1(x)$

where $C = C(f), C \in R$

∴ $f_1(x)$ is a primitive in $R[x]$.

By lemma,

If R is a UFD and if $P[x]$ is a primitive polynomial in $R[x]$,

Then it can be factorial in a unique way as a product of irreducible element in $R[x]$.

$$f_1(x) = P_1(x) \dots P_n(x)$$

where $P_i(x)$ is irreducible polynomial in $R[x]$

R is a UFD.

suppose $C = C_1 C_2 \dots C_n$

Also

$$f(x) = C_1 \dots C_n P_1(x) \dots P_n(x)$$

Hence the theorem.

Theorem (Gauss lemma):

Let R be a UFD and F the quotient field of R. Let $f(x) \in R[x]$ be irreducible in $R[x]$. Then $f(x)$ is also irreducible in $F[x]$.

Proof :

If possible Let $f(x)$ be reducible in $F[x]$

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

with $\deg g < \deg h < \deg f$.

we can write

$$g(x) = (a/b) g_1(x)$$

and $h(x) = (c/d) h_1(x)$

where $a, b, c, d \in R$

And $g_1(x), h_1(x) \in R[x]$ both being primitive.

Then $f(x) = ac/bd g_1(x) h_1(x)$

by Lemma,

Let R be a UFD then the product of two primitive polynomials over R is also a primitive polynomial.

∴ $g_1(x) h_1(x)$ is primitive.

since $f(x) \in R[x]$ is irreducible.

∴ $c(f) / f$

∴ $c(f) = 1$.

∴ f is primitive.

now

$$bdf(x) = acg_1(x)h_1(x) \text{ and comparing contents on both sides,}$$

we have

$$\text{∴ } bd = ac.$$

Hence $f(x) = g_1(x) h_1(x)$ where $g_1(x), h_1(x) \in R[x]$ and

$$\deg g_1 = \deg g < \deg f,$$

$$\deg h_1 = \deg h < \deg f$$

This contradicts the assumption that

$$f(x) \in R[x] \text{ is irreducible.}$$

Hence $f(x)$ is irreducible in $F[x]$.

This proves the lemma.

Cor :

If P is prime, then $f(x) = 1 + x + x^2 + \dots + x^{p-1} \in \mathbb{Q}[x]$ is irreducible.

Proof :

$$\begin{aligned}
 \text{Let } f(x) &= 1+x+x^2+\dots+x^{p-1} \\
 f(x+1) &= 1+(x+1)+\dots+(x+1)^{p-1} \\
 &= \frac{(x+1)^p-1}{(x+1)-1} \\
 &= x^{p-1} + \binom{p}{1}x^{p-2} + \dots + p \\
 &= p + \binom{p}{1}x + \binom{p}{2}x^2 + \dots + x^{p-1}
 \end{aligned}$$

Since

By Eisenstein's criterion,

$f(x+1)$ is irreducible over $\mathbb{Z}$.

Hence $f(x) \in \mathbb{Z}[x]$ is irreducible.

By Gauss lemma,

$\therefore f(x)$ is irreducible also in $\mathbb{Q}[x]$.

Theorem (Gauss Theorem) :

Let R be a UFD then the polynomial ring $R[x]$ is also a UFD.

Proof :

we shall show first that R is a factorization domain.

Let $f(x) \in R[x]$

and let F be the quotient field of R .

Let $f(x) = d \cdot f_1(x)$

where $d = C(f)$ and $f_1(x) \in R[x]$ is primitive.

Since $F[x]$ is a UFD.

we can write

$$f_1(x) = p_1(x)p_2(x)\dots p_n(x)$$

where $p_i(x) \in F[x]$ are irreducible.

write $p_i(x) = (a_i/b_i)q_i(x)$ where $a_i, b_i \in R$

and $q_i(x) \in R[x]$ and primitive.

$$\text{Then } f_1(x) = \frac{a_1 a_2 \dots a_n}{b_1 b_2 \dots b_n} q_1(x) \dots q_n(x)$$

$$\circ (b_1 b_2 \dots b_n) f_1(x) = a_1 \dots a_n q_1(x) \dots q_n(x)$$

since $f_1(x)$ and $q_1(x) q_2(x) \dots q_n(x)$ are primitive.

By comparing the contents on both sides,

we have

$$(b_1 \dots b_n) = (a_1 \dots a_n)$$

$$\text{Thus } f_1(x) = q_1(x) \dots q_n(x) \text{ with } q_i(x) \in R[x]$$

primitive and irreducible in $F[x]$

Then $q_i(x)$ are irreducible as elements of $R[x]$ also.

We can factorize $C(f) = d = \pi_1 \pi_2 \dots \pi_k$

where $\pi_i \in R$ are irreducible.

So that $f(x) = d f_1(x) = \pi_1 \pi_2 \dots \pi_k q_1(x) \dots q_n(x)$ is a factorization of $f(x)$ as a product of irreducible elements of $R[x]$.

now we shall prove the uniqueness of factorization.

$$\text{Let } f(x) = \pi_1 \dots \pi_k q_1(x) \dots q_n(x) \text{ and}$$

$$f(x) = \pi_1^1 \dots \pi_l^1 q_1^1(x) \dots q_m^1(x) \text{ be}$$

two factorizations of $f(x)$ as products of irreducible elements.

where $\pi_i, \pi_j^1 \in R$, $\deg q_i, \deg q_j^1$ positive

since $q_i(x), q_j^1(x)$ are irreducible in $R[x]$, they are primitive.

Hence the products $q_1(x) \dots q_n(x)$ and $q_1^1(x) \dots q_m^1(x)$ are also primitive.

Comparing contents on both sides,

$$\text{we have } C(f) = \pi_1 \dots \pi_k = \pi_1^1 \dots \pi_l^1$$

$$\text{and hence } q_1(x) \dots q_n(x) = q_1^1(x) \dots q_m^1(x)$$

Since R is a UFD.

$$k = l \text{ and each } \pi_i = u_i \pi_i^1$$

where $u_i \in R$ is a unit.

now consider the relation $q_1(x)q_2(x)\dots q_n(x)$

$$= q_1^1(x)q_2^1(x)\dots q_m^1(x)$$

Each $q_i(x)$ & $q_i^1(x)$ is primitive and irreducible in $R[x]$

By Gauss lemma,

They are irreducible in $F[x]$ also

Since $F[x]$ is a UFD.

We have $n=m$ and $q_i(x) = (a_i/b_i) q_i^1(x)$ with $a_i/b_i \in F$, $a_i/b_i \neq 0$

now,

$$p_i q_i(x) = a_i q_i^1(x)$$

By comparing contents on both sides,

we have

$$b_i = a_i$$

Thus

$$q_i(x) = q_i^1(x) \text{ for each } i.$$

Hence the factorization is unique.

This proves the Gauss theorem.

Definition :

Let R be an integral domain. Then the quotient field of $R[x]$ is called the field of rational functions in x over R .

It is usually denoted by the symbol $R(x)$. Elements of $R(x)$ are of the form $f(x)/g(x)$ where $f(x), g(x) \in R[x]$, $g(x) \neq 0$

Lemma :

Let R be an integral domain, K its quotient field. Then the field of rational function $R(x)$ over R is the same as the field of rational functions $K(x)$ over K .

Proof :

Since $R \subset K$, $R(x) \subset K(x)$

conversely

Let $1(x) \in k(x)$

so that $q(x) = f(x)/g(x)$

where $f(x), g(x) \in k[x]$, $g(x) \neq 0$

we can write $f(x) = (a/b)f_1(x)$, $a, b \in R$, $b \neq 0$ and $f_1(x) \in R[x]$

and $g(x) = (c/d)g_1(x)$, $c, d \in R$, $d \neq 0$ and $g_1 \in R[x]$

$$\text{Then } q(x) = \frac{ad f_1(x)}{bc g_1(x)} = \frac{\phi(x)}{\psi(x)}$$

where $\phi(x) = ad f_1(x)$ and

$\psi(x) = bc g_1(x)$ both belong to $R[x]$.

Thus $q(x) \in R(x)$ showing that $k(x) = R(x)$

This proves the lemma.

Lemma (i) :

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

Proof :

Given $f(x)$ is primitive and

irreducible in $R[x]$.

To P.T. $f(x)$ is irreducible in $F[x]$.

It possible $f(x)$ is reducible in $F[x]$

$$f(x) = g(x)h(x) \text{ where } g_0(x), h_0(x) \in R[x] \text{ } a, b \in R$$

$$abf(x) = c_1 g_1(x) c_2 h_1(x)$$

where $c_1 = c(g_0)$

$$c_2 = c(h_0)$$

$g_1(x)$ and $h_1(x)$ are primitive polynomial in $R[x]$.

$$= c_1 c_2 g_1(x) h_1(x)$$

$$f(x) = g_1(x) h_1(x) \text{ [} g_1(x), h_1(x) \text{ is primitive}$$

$$ab = c_1 c_2 \text{ upto associates]}$$

$$\Rightarrow f(x) \text{ is reducible in } R[x]$$

$\Rightarrow \Leftarrow$

$\therefore f(x)$ is irreducible in $F[x]$.

Lemma (ii) :

If R is an UFD and if $p[x]$ is primitive polynomial in $R[x]$. Then it can be factorial in a unique way as the product of irreducible element in $R[x]$.

Proof :

Given $P(x) \in R[x]$

$\Rightarrow P(x) \in F[x]$

$F[x]$ is UFD.

$\circ P(x) = P_1(x) \dots P_n(x)$ where $P_i \in F[x]$

$$= \frac{q_1(x)}{a_1} \frac{q_2(x)}{a_2} \dots \frac{q_n(x)}{a_n}$$

where $q_i \in R[x], a_i \in R$

$P_i(x)$ are irreducible in $F[x]$

$q_i(x)$ are irreducible in $F[x]$

$\circ a_1 a_2 \dots a_n P(x) = c_1 s_1(x) c_2 s_2(x) \dots c_n s_n(x)$

where $c_i = c(q_i)$

$$= c_1 c_2 \dots c_n s_1(x) \dots s_n(x)$$

$[s_i(x)$ is primitive and irreducible polynomial in $R[x]$]

since $p(x), s_1(x) \dots s_n(x)$ are primitive

$$a_1 \dots a_n = c_1 c_2 \dots c_n$$

$$P(x) = s_1(x) s_2(x) \dots s_n(x)$$

$\circ P(x)$ can be written as the product of irreducible elements in $R[x]$.

To prove the uniqueness If possible

Let $P(x) = t_1(x) t_2(x) \dots t_n(x)$

where $t_i(x)$ is primitive and irreducible in $R[x]$

$t_i(x)$ is irreducible in $F[x]$ also.

by lemma (i) $\parallel^y s_i(x)$ is irreducible in $F[x]$

now in $F[x]$ is

$$P(x) = s_1(x) s_2(x) \dots s_n(x)$$

$$P(x) = t_1(x) t_2(x) \dots t_n(x)$$

Since $F[x]$ is an UFD. These two are equal upto associates.

$$s_1(x) \dots s_n(x) \doteq t_1(x) t_2(x) \dots t_n(x)$$

Hence $P(x)$ has UFD as a product of irreducible element in $R[x]$.

This proves the lemma.

Lemma :

If $f(x)$ be a non-zero polynomials in $R[x]$ where R is an integral domain with unity, then $f(x) = df_1(x)$ where f_1 is primitive and $d=c(f)$.

Proof :

$$\text{Let } f(x) = a_0 + a_1x + \dots + a_nx^n$$

$$\text{and } c(f) = d = \text{g.c.d.}(a_0, a_1, \dots, a_n)$$

$$\text{then } d/a_i \forall i$$

$$\Rightarrow a_i = du_i \text{ for some } u_i$$

$$f(x) = du_0 + du_1x + \dots + du_nx^n$$

$$= d(u_0 + u_1x + \dots + u_nx^n)$$

$$\Rightarrow f(x) = df_1(x)$$

where $f_1(x)$ will be primitive

Theorem :

In a UFD an element is prime iff it is irreducible.

Proof :

Let $a \in R$ be a prime element, then since R is an integral domain with unity, a will be irreducible.

conversely, Let $a \in R$ be irreducible then a is non-zero unit. Let a/bc then $bc=ak$ for some k .

Case (i) :

b is a unit

$$\text{then } c = akb^{-1} = a(kb^{-1}) \Rightarrow a/c$$

Case (ii) :

C is a unit then similarly, a/b

Case (iii) :

b, c is a non-unit if k is a unit.

then

$$bc = ak$$

$\Rightarrow$

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

Since a is irreducible, either b or ck^{-1} is a unit. But b is not a unit.

Thus ck^{-1} is a unit.

But that implies c is a unit, which is again not true.

Hence k is not a unit.

we can thus express

$$b = p_1 p_2 \dots p_m$$

$$c = q_1 q_2 \dots q_n$$

$$k = r_1 r_2 \dots r_t \text{ as product of irreducibles}$$

(by definition of UFD)

$\therefore$

$$bc = ak \text{ becomes}$$

$$p_1 p_2 \dots p_m q_1 q_2 \dots q_n = a r_1 r_2 \dots r_t = x \text{ (say)}$$

Then x is an element having two representations as product of irreducible elements by definition of UFD each element in one representation is an associate of some element.

$\Rightarrow a$ is an associate of some p_i or some p_j .

$\Rightarrow ua = p_i$ or $ua = q_j$ for some unit $(p_i/b, q_j/c)$

$\Rightarrow a/p_i$ or $a/q_j \Rightarrow a/b$ or a/c

$\Rightarrow a$ is primitive.

FIELD EXTENSION

Definition :

Let F be a field and K another field containing F . Then K is called an extension of F and is denoted by the symbol K/F .

Example :

- 1) $F = \mathbb{Q}$, $K = \mathbb{R}$ and $L = \mathbb{C}$, the field of rational real and complex numbers. Then K is an extension of F and L is an extension of K .
- 2) Let F be any field and $K = F(x)$, the field of rational function in x over F . i.e. the quotient field of the polynomial ring $F[x]$. Then K is an extension of F .

Definition :

Let K/F be extension, $\alpha_1, \alpha_2, \dots, \alpha_n \in F$. The smallest subfield of K containing F and $\alpha_1, \alpha_2, \dots, \alpha_n$ is called the field generated by $\alpha_1, \dots, \alpha_n$ over F and is denoted by $F(\alpha_1, \alpha_2, \dots, \alpha_n)$.

Definition :

K/F is called a simple extension if $K = F(\alpha)$

Example :

Let $F = \mathbb{Q}$ and

$$K = \left\{ \frac{a+b\sqrt{2}}{c+d\sqrt{2}} \mid a, b, c, d \in \mathbb{Q}, c \text{ or } d \neq 0 \right\}$$

Then K is a field and $K = \mathbb{Q}(\sqrt{2})$ is a simple extension of $\mathbb{Q}$.

Lemma :

Let K/F be a field extension and $\alpha_1, \alpha_2, \dots, \alpha_n \in K$. If

$$L = \left\{ \frac{f(\alpha_1, \dots, \alpha_n)}{g(\alpha_1, \dots, \alpha_n)} \mid f, g \in [x_1, \dots, x_n], g(\alpha_1, \alpha_2, \dots, \alpha_n) \neq 0 \right\} \text{ then } L \text{ is an extension}$$

of F and is the smallest extension of F containing $\alpha_1, \alpha_2, \dots, \alpha_n$.

Proof :

Part I :

To show that L is a field and that $L \supseteq F$

$$a \in F \Rightarrow a = a/1 \in L$$

Since the Nr & Dr are constant functions of $\alpha_1, \dots, \alpha_n$.

Thus $F \subseteq L$ suppose $x, y \in L$.

$$\text{Then } x = \frac{f_1(\alpha_1, \dots, \alpha_n)}{g_1(\alpha_1, \dots, \alpha_n)}$$

$$y = \frac{f_2(\alpha_1, \dots, \alpha_n)}{g_2(\alpha_1, \dots, \alpha_n)} \text{ with } f_1, f_2, g_1, g_2 \in F[x_1, x_2, \dots, x_n]$$

are polynomials in n indeterminants $x_1, \dots, x_n$ over F and $g_1(\alpha_1, \dots, \alpha_n) \neq 0$, $g_2(\alpha_1, \dots, \alpha_n) \neq 0$

$$\text{Then } x+y = \frac{f(\alpha_1, \dots, \alpha_n)}{g(\alpha_1, \dots, \alpha_n)} \text{ where } g = g_1 g_2.$$

$$f = f_1 g_2 + f_2 g_1 \in F[x_1, \dots, x_n] \text{ and}$$

$$g(\alpha_1, \dots, \alpha_n) = g_1(\alpha_1, \alpha_2, \dots, \alpha_n) \cdot g_2(\alpha_1, \alpha_2, \dots, \alpha_n) \neq 0$$

$$\text{Hence } x+y \in L$$

III^{ly} $x-y \in L$, $xy \in L$ and if $x \neq 0$

then

$$f_1(\alpha_1, \alpha_2, \dots, \alpha_n) \neq 0$$

$$\therefore 1/x = \frac{g_1(\alpha_1, \dots, \alpha_n)}{f_1(\alpha_1, \dots, \alpha_n)} \in L$$

This proves that L is a subfield of K and that $L \supseteq F$.

Part II :

To prove L is the smallest subfield containing F and $\alpha_1, \dots, \alpha_n$.

Let M be any field (contained in K) containing F and $\alpha_1, \dots, \alpha_n$.

Then clearly $f(\alpha_1, \dots, \alpha_n) \in M \forall f \in F[x_1, \dots, x_n]$

If $g \in F[x_1, \dots, x_n]$ with $g(\alpha_1, \dots, \alpha_n) \neq 0$

then $\frac{f(\alpha_1, \dots, \alpha_n)}{g(\alpha_1, \dots, \alpha_n)} \in M$

This shows that every element of L is an element M .

Hence we have shown that L is the smallest subfield of K containing F and $\alpha_1, \dots, \alpha_n$.

This completes the proof of the Lemma.

Lemma :

Let K/F be a simple extension with $K = F(\alpha)$. Then, either (i) there does not exist any non-zero polynomial $g(x) \in F[x]$ with $g(\alpha) = 0$, (or) (ii) there exists a unique monic polynomial $f(x)$ of least degree with $f(\alpha) = 0$

Proof :

Consider the map $\phi: F[x] \rightarrow F[\alpha]$

defined by $\phi(h(x)) = h(\alpha)$, $h(\alpha) \in F[\alpha]$

ϕ is clearly a ring homomorphism which is onto.

Let $I = \text{Ker } \phi$.

Case (i) :

If $I = 0$, there does not exist any non-zero polynomial $g(x) \in F[x]$ with $g(\alpha) = 0$, proving (i).

Case (ii) :

If $I \neq 0$

In this case, $I = (f(x))$

since $F[x]$ is a PID.

$f(x)$ unique if it is chosen to be monic.

clearly $f(\alpha) = 0$

Let $h(x) \in F[x]$ with $h(\alpha) = 0$

Then $h(\alpha) \in I$ and $h(x)$ is a multiple of $f(x)$.

$\deg h \geq \deg f$

proving (ii) :

We see further that I is a non-zero prime ideal since $F[x]$ is a domain and hence I is maximal.

$$\circ \quad \frac{F[x]}{I} \simeq F[\alpha] \text{ is a field}$$

This shows that $F[\alpha] = F[\alpha]$

Definition :

Let K/F be an extension $\alpha \in K$. α is called transcendental over F if there does not exist any non-zero $f(x) \in F[x]$ with $f(\alpha) = 0$. Otherwise α is called algebraic over F and the unique monic polynomial $f(x) \in F[x]$ of least degree with $f(\alpha) = 0$ is called the minimum polynomial of α .

Example :

- 1) Let $F = \mathbb{R}$ then $\alpha = i = \sqrt{-1}$ is algebraic over F with minimum polynomial $x^2 + 1$
- 2) Let $F = \mathbb{R}$ and $\alpha = e$ or π then α is transcendental over F .
- 3) Let $F = \mathbb{Q}$ and $\alpha = \sqrt[3]{2}$ then α is algebraic over F with minimum polynomial $x^3 - 2 \in \mathbb{Q}[x]$

Lemma :

Let $\alpha \in K$ be algebraic over F and $f(x)$ the minimum polynomial of α , with $\deg f(x) = n$. Then $F(\alpha)$ has dimension n as a vector space over F .

Proof :

Let K/F be a simple extension with $K = F(\alpha)$ then there exists a unique monic polynomial $f(x)$ of least degree with $f(\alpha) = 0$

$$\text{by} \quad F(\alpha) \simeq \frac{F[x]}{(f(x))} \simeq F[\alpha], \text{ where}$$

$$f(x) = x^n + a_1 x^{n-1} + \dots + a_n, \quad a_i \in F$$

we claim that $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$ is a basis of $F(\alpha)$.

They are clearly linearly independent for otherwise α will satisfy a polynomial of degree less than n over F contradicting that $f(x)$ is the minimum polynomial of α .

$$\text{Since} \quad \alpha^n = -(a_1 \alpha^{n-1} + \dots + a_n)$$

$$\alpha^{n+1} = -(a_1\alpha^n + a_2\alpha^{n-2} + \dots + a_n\alpha)$$

This is again an F - linear combination of $1, \alpha, \dots, \alpha^{n-1}$ by substituting for α^n
 IIIly, Any power of α is an F - linear combination of $1, \alpha, \dots, \alpha^{n-1}$.

Thus $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$ is a generating set of $F(\alpha)$.

$\therefore F(\alpha)$ over F .

In particular $\dim_F F(\alpha) = n$

This proves the lemma.

Definition :

Let K/F be an extension. It is called a finite extension if $\dim_F K < \infty$ and this dimension is denoted by $[K:F]$

Example :

If α is algebraic over F with minimum polynomial of degree n , then $[F(\alpha):F] = n$.

Theorem :

Let K/F be a finite extension. Then K/F is an algebraic extension (or) (Every finite extension is an algebraic extension).

Proof :

Let $[K:F] = n$ So that any set of $(n+1)$ elements of K is L.D over F .

If α is any element of K , then the set $\{1, \alpha, \alpha^2, \dots, \alpha^n\}$ of $(n+1)$ elements is L.D. over F
 $\Rightarrow \exists$ elements

$a_0, a_1, \dots, a_n$ not all zero in F such that $a_0 + a_1\alpha + \dots + a_n\alpha^n = 0$

ie) $f(\alpha) = 0$ where $f(\alpha) = \sum_{i=0}^n a_i x^i \neq 0$

Hence α is algebraic over F .

Since every $\alpha \in K$ is algebraic over F , K/F is an algebraic extension.

Theorem :

Let $F \subset K \subset L$ be extensions such that K/F and L/F are finite. Then L/F is finite and $[L:F] = [L:K][K:F]$

Proof :

Let $\{\ell_1, \ell_2, \dots, \ell_n\}$ be a basis of K/F and $\{f_1, f_2, \dots, f_m\}$ be a basis of L/F . we claim that $\{\ell_i f_j\}$, $1 \leq i \leq n$, $1 \leq j \leq m$ is a basis of L/F .

Let $\alpha \in L$ So that $\alpha = \sum_{j=1}^n b_j f_j$, $b_j \in K$

now

$$b_j = \sum_i \lambda_{ij} e_i, \lambda_{ij} \in F$$

Then

$$\begin{aligned} \alpha &= \sum_j \left(\sum_i \lambda_{ij} e_i \right) f_j \\ &= \sum_{i,j} \lambda_{ij} e_i f_j, \lambda_{ij} \in F \end{aligned}$$

This shows that $\{\ell_i f_j\}$ generates L over F .

To prove the linear independence,

Let

$$\sum_{ij} \mu_{ij} e_i f_j = 0, \mu_{ij} \in F$$

Then

$$\sum_j \left(\sum_i \mu_{ij} e_i \right) f_j = 0$$

since $f_1, \dots, f_m$ are linearly independent over k .

$$\sum_i \mu_{ij} e_i = 0, \forall j$$

since $\ell_1, \ell_2, \dots, \ell_n$ are linearly independent over F , $\mu_{ij} = 0 \forall i, j$

Thus $\{\ell_i f_j\}$ is a basis of L over F .

In particular,

$$[L:F] = mn = [L:K][K:F]$$

Hence the theorem.

Cor :

Let K/F be a finite extension and $\alpha \in k$ with minimum polynomial of degree n . Then n divides $[K:F]$

Proof :

This is because $[K:F] = [K:F(\alpha)][F(\alpha):F]$ and $[F(\alpha):F] = \text{degree of the minimal polynomial of } \alpha \text{ over } F = n$.

Cor :

Let K/F be an extension, $\alpha_1, \dots, \alpha_n \in K$ algebraic over F . Then $F(\alpha_1, \dots, \alpha_n)/F$ is a finite extension.

Proof :

By induction on n

Take $n = 1$. Then $F(\alpha_1)$ is a finite extension of F .

Assume the result for n elements.

Consider $F(\alpha_1, \dots, \alpha_{n+1})$

α_{n+1} is algebraic over F .

α_{n+1} is algebraic over $F(\alpha_1, \dots, \alpha_n)$

$F(\alpha_1, \dots, \alpha_{n+1})$ is a finite extension of $F(\alpha_1, \dots, \alpha_n)$

By induction hypothesis $F(\alpha_1, \dots, \alpha_n)$ is a finite extension of F .

now

$$[F(\alpha_1, \dots, \alpha_{n+1}):F] = [F(\alpha_1, \dots, \alpha_{n+1}):F(\alpha_1, \dots, \alpha_n)] \times [F(\alpha_1, \dots, \alpha_n):F]$$

$\therefore$ L.H.S is finite

This proves the result for $(n+1)$ elements

Hence the result follows.

Cor :

Let K/F be an extension, $\alpha, \beta \in K$ algebraic over F . Then $\alpha \pm \beta, \alpha\beta, \alpha^{-1}$ are all algebraic over F .

Proof :

Let $F(\alpha, \beta)$ be the smallest subfield of K containing F, α, β .

$F(\alpha)$ is the smallest subfield containing F and α .

Let $\deg \alpha$ over F be n .

$$\circ [F(\alpha):F] = n$$

Hence $F(\alpha)$ is a finite extension of F .

$\circ F(\alpha)$ is an algebraic extension of F .

If $\beta \in F(\alpha)$, $F(\alpha)$ is a field.

$$\circ \alpha + \beta, \alpha - \beta, \alpha\beta, \alpha^{-1} \in F(\alpha)$$

$\circ \alpha + \beta, \alpha - \beta, \alpha\beta, \alpha^{-1}$ are all algebraic over F .

Suppose $\beta \notin F(\alpha)$

$$F(\alpha) \subset F(\alpha, \beta)$$

$$F(\alpha)(\beta) = F(\alpha, \beta)$$

now β is algebraic over F .

But $F \subset F(\alpha)$

$\circ \beta$ is algebraic over $F(\alpha)$

$\circ [F(\alpha)(\beta):F(\alpha)]$ is finite

$$\circ [F(\alpha)(\beta):F] = [F(\alpha)(\beta):F(\alpha)][F(\alpha):F]$$

$\circ F(\alpha)(\beta)$ is a finite extension of F .

$\circ F(\alpha)(\beta)$ is an algebraic extension of F .

$\circ F(\alpha, \beta)$ is an algebraic extension of F .

But $F(\alpha, \beta)$ is a field.

$$\alpha + \beta, \alpha - \beta, \alpha\beta, \alpha^{-1} \in F(\alpha, \beta)$$

$\circ \alpha + \beta, \alpha - \beta, \alpha\beta, \alpha^{-1}$ are all algebraic over F .

Definition :

A field F is called algebraically closed if it has no proper algebraic extension ie if K/F is an algebraic extension of F then $K=F$.

Examples :

1) The field $\overline{Q}$ is algebraically closed, for let $\frac{K}{Q}$ be algebraic and $\alpha \in K$ then α is algebraic over $\overline{Q}$ and hence over Q . Hence $\alpha \in \overline{Q}$. ie) $K = \overline{Q}$

Definiton :

Let $\bar{F}$ be an extension $\bar{F}$ is called an algebraic closure of F if

- (i) $\bar{F}$ is algebraic.
- (ii) $\bar{F}$ is an algebraically closed field.

Examples :

- 1) $\bar{Q}$ is an algebraic closure of Q .
- 2) C is an algebraic closure of R , the field of real numbers as $C = R(i)$, $i = \sqrt{-1}$ is an algebraic extension of degree 2 over R and C is algebraically closed.

Thm :

Let $\frac{K}{F}$ and $\frac{L}{K}$ be algebraic extensions. Then $\frac{L}{F}$ an algebraic extension.

Proof :

$$T \in L.$$

Weclaim :

t is algebraic over F .

G.T L is algebraic over F . it satisfies some polynomial over K .

Let $g(x) = \beta_0 + \beta_1 x + \dots + \beta_m x^m$ be a polynomial satisfies by t . where $\beta_0, \beta_1, \dots, \beta_n \in K$.

K is an algebraic extension of F .

∴ Every element of K is algebraic over F .

∴ $\beta_0, \beta_1, \beta_2, \dots, \beta_m$ is algebraic over $F(\beta_0)$ is a finite extension of F .

β_1 is algebraic over $F \Rightarrow \beta_1$ algebraic over.

∴ $F(\beta_0)(\beta_1)$ is a finite extension of $F(\beta_0)$.

∴ $F(\beta_0\beta_1)$ is a finite extension of F .

Proceeding like this,

$F(\beta_0, \beta_1, \dots, \beta_m)$ is a finite extension of F . Let $M = F(\beta_0, \dots, \beta_n)$. M is a finite extension of F .

$$(M:F) = r$$

Now

t satisfies the polynomial

$$g(x) = \beta_0 + \beta_1 x + \dots + \beta_m x^m \text{ where } \beta_1, \dots, \beta_n \in M.$$

∴ f is algebraic over M .

∴ $M(t)$ is a finite extension of M .

$$(M(t):M) = s.$$

$$(M(t):F) = (M(t):M)(M:F)$$

$$= s.r$$

∴ $M(t)$ is a finite extension of F .

∴ t is algebraic over F .

∴ L is an algebraic extension of F .

This Proves the thm.

Exercises :

1) Find the degree of the following field extensions :

$$(i) \frac{Q(\sqrt[3]{2}, \sqrt{3})}{Q} \quad (ii) \frac{Q(\sqrt{2}, \sqrt{3}, \sqrt{5})}{Q}$$

2) Show that a finite extension of prime degree is a simple extension.

3) Show that an extension $\frac{K}{F}$ is algebraic iff every ring R with $F \subset R \subset K$ is a field.

Normal extensions :

Lemma :

Let $f(x) \in F[x]$ be an irreducible polynomial. Then there exists an extension $\frac{K}{F}$ which contains a root of $f(x)$.

Proof :

Since $f(x)$ is irreducible,

The ideal $I = (f(x))$ in $F[x]$ is a maximal ideal and

Hence $K = F[x]/I$ is a field.

The map $F \rightarrow K$ given by $a \rightarrow a+I$ is an isomorphism of F onto its image $F^1 \subset K$. Identifying F with $F^1 \subset K$ we can consider K as an extension of F .

We claim that $\alpha = x + I \in K$ is a root of $f(x)$.

This is so because

$$f(x) = f(x+I) = f(x) + I = \bar{0} \text{ as } f(x) \in I.$$

Cor :

Let $g(x) \in F[x]$ be any non-constant polynomial. Then there exists an extension K/F which contains a root of $g(x)$.

Proof :

Consider an irreducible factor $f(x)$ of $g(x)$ and take the extension K/F which contains a root α of $f(x)$.

Then α is also a root of $g(x)$.

It $g(x) \in F[x]$ is of degree n .

by lemma,

Let F be a field and let $f(x) \in F[x]$ be a polynomial of deg n . Then $f(x)$ has at most n roots in F . where a root of multiplicity K is counted K times.

It $g(x)$ can have at most n roots in any extension K/F , counting a root of multiplicity K , as K roots. We now show that there exists a field K/F which contains all the n roots of $f(x)$ and in fact we can obtain a smallest extension which contains all the n roots.

Definition :

Let $f(x) \in F[x]$ be of degree n . An extension K/F is called a splitting field of $f(x)$ if (i) K contains n roots $\alpha_1, \dots, \alpha_n$ of $f(x)$ and (ii) $K = F(\alpha_1, \alpha_2, \dots, \alpha_n)$.

Theorem :

Let $f(x) \in F[x]$ be of degree n . Then $f(x)$ has a splitting field.

Proof :

The Proof is by induction on n .

If $n = 1$,

$$f(x) = a_1x + a_0.$$

Then $\alpha = -a_0/a_1 \in F$ is a root of $f(x)$.

$$\therefore K = F.$$

Let $n > 1$.

Let $f_1(x)$ be an irreducible factor of $f(x)$.

$$\therefore L = F(\alpha_1) \text{ be an extension such that } f_1(\alpha_1) = 0.$$

$$\text{Then } f(\alpha_1) = 0$$

$$\text{Hence } f(x) = (x - \alpha_1) g(x)$$

$$\forall g(x) \in L[x].$$

$$\text{Since } \deg g(x) = n-1.$$

By induction, there exists K/L which contains $n-1$ roots $\alpha_2, \dots, \alpha_n$ of $g(x)$ such that $K = L(\alpha_2, \dots, \alpha_n)$.

Then $K = F(\alpha_1, \alpha_2, \dots, \alpha_n)$ is the required splitting field of $f(x)$.

Remark :

Let $f(x) \in F[x]$ and K/F a splitting field of $f(x)$ with roots $\alpha_1, \alpha_2, \dots, \alpha_n$.

$$\text{Then } f(x) = \prod_{i=1}^n (x - \alpha_i) \text{ over } K[x].$$

Examples :

1) $x^2 - 3 \in \mathbb{Q}[x]$ has splitting field $\mathbb{Q}(\sqrt{3})$.

2) $x^3 - 2 \in \mathbb{Q}[x]$ has splitting field $\mathbb{Q}(\omega, \sqrt[3]{2})$ where ω is a cube root of unity.

i.e.) $w = e^{2\pi/3}$

We now show that the splitting field is unique upto isomorphism.

Definition :

Let K/F and K^1/F be extension fields. An isomorphism $\sigma : K \rightarrow K^1$ of K onto K^1 is called an F -isomorphism if $\sigma|_F = \text{Id}$.

Lemma :

Let $\sigma : F \rightarrow F^1$ be an isomorphism of F onto F^1 , $f(x) \in F[x]$ an irreducible polynomial, $f(x) = \sum a_i x^i$, $\bar{f}(x) = \sum \bar{a}_i x^i$, $\bar{a}_i = \sigma(a_i)$, the image polynomial over $F^1[x]$. Let α, α^1 be respectively roots of $f(x)$ and $\bar{f}(x)$. Then σ can be extended to an isomorphism $\bar{\sigma} : F(\alpha) \rightarrow F^1(\alpha^1)$ such that $\bar{\sigma}|_F = \sigma$.

Proof :

Since σ is an isomorphism and $f(x) \in F[x]$ is irreducible.

∴ $\bar{f}(x) \in F^1[x]$ is also irreducible.

∴ σ can be extended to an isomorphism

$$\sigma_1 : F[x] \rightarrow F^1[x]$$

$$\text{Where } \sigma_1(\sum b_i x^i) = \sum \bar{b}_i x^i.$$

Then $\sigma_1(f(x)) = \bar{f}(x)$ and this induces an isomorphism of the quotient rings

$$\bar{\sigma}_1 : \frac{F[x]}{f(x)} \rightarrow \frac{F^1[x]}{\bar{f}(x)} \text{ with } \bar{\sigma}_1 : (x + f(x)) \mapsto (x + \bar{f}(x))$$

Since, for any root σ of $f(x)$,

$F(\alpha) \cong F[x]/(f(x))$ we have an isomorphism

$$\bar{\sigma} : F(\alpha) \rightarrow F^1(\alpha^1) \text{ clearly } \bar{\sigma}(\alpha) = \alpha^1 \text{ and } \bar{\sigma}|_F = \sigma.$$

Theorem :

Let $\sigma : F \rightarrow F^1$ be an isomorphism of F onto F^1 , $f(x) \in F[x]$, $f(x) = \sum a_i x^i$, $\bar{f}(x) = \sum \bar{a}_i x^i$, $\bar{a}_i = \sigma(a_i)$. Let K, K^1 be splitting fields of $f(x)$ and $\bar{f}(x)$ respectively. Then there exists an isomorphism $\bar{\sigma} : K \rightarrow K^1$ of K onto K^1 such that $\bar{\sigma}|_F = \sigma$.

Proof :

The proof is by induction on $n = \deg f$. If $n=0$ there is nothing to prove.

Assume $n \geq 1$.

Let $f_1(x)$ be an irreducible factor of $f(x)$, α a root of $f_1(x)$ and α^1 a root of $\sigma(f_1)$.
By lemma,

Let $\sigma : F \rightarrow F^1$ be an isomorphism of F onto F^1 , $f(x) \in F[x]$ an irreducible polynomial, $f(x) = \sum a_i x^i$, $\bar{f}(x) = \sum \bar{a}_i x^i$, $\bar{a}_i = \sigma(a_i)$, the image polynomial over $F^1[x]$. Let α, α^1 be respectively roots of $f(x)$ and $\bar{f}(x)$. Then σ can be extended to an isomorphism $\bar{\sigma} : F(\alpha) \rightarrow F^1(\alpha^1)$ such that $\bar{\sigma}/F = \sigma$.

σ can be extended to an isomorphism

$$\sigma_1 : F(\alpha) \rightarrow F^1(\alpha^1) \text{ with } \sigma_1/F = \sigma.$$

$$\text{Let } f(x) = (x - \alpha) g(x), g(x) \in F(\alpha)[x]$$

So that

$$\sigma(f(x)) = (x - \alpha^1) \sigma_1(g).$$

Then K (respectively K^1) is a splitting field of $g(x)$ over $F(x)$ (respectively $\sigma_1(g)$ over $F^1(\alpha^1)$).

By induction.

σ_1 can be extended to an isomorphism

$$\bar{\sigma} : K \rightarrow K^1 \text{ of } K \text{ onto } K^1.$$

$$\text{Clearly } \bar{\sigma}/F = \sigma_1/F = \sigma.$$

Definition :

An extension K/F is called normal extension if it is algebraic and for any irreducible polynomial $f(x) \in F[x]$ which has a root in K , $f(x)$ has all its roots in K .

Examples :

1) Let K/F be an extension of degree 2. Then it is normal. Let $\alpha \in K$ with minimum polynomial $f(x)$. Then $\deg f(x) \leq 2$ and it $\deg f(x) = 1$, $\alpha \in F$.

It $\deg f(x) = 2$, $f(x) = x^2 + ax + b$, $a, b \in F$. Then the other root β is $\alpha - a$ as the sum of the roots is $-a$.

Hence $\beta \in K$. ie) K/F is normal.

2). $Q(3\sqrt{2})/Q$ is not normal. $\alpha = 3\sqrt{2}$ has minimum polynomial $x^3-2 \in Q[x]$.

Whese roots are $\alpha_1=3\sqrt{2}$, $\alpha_2=\omega 3\sqrt{2}$, $\alpha_3=\omega^2 3\sqrt{2}$ now $\alpha_2, \alpha_3 \notin Q(3\sqrt{2})$. Hence $Q(3\sqrt{2})/Q$ is not normal.

Definition :

Two algebraic elements α and α^1 are said to be conjugate over F if there exists an F isomorphism $\sigma: F(\alpha) \rightarrow F(\alpha^1)$ with $\sigma(\alpha) = \alpha^1$

Theorem :

Two elements α and α^1 are conjugate over F iff they have the same minimum polynomial over F .

Proof :

Part I :

$\Rightarrow$ By hypothesis $\exists$ an isomorphism

$$\sigma : F(\alpha) \xrightarrow{\sim} F(\alpha^1) \text{ with } \sigma(\alpha) = \alpha^1.$$

Let
$$f(x) = a_0 + a_1x + \dots + a_{n-1}x^{n-1} + x^n$$

be the minimal polynomial of α over F .

Then
$$0 = a_0 + a_1\alpha + a_2\alpha^2 + \dots + a_{n-1}\alpha^{n-1} + \alpha^n.$$

$$\begin{aligned} \Rightarrow 0 &= \sigma(0) = \sigma(a_0 + a_1\alpha + \dots + \alpha^n) \\ &= \sigma(a_0) + \sigma(a_1)\sigma(\alpha) + \dots + \sigma(a_{n-1})\sigma(\alpha^{n-1}) + \sigma(\alpha^n) \\ &= a_0 + a_1\alpha^1 + a_2\alpha^2 + \dots + a_{n-1}\alpha^{n-1} + \alpha^n. \end{aligned}$$

$\Rightarrow \alpha^1$ is not root of $f(x)$. It $m(x)$ is the minimal polynomial of α^1 over F .

Then
$$f(\alpha^1) = 0 \Rightarrow m(x)/f(x)$$

Then $f(x)$ is irreducible over F

$\deg m(x) \geq 1$ and both $m(x)$, $f(x)$ are monic

It $f(x)$ is the minimum polynomial of α .

Then $\sigma(f(x)) = f(x)$ is the minimum polynomial of $\sigma(\alpha) = \alpha^1$.

The first half of the Thm is proved.

Part II :

$\Leftarrow$ Suppose α, α^1 have the same minimal polynomial $m(x)$ over F .

Then $m(x)$ is irreducible over F .

α is a root of $F[x]$ and α^1 is a root of $f(x)$.

∴ there exists an isomorphism

$\phi : F(x) \rightarrow f(\alpha^1)$ extending $\sigma : F \rightarrow \bar{F}$ where σ is the identity map on F and mapping α into α^1 .

This proves the second part of the Theorem.

Theorem:

Let $f(x) \in F[x]$ and K be a splitting field of $f(x)$. For any extension L/F and any F -isomorphism $\sigma : K \rightarrow L$, we have $\sigma(K) = K$.

Proof:

Let $\alpha_1, \alpha_2, \dots, \alpha_n$ be the roots of $f(x) \in K$.

So that $K = F(\alpha_1, \alpha_2, \dots, \alpha_n)$.

Let $\sigma : K \rightarrow L$ be an F -isomorphism.

Then $\sigma(\alpha_1), \sigma(\alpha_2), \dots, \sigma(\alpha_n)$ are also roots of $f(x)$. $\sigma(\alpha_1), \sigma(\alpha_2), \dots, \sigma(\alpha_n)$ must be the same as $\alpha_1, \alpha_2, \dots, \alpha_n$ in some order.

∴ σ permutes the roots $\alpha_1, \alpha_2, \dots, \alpha_n$.

Now,

$$\begin{aligned}\sigma(K) &= \sigma(F(\alpha_1, \alpha_2, \dots, \alpha_n)) \\ &= F(\sigma(\alpha_1), \sigma(\alpha_2), \dots, \sigma(\alpha_n)) \\ &= F(\alpha_1, \alpha_2, \dots, \alpha_n)\end{aligned}$$

$$\Rightarrow \sigma(K) = K$$

This proves the Thm.

Theorem :

Any splitting field of a polynomial over F is a normal extension of F . conversely, any finite normal extension over F is the splitting field of some polynomial over F .

Proof :

Let $f(x) \in F[x]$ and K/F be a splitting field of $f(x)$.

Let $\alpha_1, \alpha_2, \dots, \alpha_n$ be all the roots of $f(x)$.

$$\therefore K = F(\alpha_1, \alpha_2, \dots, \alpha_n)$$

Let $\beta \in K$ be any root of an irreducible polynomial $g(x) \in F[x]$.

• L is a splitting field of $g(x)$. $\forall \beta \in L$.

Let β^1 be another root of $g(x) \in L$.

Since β and β^1 have the same minimum polynomial $g(x)$ over F .

Then there exists an F -isomorphism

$\sigma : F(\beta) \rightarrow F(\beta^1)$ with $\sigma(\beta) = \beta^1$.

Since the splitting field of $f(x)$

(respectively $\sigma(f(x)) = f(x)$ over $F(\beta)$).

(respectively over $F(\beta^1)$ is $K = K(\beta) = F(\beta, \alpha_1, \dots, \alpha_n)$)

(respectively $K(\beta^1) = F(\beta^1, \alpha_1, \dots, \alpha_n)$)

σ can be extended to an F -isomorphism of $\bar{\sigma}$ of K onto $K(\beta^1)$

by Theorem,

Let $f(x) \in F[x]$ and K be a splitting field of $f(x)$.

For any extension L/F and any F -isomorphism $\sigma : K \rightarrow L$, we have $\sigma(K) = K$.

• $\bar{\sigma}(K) = K$.

• $\beta^1 = \bar{\sigma}(\beta) \in K$

This proves that K/F is normal.

Conversely,

Let K/F be a finite normal extension.

Then $K = F(\alpha_1, \dots, \alpha_n)$ for some $\alpha_i \in K$.

Let $f_i(x) \in F[x]$ be the minimal polynomial of α_i over F for each i .

Then each $f_i(x)$ is irreducible over F .

Each $f_i(x)$ has one root $\alpha = \alpha_i$.

Say in K and K is a normal extension of F .

$$f_i(x) = (x - \alpha_{i1})(x - \alpha_{i2}) \dots (x - \alpha_{iK_i}) \text{ for some } \alpha_{ij} \in K.$$

Consider

$$f(x) = f_1(x) f_2(x) \dots f_n(x)$$

Then

$$f(x) = \prod_{i,j} (x - \alpha_{ij}) \text{ and}$$

$$F(\alpha_{11}, \dots, \alpha_{1K_1}, \alpha_{21}, \dots, \alpha_{2K_2}, \dots, \alpha_{n1}, \dots, \alpha_{nK_n}) \subseteq K$$

(Since $\alpha_{ij} \in K \forall ij$) and on the other hand.

$$F(\alpha_{11}, \dots, \alpha_{1K_1}, \alpha_{21}, \dots, \alpha_{2K_2}, \dots, \alpha_{n1}, \dots, \alpha_{nK_n}) \supseteq$$

$$F(\alpha_{11}, \alpha_{21}, \dots, \alpha_{nK_n}) = F(\alpha_1, \alpha_2, \dots, \alpha_n) = K$$

$\therefore K = F(\{\alpha_{ij}\}/i,j)$ is a splitting field of the polynomial $f(x)$ over F .

This proves the thm.

Theorem :

Let F be a finite extension of K . Then $\exists N \supset F$ s.t N is normal extension of K .

Proof :

Let F be a finite extension of K .

$$F = K(\alpha_1, \dots, \alpha_m)$$

$\alpha_1, \dots, \alpha_m$ are algebraic over K .

Let $m_1(x), m_2(x), \dots, m_m(x)$ are minimal polynomial of $\alpha_1, \dots, \alpha_m$ respectively put

$$f(x) = m_1(x) \dots m_m(x)$$

Let N be the splitting field for $f(x)$ over F .

We already have $\alpha_1, \dots, \alpha_m \in F$.

$\therefore N$ is splitting field for $f(x)$ over K .

$\therefore N$ is normal extension of K .

Theorem :

Let $N_1, N_2, N_3, \dots, N_k$ be normal extension of a field K . Then a normal extension N of K and K - isomorphism $\sigma : N_i \rightarrow N$

Proof :

By the thm

Let N_i be a finite normal extension of K .

Each N_i is the splitting field of some polynomial f_i over K .

Put $f = \prod_{i=1}^k f_i$, $i = 1, 2, \dots, k$.

Let N be the splitting field of f over K .

Then N is a normal extension of K .

Since every root of f_i is also a root of f ,

$\therefore N$ contains the splitting field of f_i .

$i = 1, 2, \dots, k$

i.e.) we have a K - isomorphism.

$\sigma_i : N_i \rightarrow N$, $i = 1, 2, \dots, k$

This proves The Thm.

Exercises :

- Any two splitting fields of $f(x) \in F[x]$ are f -isomorphic.
- Let K_1/F , K_2/F be normal extension such that $K_1 \subset L$ and $K_2 \subset F$ for some field L . Show that $K_1 K_2$ is a normal extension of F .

Separable extension :

Definition :

Let $f(x) \in F[x]$ be an irreducible polynomial $f(x)$ is called a separable polynomial if all its roots in its splitting field are simple.

A polynomial $g(x) \in F[x]$ is called separable if all its irreducible factors are separable. A polynomial which is not separable is called an inseparable polynomial.

Exercises :

- $x^3 - 2 \in \mathbb{Q}[x]$ is a separable polynomial as its roots $2\sqrt[3]{2}, \omega 2\sqrt[3]{2}, \omega^2 2\sqrt[3]{2}$ are distinct, $\omega = e^{2\pi i/3}$

We show, infact, that over any field F of char $p > 0$, every irreducible polynomial is separable. We therefore, have to look for inseparable polynomials (irreducible) only over fields of char $p = 0$.

Theorem (i) :

Let $f(x) \in K[x]$ splitting field of $f(x)$ over K , Let α be a root $f(x) \in E$. Then α is a multiple root of $f(x)$ iff α is a root of $f'(x)$.

Proof :

Suppose α is a multiple root of $f(x)$.

$$f(x) = (x-\alpha)^2 g(x)$$

$$f'(x) = 2(x-\alpha)g(x) + (x-\alpha)^2 g'(x)$$

$$\circ \quad f'(\alpha) = 0.$$

$$\Rightarrow \alpha \text{ is a root of } f'(x)$$

Conversely,

Suppose α is a root of $f'(x)$. To prove that α is a multiple root of $f(x)$.

Claim :

$$(x-\alpha)^2/f(x)$$

$$f(x) = (x-\alpha)h(x)$$

$$\Rightarrow f'(x) = h(x) + (x-\alpha)h'(x)$$

$$\Rightarrow f'(x) = (x-\alpha)K[x].$$

$$(x-\alpha)K[x] = h(x) + (x-\alpha)h'(x)$$

$$\Rightarrow (x-\alpha)K[x] = h(x) + (x-\alpha)h'(x)$$

$$\Rightarrow (x-\alpha)K[x] - (x-\alpha)h'(x) = h(x)$$

$$\Rightarrow (x-\alpha)[K[x] - h'(x)] = h(x)$$

$$\circ \quad (x-\alpha)/h(x)$$

$$f(x) = (x-\alpha)h(x)$$

$$= (x-\alpha)(x-\alpha)h_1[x]$$

$$\Rightarrow f(x) = (x-\alpha)^2 h_1[x]$$

$\circ \quad \alpha$ is a multiple root of $f(x)$.

Theorem :

Let $p(x) \in K[x]$ be irreducible. Then $p(x)$ is inseparable iff $p'(x)=0$.

Proof :

Let $p(x) \in K[x]$ be irreducible. Suppose $p(x)$ is inseparable.

Let α be a multiple root of $p(x)$.

$$\begin{aligned} \circ \quad p(x) &= (x-\alpha)^2 q(x) \\ p'(x) &= 2(x-\alpha)q(x) + (x-\alpha)^2 q'(x) \\ &= (x-\alpha) [2q(x) + (x-\alpha)q'(x)] \end{aligned}$$

or

α is a root of $p'(x)$

But $p(x)$ is irreducible

$$\begin{aligned} \circ \quad p(x) &= cm(x) \\ \text{It} \quad f(\alpha) &= 0 \text{ then } m(x)/f(x) \end{aligned}$$

$$\circ \quad P(x)/p'(x) \quad (\deg p'(x) < \deg p(x))$$

$$\circ \quad p'(x) = 0,$$

Conversely,

To P.T $p(x)$ is inseparable.

$$\begin{aligned} \text{Since} \quad p'(x) &= 0 \\ &= (x-\alpha)/p'(x) \\ p(x) &= (x-\alpha)g(x) \\ p'(x) &= g(x) + (x-\alpha)g'(x) \\ \circ \quad (x-\alpha)/p'(x) \end{aligned}$$

$$\circ \quad (x-\alpha)/g(x)$$

$$p(x) = (x-\alpha)^2 g_1(x)$$

$p(x)$ is inseparable.

Hence the Thm.

Lemma : (i)

Let $\text{ch } F=0$ and $f(x) \in F[x]$ be a monic irreducible polynomial. Then $f(x)$ is separable.

Proof :

$$\text{Let} \quad f(x) = \sum_i a_i x^i \text{ be inseparable.}$$

Then
$$f'(x) = \sum_i a_i x^{i-1} = 0$$

by lemma,

Let $f(x) \in F[x]$ be a monic irreducible polynomial.

Then f has a multiple root iff $f' = 0$.

In particular,

$$ia_i = 0 \quad \forall i \geq 1$$

As
$$ch F = 0$$

$$a_i = 0, i \geq 1$$

∴
$$f(x) = a_0.$$

∴ a constant polynomial which is a contradiction as $f(x)$ is irreducible.

Hence $f(x)$ is separable.

Lemma : (ii)

Let $f(x) \in K[x]$ be irreducible. Then $f(x)$ is inseparable iff $\exists$ a polynomial $g(x) \in K[x]$ s.t $f(x) = g(x^p)$.

Proof :

$f(x)$ is inseparable. So it has a multiple root.

∴
$$f' = 0.$$

If
$$f(x) = \sum_{i=0}^n a_i x^i$$

$$f'(x) = \sum_{i=1}^n a_i x^{i-1}$$

∴
$$f' \equiv 0 \Rightarrow ia_i = 0 \quad \forall i = 1, \dots, n.$$

p is the characteristic of K . (smallest $(+ve)$ integer s.t $p \cdot a = 0, a \in K$)

So
$$ia_i = 0 \Rightarrow p/i \text{ Whenever } a_i \neq 0$$

$$p/i \Rightarrow i = p \cdot n_i$$

∴
$$f(x) = \sum a_i x^{p n_i}$$

(a_i are non-zero coefficients)

∴
$$f(x) = \sum a_i (x^p)^{n_i}$$

Take $g(x) = \sum a_i y^{ni}$.

Then $f(x) = g(x^p)$.

Suppose $f(x) = g(x^p)$.

To S.T is a multiple root of $f(x)$.

$$f'(x) = g'(x^p) p x^{p-1}$$

∴ p is a char of K .

$$\therefore f'(x) = 0.$$

⇒ α is a multiple root.

∴ $f(x)$ is inseparable

Hence the lemma.

Definition :

Let K/F be an extension $\alpha \in K$ is called separable over F if it is algebraic and its minimum polynomial over F is a separable polynomial.

Otherwise α is called inseparable.

Definition:

An extension K/F is called separable if it is algebraic and every $\alpha \in K$ is separable over F .

Examples :

1) Let $\text{Ch } F = p > 0$, $f(x) = x^p - a \in F[x]$ with no root in F . Then $f(x)$ is an inseparable polynomial. Let α_1, α_2 be two roots of $f(x)$ in some extension field.

$$\text{Then } \alpha_1^p = a = \alpha_2^p.$$

Now $(\alpha_1 - \alpha_2)^p = \alpha_1^p - \alpha_2^p$ as all the other terms in the binomial expansion are zero, the coefficients being divisible by p .

$$\text{Hence } (\alpha_1 - \alpha_2)^p = \alpha_1^p - \alpha_2^p = a - a = 0$$

$$\therefore \alpha_1 = \alpha_2$$

Thus, all the roots of $f(x)$ are the same and there is only one root α of $f(x)$ with multiplicity p .

We claim that $f(x)$ is irreducible over F .

Let $g(x)$ be an irreducible factor of $f(x)$.

$$\circledast \quad g(\alpha) = 0$$

$\circledast$ $g(x)$ is the minimum polynomial of α .

Thus the only irreducible factor of $f(x)$ is the minimum polynomial $g(x)$ of α .

$$\circledast \quad f = g^m.$$

In particular,

$$\deg f = p = m \deg g.$$

$$\circledast \deg g/p.$$

But $\deg g > 1$.

As $f(x)$ has not root in F .

Hence $m = 1$.

$\circledast$ $f = g$ is irreducible.

Definition :

F is called a perfect field if every algebraic extension K/F is separable.

Theorem :

Let $\text{ch } F = P > 0$. Then (i) F is perfect iff (ii) every element of F has a p -th root in F . i.e.) for every $a \in F$, There exists $b \in F$ with $b^p = a$.

Proof :

Part I :

(i) $\Rightarrow$ (ii)

Assuming as hypothesis that every algebraic extension field F is a separable extension of F .

We have to prove (ii).

Let $a \in F$. We want to prove that a has atleast one p^{th} root in F .

Suppose the contrary that a has no p^{th} root in F .

By example (i),

The polynomial $f(x) = x^p - a$ is irreducible over F .

If we adjoin one root α of $f(x)$ to F .

$$\circledast f(\alpha) = F[\alpha]$$

We have $x^p - a$ has repeated roots in $F(\alpha)$.

∴ $F(\alpha)$ is an inseparable extension of F , a contradiction to our hypothesis that every algebraic extension of F is a separable extension.

This contradiction proves that (i) $\Rightarrow$ (ii).

Part II :

To prove (ii) $\Rightarrow$ (i).

Our hyp (ii) now is that every element of F has at least one p^{th} root in F . To prove that F is a perfect field .

i.e.) That is every algebraic extension at F is a separable extension.

Suppose the contrary that F has an (algebraic) inseparable extension K .

Then K contains an inseparable elements α which means that the minimal polynomial $f(x)$, say α over F has repeated roots in some extension of F .

Then by lemma (ii) to thm (i).

We have

$$f(x) = g(x^p) = a_0 + a_1 x^p + a_2 x^{2p} + \dots + a_k x^{kp}$$

for some $a_k \in F$ and it irreducible over F .

Now $a_i \in F$ and

It $b_i \in F$ such that $a_i = b_i^p \quad \forall i = 0, 1, \dots, k$.

$$\begin{aligned} \Rightarrow f(x) &= b_0^p + b_1^p x^p + \dots + b_k^p x^{kp} \\ &= (b_0 + b_1 x + \dots + b_k x^k)^p \\ &= (h(x))^p \end{aligned}$$

Where $h(x) = b_0 + b_1 x + \dots + b_k x^k \in F[x]$.

$$\Rightarrow f(x) = (h(x))^p$$

contradicts the fact that $f(x)$ is irreducible over F .

Hence any element algebraic over F is separable.

∴ F is perfect

This proves that (ii) $\Rightarrow$ (i)

Cor :

Any finite field F is perfect.

Proof :

Let F be any finite field.

So that its characteristic is $p > 0$.

Consider the mapping $\phi : F \rightarrow F$ given by

$$\phi(x) = x^p, \forall x \in F.$$

Then

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

$$\Rightarrow x^p = y^p$$

$$\Rightarrow x^p - y^p = 0$$

$$\Rightarrow (x-y)^p = x^p - y^p = 0$$

$$\Rightarrow x = y.$$

Hence $\phi : F \rightarrow F$ is 1-1 map and F is finite.

$\therefore \phi : F \rightarrow F$ is an onto map.

$\therefore$ For each $a \in F$.

There exists a unique element $b \in F$ such that $a = b^p$.

by the above thm

$\therefore F$ is a perfect field.

Cor :

Any algebraically closed field F is perfect.

Proof :

If $\text{ch } F = 0$.

$\therefore F$ is perfect.

It $\text{ch } F = p > 0$, and $a \in F$,

$x^p - a \in F[x]$ has a root in F .

As F is algebraically closed.

Thus every $a \in F$ has p^{th} root in F .

$\therefore F$ is perfect.

We now give an alternative criterion for the separability of K/F in terms of the F -automorphisms of K .

Theorem :

Let K/F and L/K be finite extension and N/F a finite normal extension. $L \subset N$. If m is the number of F - isomorphism of K in N and n is the number of K - isomorphism of L in N , the number of F - isomorphisms of L in N is mn .

Proof :

Let $\sigma_1, \sigma_2, \dots, \sigma_m$ be the set of distinct F - isomorphisms of K into N .

Let $\ell_1, \ell_2, \dots, \ell_n$ be the set of distinct K - isomorphisms of L into N .

$\sigma_i : K \rightarrow N$ is a F - isomorphisms of an intermediate field.

$\exists$ an automorphism $\bar{\sigma}_i$ of N into N s.t $\bar{\sigma}_i$ extends σ_i .

$\forall$ pair i, j

$\bar{\sigma}_i \cdot \ell_j : L \rightarrow N$ is a F - isomorphism.

Claim :

$\left\{ \bar{\sigma}_i \ell_j \mid \begin{matrix} 1 \leq i \leq m \\ 1 \leq j \leq n \end{matrix} \right\}$ is a set of distinct F - isomorphism of L into N .

Suppose $\bar{\sigma}_i \ell_j = \bar{\sigma}_r \ell_s$.

By induction $\forall x \in L$.

$$\bar{\sigma}_i \ell_j(x) = \bar{\sigma}_r \ell_s(x)$$

$$\bar{\sigma}_i(\ell_j(x)) = \bar{\sigma}_r(\ell_s(x)) \quad \forall x \in K.$$

$$\bar{\sigma}_i(x) = \bar{\sigma}_r(x)$$

$$\bar{\sigma}_i = \bar{\sigma}_r \Rightarrow i = r.$$

$$\bar{\sigma}_i \ell_j = \bar{\sigma}_i \ell_s$$

$$(\bar{\sigma}_i)^{-1}(\bar{\sigma}_i \ell_j) = (\bar{\sigma}_i)^{-1}(\bar{\sigma}_i \ell_s)$$

$$\ell_j = \ell_s \Rightarrow j = s$$

$\therefore$ The claim follows.

Let $\theta : L \rightarrow N$ be a F - isomorphism.

$\therefore (\theta/K)$ is a F - isomorphism of K into N .

$\therefore (\theta/K) = \bar{\sigma}_i$ for some i .

Consider $(\bar{\sigma}_i)^{-1} \circ \theta$ is a F - isomorphism of L into N .

Let $x \in K$.

$$\begin{aligned} (\bar{\sigma}_i)^{-1} \circ \theta(x) &= (\bar{\sigma}_i)^{-1}(\theta(x)) \\ &= (\bar{\sigma}_i)^{-1}(\sigma_i(x)) \\ &= (\bar{\sigma}_i)^{-1}(\bar{\sigma}_i(x)) \\ &= x. \end{aligned}$$

∴ $(\bar{\sigma}_i)^{-1} \circ \theta$ is an isomorphism of L into N .

∴ $\bar{\sigma}_i^{-1} \circ \theta = \ell_j$ for some j

∴ $\theta = \bar{\sigma}_i \circ \ell_j$

$\{\bar{\sigma}_i \circ \ell_j\}$ is the set of all F - isomorphism of L into N .

∴ The number of F - isomorphisms of L into N is mn .

Hence The Thm.

Theorem :

Let K be a finite extension of F . and N/F a finite normal extension, $K \subset N$. Then the number of F - isomorphisms of K in N is $\leq [K:F]$.

Proof :

Let $[K:F] = n$.

Proof by induction on n .

Suppose $n = 1$. Then $K = F$.

Then the number F - isomorphism of F into N is $1 = [F:F]$.

The result holds for $n=1$.

Assume now that the result holds for extensions of degree $< n$.

Let $[K:F] = n > 1$.

Choose and $\alpha \in K/F$.

Now $K \subset F(\alpha) \subseteq K$

Let $m = [F(\alpha):F] =$ The degree of α over F .

$=$ The degree of the minimal polynomial $m(x)$ of α .

$\deg m(x) = [F(\alpha):F] \leq [K:F]$

Since N is a normal extension of F , $m(x)$ is an irreducible polynomial and one root α of $m(x)$ is in N .

◦ $m(x)$ splits completely into linear factors in $N[x]$.

Let $\alpha_1, \alpha_2 \dots \alpha_r$ be the distinct roots of $m(x) \in N$.

◦ $r \leq m$.

◦ $\forall i, \exists \sigma_i$ an F -isomorphism of $F(\alpha)$ to $F(\alpha_i)$

◦ We have r distinct F -isomorphisms σ_i of $F(\alpha)$ into N .

It $s: F(\alpha) \rightarrow N$ is a F -isomorphism.

$s(\alpha)$ is a root of $m(x)$.

◦ $s(\alpha) = \alpha_i$

◦ $s = \sigma_i$

The number of distinct F -isomorphism of $F(\alpha)$ into $N = r \leq m = [F(\alpha):F]$

$[K:F(\alpha)] < n$.

By induction hypothesis,

The number of distinct $F(\alpha)$ isomorphism of K into $N \leq [K:F(\alpha)]$.

By the Lemma,

The number of distinct F -isomorphism of K into N .

$= r$ (the number of distinct $F(\alpha)$ isomorphism of K into N)

$\leq [F(\alpha):F] [K:F(\alpha)]$

$\leq [K:F]$

◦ The result holds for n .

By induction the thm follows.

Theorem :

Let K/F be a finite extension. Then K/F is separable $\Leftrightarrow$ the number of F -isomorphisms of K in N , for any finite normal extension N/F , $K \subset N$ is equal to $[K:F]$.

Proof :

Suppose K is a separable extension of F . Let N be a finite extension of K . s.t N is a normal extension of F . We prove by induction on n .

Suppose $n = 1$.

Then $K=F$ and so the result is trivial. Assume the result for extensions of degree $< n$.

Let $[K:F] = n > 1$.

Choose an element $\alpha \in K/F$.

Then $[K:F(\alpha)] < n$.

By the lemma,

K is a separable extension of $F(\alpha)$. By induction hypothesis, the number of distinct $F(\alpha)$ - isomorphism of K into $N = [K:F(\alpha)]$.

$\alpha \in K$ is separable over F .

Let $\deg \alpha = m$

Let $m(x)$ be the minimal polynomial of α over F .

$$[F(\alpha):F] = \deg m(x) = m.$$

$\alpha \in N$, $m(x)$ is an irreducible polynomial. N is a normal extension of F .

$\therefore m(x)$ splits into linear factors in N .

$\exists$ roots $\alpha_1, \alpha_2, \dots, \alpha_m$ of $m(x)$ in N .

$\forall i$, a F - isomorphism of $F(\alpha)$ to $F(\alpha_i)$

$\therefore \exists m$ F - isomorphism of $F(\alpha)$ into N .

But the number of F - isomorphism of $F(\alpha)$ into N is $\leq [F(\alpha):F]$.

The number of distinct F - isomorphism of $F(\alpha)$ into N is $m = [F(\alpha):F]$.

The number of F - isomorphism of K into $n = [K:F(\alpha)][F(\alpha):F]$

$$= [K:F]$$

The result holds for n .

Hence by induction, the result holds converse of the thm,

Suppose $n = [K:F]$ and there are n distinct F - isomorphisms into N .

To P.T

K is separable.

Let $\alpha \in K$.

To P.T

α is separable

$$\begin{aligned} n &= \text{The number of distinct } F\text{-isomorphism of } K \text{ into } N. \\ &= (\text{The number of distinct } F\text{-isomorphism of } F(\alpha) \text{ into } N) \times (\text{The number of distinct } F(\alpha)\text{-isomorphism of } K \text{ into } N). \\ &\leq [F(\alpha):F] \times [K:F(\alpha)] \\ &= [K:F] = n. \end{aligned}$$

The number of distinct F -isomorphisms of $F(\alpha)$ into $N = [F(\alpha):F]$

i.e.), all the conjugates at α are distinct.

∴ α is separable.

∴ K is separable.

∴ The Theorem follows.

Cor :

Let K/F and L/K be finite separable extensions. Then L/F is separable.

Proof :

Let $[L:K] = m$, $[K:F] = n$.

As $[K:F] = n$ and K/F is separable. The number of F -isomorphisms of K into a finite normal extension N of F . Such that $N \supseteq L$ is n .

And the number of K -isomorphism of L into N is m .

∴ The number of F -isomorphism of L into N is $mn = [L:K][K:F] = [L:F]$ and This $\Rightarrow$ that L is a separable extension of F .

Hence the proof.

Cor :

Let K/F be an extension $\alpha_1, \alpha_2, \dots, \alpha_n \in K$ separable over F . Then $F(\alpha_1, \dots, \alpha_n)/F$ is a separable extension.

Proof :

The proof is by induction on n . Let N/F be any finite normal extension.

If $n = 1$.

The number of F - isomorphism of $F(\alpha_1)$ in N is $[F(\alpha_1):F]$ as α_1 is separable.

Hence $F(\alpha_1)/F$ is separable.

By induction.

$F(\alpha_1, \dots, \alpha_{n-1})/F$ is separable.

Since α_n is separable over F .

∴ It is separable over $F(\alpha_1, \dots, \alpha_{n-1})$

∴ $F(\alpha_1, \alpha_2, \dots, \alpha_n)/F(\alpha_1, \dots, \alpha_{n-1})$ is separable.

Hence $F(\alpha_1, \dots, \alpha_n)/F$ is separable.

Thm :

Let K/F be a finite separable extension, Then $K = F(\alpha)$ for some element $\alpha \in K$.

Proof :

Let K be a finite separable extension of a field f .

Let $[K:F] = n$.

Let N be a finite normal extension of F s.t $K \subset N$.

By the Thm,

∃ exactly n distinct F - isomorphism $\sigma_1, \dots, \sigma_n$ of K into N . without loss generality.

$$\sigma_1 = \text{id}.$$

If $i \neq j, \sigma_i \neq \sigma_j$.

ie, $\exists X \in K$ s.t $\sigma_i(X) \neq \sigma_j(X)$.

$$\forall a \in F, \sigma_i(a) = \sigma_j(a) = a.$$

$$\text{Put } v_{ij} = \{x \in K \mid \sigma_i(x) = \sigma_j(x)\}$$

$$F \subset v_{ij}.$$

∴ v_{ij} is a vectorspace.

∴ v_{ij} is a proper subspace of K .

Case (i) :

Suppose F is an infinite field.

$$\circ K \neq \bigcup_{ij} v_{ij}.$$

$$\circ \exists \alpha \in K \setminus \bigcup_{ij} v_{ij}.$$

If $i \neq j, \alpha \notin v_{ij}.$

$$\circ \sigma_i(\alpha) \neq \sigma_j(\alpha)$$

$$\sigma_1(\alpha) = \alpha, \sigma_2(\alpha) \dots \sigma_n(\alpha) \text{ are all distinct.}$$

If $m(x)$ is the minimal polynomial of $\alpha, \sigma_1(\alpha), \dots, \sigma_n(\alpha)$ are all roots of $m(x)$.

$$\deg m(x) \geq n.$$

$$\text{But } [K:F] = n \deg \alpha \leq n.$$

$$\circ \deg \alpha = \deg m(x) = n.$$

$$\circ [F(\alpha):F] = n.$$

$$\Rightarrow [K:F] = n.$$

$$\circ K = F(\alpha)$$

Case (ii) :

F is a finite field.

$$[K:F] = n.$$

$\circ K$ is a finite field.

$\{K/\{0\}, \cdot\}$ is a cyclic group generated by α say

$$\circ F(\alpha) = K.$$

Hence the theorem.

Exercises :

- 1) Let $x^p - a \in F[x]$, where $p = \text{char } F$. Then $x^p - a$ is irreducible over F or $x^p - a$ is a p^{th} - power of a linear polynomial in F .
- 2) Let $f \in K[x]$. Then the roots of f are simple iff f & f' are relatively prime.

GALOIS EXTENSION

Definition :

A finite extension K/F is called a Galois extension if it is normal and separable.

Lemma :

Let K/F be a Galois extension. The set of all F -automorphism of K is a group for composition.

Proof :

The identity is an F -automorphism of K , and so is an element of $G(K/F)$.

Let $\sigma, \ell \in G(K/F)$.

Then their composite σ, ℓ is also an F -automorphism of K .

$\therefore \sigma, \ell \in G(K/F)$.

Let $\sigma \in G(K/F)$. Then $\sigma: K \rightarrow K$ is 1-1 and onto

$\Rightarrow \sigma^{-1}$ exists and is both 1-1 and onto.

If $x, y \in K$.

$$\therefore \sigma^{-1}(xy) = \sigma^{-1}(x)\sigma^{-1}(y)$$

$$\text{Let } x_1 = \sigma^{-1}(x), y_1 = \sigma^{-1}(y)$$

$$\Rightarrow x = \sigma(x_1), y = \sigma(y_1)$$

$$\therefore xy = \sigma(x_1)\sigma(y_1)$$

$$\Rightarrow xy = \sigma(x_1 y_1)$$

$$\Rightarrow \sigma^{-1}(xy) = x_1 y_1 \Rightarrow \sigma^{-1}(x)\sigma^{-1}(y)$$

Hence $\sigma^{-1}: K \rightarrow K$ is an F -automorphism

$$\therefore \sigma^{-1} \in G(K/F)$$

This proves that $G(K/F)$ is a group under the operation of composition of maps.

Definition :

The group of all F -automorphisms of K onto K is denoted by $G(K/F)$ is called the Galois group of the extension K/F .

Example :

1) Let $F = Q(\sqrt{m})$ where m is a square free integer.

$F = Q(\sqrt{m}) = \{a+b\sqrt{m} \mid a, b \in Q\}$. Then F/Q is a finite normal, separable extension of Q .

∴ $\text{Ch of } Q = 0 \Rightarrow F/Q \text{ is separable and } [F:Q]=2 \Rightarrow F/Q \text{ is normal.}$

So that F/Q is a Galois extension of Q .

If $\sigma(a+b\sqrt{m}) = a-b\sqrt{m} \quad \forall a, b \in Q$.

Then σ is a Q -automorphism of F and we assert that $F/Q = \{\text{Id}, \sigma\}$.

Example :

If $F = Q(\sqrt[3]{2})$ then F is a finite, separable extension of Q but not a normal extension of Q .

Hence F/Q is not a Galois extension.

Definition :

Let S be a set of automorphisms of a field K and let $F = \{x \in K \mid \sigma(x) = x \quad \forall \sigma \in S\}$. Then F is subfield of K . (Proved below) and F is called the fixed field of S .

To prove that F is a subfield of K .

As $\sigma(O_K) = O_K$ and $\sigma(I_K) = I_K \quad \forall \sigma \in S$.

We see that $O_K, I_K \in F$.

Suppose $a, b \in F$ so that $\sigma(a)=a, \sigma(b)=b \quad \forall \sigma \in S$.

Then $\sigma(a-b) = \sigma(a)-\sigma(b) = a-b, \quad \forall \sigma \in S$

$\Rightarrow a-b \in F$.

$\sigma(ab) = \sigma(a) \cdot \sigma(b) = ab \quad \forall \sigma \in S$

$\Rightarrow ab \in F$

If $a \neq 0$

Then $\sigma(a)^{-1} = (\sigma(a))^{-1} = (a)^{-1}, \quad \forall \sigma \in S$

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

These together prove that F is a subfield of K .

Theorem 1 :

Let K/F be a Galois extension of degree n . Then $G(K/F)$ is a group of order n and F is the fixed field of $G(K/F)$.

$$\text{i.e.) } F = \{x \in K / \sigma(x) = x, \sigma \in G(K/F)\}$$

Proof : Step (i)

If K/F is a separable extension and N is a finite, normal extension of F with $N \supseteq K$.

By theorem

Let K/F be a finite extension. Then K is a separable extension of F iff the number of distinct F -isomorphism of K into any first normal extension N of F (with $N \supseteq K$) is precisely $[K:F]$.

The no. of F -isomorphisms of K into N equals $[K:F]$.

As K/F is a Galois extension we have K/F is a normal extension.

On taking $N=K$ the no. of F -isomorphisms of K into $K=[K:F]$.

As K is a finite dimensional vector space over F .

If $\sigma \in G(K/F)$, $\sigma: K \rightarrow K$ is 1-1 $\Rightarrow \sigma$ is onto.

$$\begin{aligned} \text{Let } [K:F] &= \text{the no. of } F\text{-isomorphisms of } K \text{ onto } K. \\ &= \text{the no. of } F\text{-isomorphisms of } K. \\ &= O((G/F)). \end{aligned}$$

Hence we have $O((G/F)) = [K:F] = n$.

This proves the first assertion in the theorem.

Step (ii) :

To prove that the fixed field of $G(K/F)$ is F .

Let $G = G(K/F)$

Let L be the fixed field of G .

Now

$$x \in F \Rightarrow \sigma(x) = x, \forall x \in G \Rightarrow x \in \text{fixed field of } G = L.$$

Hence $F \subseteq L$.

We want to prove that $F=L$.

Suppose the contrary that $F \subsetneq L$.

So that there exists an element $\alpha \in L$.

with $\alpha \notin F$

Let $m(x)$ be the minimal polynomial of α over F .

Then $m(x)$ is irreducible over F and has one root α in K .

Where K is a normal extension of F .

So $m(x)$ splits into linear factors over F .

$\sigma \notin F$ $[F(\alpha):F] \geq 2$

$\Rightarrow \deg m(x) \geq 2$.

$\therefore K$ is a separable extension of F .

$\Rightarrow m(x)$ has only simple roots in K .

(and $\deg m(x) \geq 2 \Rightarrow m(x)$ has atleast one root $\beta \in K$ such that $\beta \neq \alpha$)

There exists an F -isomorphism $\sigma: F(\alpha) \rightarrow F(\beta)$ with $\sigma(\alpha) = \beta$. (by definition two algebraic elements α and α' are said to be conjugate over F if there exists an F -isomorphism

$\sigma: F(\alpha) \rightarrow F(\alpha')$ with $\sigma(\alpha) = \alpha'$)

K/F is a normal extension and $F \subseteq F(\alpha) \subseteq K$,

$F \subseteq F(\beta) \subseteq K \Rightarrow K$ is a normal extension $F(\alpha)$,

So K is a splitting field over $F(\alpha)$ of some polynomial $f(x)$ over $F(x)$

and So K is a splitting field of $f(x)$ over F .

Hence there exists an F -isomorphism

$\bar{\sigma}$ of K onto K extending σ .

So that $\bar{\sigma}(\alpha) = \sigma(\alpha) = \beta$.

now $\bar{\sigma} \in G(K/F)$ and $\bar{\sigma}(\alpha) = \beta \neq \alpha$

$\Rightarrow \alpha$ doesnot belong to the fixed field L of G .

This contradiction to our choice of $\alpha \in L$, $\alpha \notin F$ and this contradiction proves that $L=F$.

$\therefore$ that the fixed of G is F itself.

This proves the theorem.

The following theorem is a converse of theorem 1.

Theorem (2) : (Artin's theorem)

Let G be a finite group of automorphisms of K and F the fixed field of G .

i.e.) $F = \{x \in K / \sigma(x) = x, \forall \sigma \in G\}$

then K/F is a Galois extension with $G(K/F) = G$.

Proof :

Let $G = \{\sigma_1, \sigma_2, \dots, \sigma_n\}$ with $\sigma_i \neq \sigma_j$ if $i \neq j$ and $\sigma = \text{Id}_K$.

Step (i) :

To prove that K/F is a Galois extension.

Let α be any element of K .

Consider the elements $\{\alpha = \sigma_1(\alpha), \sigma_2(\alpha), \dots, \sigma_n(\alpha)\}$.

These need not all be distinct. Suppose that $\beta_1, \beta_2, \dots, \beta_m$ are all the distinct members of this set. $\forall i$ with $1 \leq i \leq n$.

$\sigma_i(\alpha)$ equals β_j for one and only one β_j .

Let $\sigma \in G$.

Then $\sigma(\beta_1), \sigma(\beta_2), \dots, \sigma(\beta_m)$ are distinct and they are the same as $\beta_1, \beta_2, \dots, \beta_m$ in some possibly different order.

$$\therefore \{\sigma(\beta_1), \dots, \sigma(\beta_m)\} = \{\sigma\sigma_1(\alpha), \dots, \sigma\sigma_n(\alpha)\}$$

and as

$$\begin{aligned} G &= \{\sigma\sigma_1, \sigma\sigma_2, \dots, \sigma\sigma_n\} \\ &= \{\sigma_1, \sigma_2, \dots, \sigma_n\} \end{aligned}$$

We have

$$\begin{aligned} \{\sigma(\beta_1), \dots, \sigma(\beta_m)\} &= \{\sigma\sigma_1(\alpha), \sigma\sigma_2(\alpha), \dots, \sigma\sigma_n(\alpha)\} \\ &= \{\sigma_1(\alpha), \dots, \sigma_n(\alpha)\} \\ &= \{\beta_1, \dots, \beta_m\} \end{aligned}$$

If

$$f(x) = \prod_{j=1}^m (x - \beta_j)$$

Then

$$\sigma(f(x)) = \prod_{j=1}^m (x - \sigma(\beta_j))$$

$$= \prod_{j=1}^m (x - \beta_j)$$

$$\Rightarrow \sigma(f(x)) = f(x)$$

$$\circ \sigma(f(x)) = f(x) \quad \forall \sigma \in G$$

$$\text{As } \beta_1, \beta_2, \dots, \beta_m \in K$$

$$\circ f(x) \in K(x)$$

$$\circ f(x) = x^m + a_1 x^{m-1} + \dots + a_m$$

for some $a_i \in K$

As

$$\sigma(f(x)) = f(x)$$

We have

$$\sigma(a_i) = a_i \quad \forall \sigma \in G$$

$$\Rightarrow a_i \in \text{fixed field of } G = F \quad \forall i$$

$$\circ f(x) \in F[x].$$

So

$\alpha \in K \Rightarrow \alpha$ satisfies a polynomial $f(x)$ of degree $m \leq n = O(G)$ over F .

Where $f(x)$ has distinct roots.

Claim (i) :

$f(x)$ is the minimal polynomial of α over F .

Let $m(x)$ be the minimal polynomial of α over F .

Then $m(x)/f(x)$, and $m(\alpha)=0$

$$\begin{aligned} \Rightarrow 0 &= 0 \sigma(m(\alpha)) \\ &= m(\sigma(\alpha)) \\ &= m(\beta_j) = \beta_j \text{ is a root of } m(x) \end{aligned}$$

$$\forall j = 1, 2, \dots, m$$

$$\Rightarrow f(x) = \prod_{j=1}^m (x - \beta_j) / m(x)$$

As $m(x)/f(x)$, $f(x)/m(x)$

and with $m(x)$, $f(x)$ are monic.

We get

$$f(x) = m(x)$$

Hence claim (i).

$f(x)$ has distinct roots $\Rightarrow m(x)$ has distinct roots.

$\Rightarrow \alpha \in K$ is separable over F .

This is true for every element α of K .

So that,

K is an algebraic extension of F and K is a separable extension F . ----- (1)

Also

$$\alpha \in K \Rightarrow [F(\alpha):F] = \deg m(x) = m \leq O(G) \text{ ----- (2)}$$

As $O(G)$ is finite, there is an element $\beta \in K$ such that $[F(\beta):F]$ is the largest among the integers $\{[F(\alpha):F] : \alpha \in K\}$.

Claim (ii) :

$$K = F(\beta)$$

Let $\alpha \in K$. Then as K is a separable extension of F .

We have $F(\alpha, \beta) = F(\gamma)$
for some $\gamma \in F(\alpha, \beta) \subseteq K$.

And

$$\begin{aligned} [F(\gamma):F] &= [F(\gamma):F(\beta)] \cdot [F(\beta):F] \\ &\leq [F(\beta):F] \end{aligned}$$

$$\text{By our choice of } \beta \Rightarrow [F(\gamma):F(\beta)] \leq 1$$

$$\Rightarrow [F(\gamma):F(\beta)] = 1$$

and

$$F(\beta) \subseteq F(\gamma)$$

This

$$\Rightarrow F(\beta) = F(\gamma)$$

$$\Rightarrow \gamma \in F(\beta) \text{ so that } F(\alpha, \beta) = F(\gamma) = F(\beta)$$

$$\Rightarrow \alpha \in F$$

$$(\alpha, \beta) = F(\beta)$$

$$\text{Thus } \alpha \in K \Rightarrow \alpha \in F(\beta) \Rightarrow K \subseteq F(\beta).$$

$$\text{But } F(\beta) \subseteq K$$

$$\text{and so } K = F(\beta)$$

This shows that K is a finite extension of F .

Claim (iii) :

K/N is a normal extension.

$$\text{Let } g(x) = \prod_{i=1}^n (x - \sigma_i(\beta))$$

where $G = \{\sigma_1, \sigma_2, \dots, \sigma_n\}$ is a group with n elements with $\sigma_1 = \text{Id}_K$.

So that

$$\sigma(\beta) = \beta$$

$$\text{now } \sigma_i(\beta) \in K \quad \forall i.$$

Arguing as before

$$\sigma(g(x)) = g(x) \quad \forall \sigma \in G.$$

So that

$$g(x) \in F[x]$$

So that $g(x)$ has all its roots $\{\sigma_1(\beta), \sigma_2(\beta), \dots, \sigma_n(\beta)\}$ in K .

$$\text{As } K \supseteq F(\sigma_1(\beta), \dots, \sigma_n(\beta)) \supseteq F(\sigma_1(\beta)) = F(\beta) = K$$

We have

$K = F(\sigma_1(\beta), \sigma_2(\beta), \dots, \sigma_n(\beta))$ is a splitting field of some polynomial $g(x)$ over F .

Hence K is a normal extension of F .

Thus we have proved that K/F is a finite separable and normal extensions.

∴ that is a Galois extension.

Subclaim (iv) :

$g(x)$ is the minimal polynomial of β over F .

Let $h(x)$ be the minimal polynomial of β over F .

So that $h(x) = [f(\beta):F]$

Then arguing as in claim (i), we get that $g(x)$ is the minimal polynomial of β over F .

So we record the following statement.

Let K be any field and Let $G = \{\sigma_1, \sigma_2, \dots, \sigma_n\}$ be a group of n elements which are automorphism of K .

Let F be the fixed field of G .

Then K/F is a Galois extension,

$K=F(\beta)$ for some element $\beta \in K$

and if $g(X) = \prod_{i=1}^n (x - \sigma_i(\beta))$

Then g is the minimal polynomial of β over F .

Also $[K:F] = n = \text{order of } G$.

Step (ii) :

To prove that $G(K/F) = \bar{G}$.

Now $\sigma \in G \Rightarrow \sigma$ is an automorphism of K

and $\sigma(a) = a \quad \forall a \in F. (\because F \text{ is the fixed field of } G)$

$\Rightarrow \sigma(ax) = \sigma(a)\sigma(x)$
 $= a\sigma(x) \quad \forall a \in F \text{ and } x \in K.$

So that σ is an F -automorphism of G .

Hence $\sigma \in G(K/F)$

Thus $\sigma \in G \Rightarrow \sigma \in G(K/F)$

Hence $G \subseteq G(K/F)$

$\therefore O(G) = n = [K:F] = \text{order of } G(K/F).$

By the previous theorem,

Hence $G = G(K/F).$

This proves the theorem.

Before we go the next theorem we make some remarks.

Remark (i) :

Let $F \subseteq L \subseteq K$ be fields. Then the following are true.

- (i) K/F is a finite extension $\Rightarrow K/L$ is a finite extension.
- (ii) K/F is a separable extension $\Rightarrow K/L$ is a separable extension.
- (iii) K/F is a finite normal extension $\Rightarrow K/L$ is a finite normal extension.
- (iv) K/F is a Galois extension $\Rightarrow K/L$ is a Galois extension.

Proof :

- (i) Is obvious.
- (ii) Proof will be contain in unit 7 (separable extension) verify this unit.
- (iii) K/F is a finite normal extension $\Rightarrow K$ is a splitting field of some polynomial $f(x)$ over F .

$\therefore K = F(\alpha_1, \dots, \alpha_n)$ where $\alpha_i \in K$.

And $f(x) = \prod_{i=1}^n (x - \alpha_i)$

As $F \subseteq L \subseteq K$.

We have $f(x) \in L[x]$

$$K = F(\alpha_1, \alpha_2, \dots, \alpha_n) \subseteq L(\alpha_1, \alpha_2, \dots, \alpha_n) \subseteq K$$

$$\Rightarrow K = L(\alpha_1, \alpha_2, \dots, \alpha_n)$$

and

$$f(x) = \prod_{i=1}^n (x - \alpha_i) \text{ in } K[x] \Rightarrow K \text{ is a splitting field of } f(x) \text{ over } L.$$

$\Rightarrow K/L$ is a normal extension.

(iv) follows from (i), (ii) and (iii).

Remark (ii) :

Let $F \subseteq L \subseteq K$ be fields. Then

- (i) K/F is a finite extension $\Rightarrow L/F$ is a finite extension.
- (ii) K/F is separable $\Rightarrow L/F$ is separable.
- (iii) K/F is normal $\Rightarrow L/F$ is normal.

Example :

Take $F=Q$, $L=Q(\sqrt[3]{2})$ and $K=Q(\sqrt[3]{2}, \omega)$ where ω is a nonreal primitive roots of unity. We know that K is a normal extension of F but L is not a normal extension of F .

(ii) So K/F is a Galois extension $\neq L/F$ is a Galois extension. (Refer theorem iv).

Now we are ready to state and prove the fundamental theorem of Galois theory.

Theorem (iii) :

(The fundamental theorem of Galois theory).

Let K/F be a Galois extension. Let $S_1 = \{L/L \text{ a subfield of } K \text{ such that } L \supseteq F\}$ be the set of all subfields of K containing F and

$S_2 = \{H/H \text{ a subgroup of } G(K/F)\}$ be the set of all subgroups of $G(K/F)$.

For each subgroup H of $G(K/F)$.

Let $K_H = \{x \in K / \sigma(x) = x \quad \forall \sigma \in H\}$ denote the fixed field of H . If

$\phi: S_2 \rightarrow S_1$ is defined by $\phi(H) = K_H$, then ϕ is a bijection.

Proof :

If L is any field such that $F \subseteq L \subseteq K$. Then K/F is a Galois extension $\Rightarrow K/L$ is a Galois extension. (by the remark made above)

and $G(K/L)$ is a subgroup of $G(K/F)$.

Thus we have a map.

$$\Psi : S_1 \rightarrow S_2.$$

defined by $\Psi(L) = G(K/L)$

by theorem

Let K/F be a Galois extension of degree n . Then $G(K/F)$ is a group of order n and F is the fixed field of $G(K/F)$

ie) $F = \{x \in K / \sigma(x) = x, \sigma \in G(K/F)\}$

The fixed subfield of $G(K/F)$ is L .

(K is a Galois extension of L)

$$\Rightarrow \phi(\Psi(L)) = L$$

$$(\phi \circ \psi)(L) = L \quad \forall L \in S_1.$$

$$\Rightarrow \phi \circ \psi = \text{Id}_{S_1}.$$

Now if H is any subgroup of $G(K/F)$. Then H is a finite group of automorphism of K and if $L = \phi(H)$ is the fixed field of H .

By Artin's theorem,

K/L is a Galois extension

and

$$H = G(K/L)$$

$$= \psi(L)$$

$$= \psi(\phi(H))$$

$$\circ \quad (\psi \circ \phi)H = H$$

And this is true for all $H \in S_2$.

Hence

$$\psi \circ \phi = \text{Id}_{S_2}$$

As $\phi \circ \psi$ and $\psi \circ \phi$ are both identity maps. We see that $\phi: S_2 \rightarrow S_1$ and $\psi: S_1 \rightarrow S_2$ are both bijective maps.

This proves the theorem.

Note (i) :

Let K/F be a Galois extension.

If $H_1, H_2 \in S_2$

i.e.) if H_1, H_2 are subgroups of $G(K/F)$ then $H_1 \subseteq H_2 \Rightarrow K_{H_2} \supseteq K_{H_1}$

i.e.) $\phi(H_1) \supseteq \phi(H_2)$

So that $\phi: S_2 \rightarrow S_1$ is an inclusion reversing map.

Also if L_1, L_2 are subfields of K with $L_1 \supseteq F, L_2 \supseteq F$

then $L_1 \subseteq L_2 \Rightarrow G(K/L_2) \subseteq G(K/L_1)$.

i.e.) $\psi(L_2) \subseteq \psi(L_1)$.

So that $\psi: S_1 \rightarrow S_2$ also an inclusion reversing map.

Note (ii) :

Let K/F be a Galois extension.

Let L_1, L_2 be subfields of K with $L_1 \supseteq F, L_2 \supseteq F$.

Let σ be any fixed element of $G(K/F)$.

i.e.) σ is a fixed F -automorphism of K .

Then $L_1 = \sigma(L_2) \Leftrightarrow L_2 = \sigma^{-1}L_1 \Rightarrow G(K/L_1) = \sigma G(K/L_2) \sigma^{-1}$

Proof :

$$\ell \in G(K/L_1) \Leftrightarrow \ell(x) = x \quad \forall x \in L_1$$

(by definition of $G(K/L_1)$)

$$\Leftrightarrow \ell(\sigma(y)) = \sigma(y) \quad \forall y \in L_2$$

$$\Leftrightarrow (\sigma^{-1}\ell\sigma)(y) = y \quad \forall y \in L_2$$

$$\Leftrightarrow \sigma^{-1}\ell\sigma \in G(K/L_2)$$

$$\Leftrightarrow \ell \in \sigma G(K/L_2) \sigma^{-1}$$

Hence $G(K/L_1) = \sigma G(K/L_2) \sigma^{-1}$

Note (iii) :

Let L_1, L_2 be subfields of K with $L_1 \supseteq F, L_2 \supseteq F$ where K/F is a Galois extension and let σ be a fixed element of $G(K/F)$

Then $G(K/L_1) = \sigma G(K/L_2) \sigma^{-1} \Rightarrow L_1 = \sigma(L_2)$

Proof :

$$y \in \sigma(L_2) \Leftrightarrow \sigma^{-1}(y) \in L_2$$

$$\Leftrightarrow \ell(\sigma^{-1}(y)) = \sigma^{-1}(y) \quad \forall \ell \in G(K/L_2)$$

$$\Leftrightarrow (\ell\sigma^{-1})(y) = y \quad \forall \ell \in G(K/L_2)$$

i.e.) $\ell_1(y) = y \quad \forall \ell_1 = \ell\sigma^{-1} \in G(K/L_2)\sigma^{-1}$

$$= G(K/L_1)$$

$$\Leftrightarrow \ell_1(y) = y \quad \forall \ell_1 \in G(K/L_1)$$

$$\Leftrightarrow y \in \text{fixed field of } G(K/L_1) = L_1$$

$$\Leftrightarrow y \in L_1.$$

Hence

$$G(K/L_1) = \sigma G(K/L_2) \sigma^{-1} \Rightarrow \sigma(L_2) = L_1$$

$$G(K/\sigma(L_2)) = \sigma G(K/L_2) \sigma^{-1}$$

Theorem (iv) :

Let $F \subseteq L \subseteq K$ where K/F is a Galois extension. Then

- (i) L/F is a normal extension $\Leftrightarrow G(K/L)$ is a normal subgroup of $G(K/F)$, and in that case
- (ii) $G(L/F) \cong \frac{G(K/F)}{G(K/L)}$

Proof :

Let $\sigma \in G(K/F)$. Then

$$G(K/\sigma(L)) = \sigma G(K/L) \sigma^{-1} \text{ by the result in note (iii) above.}$$

So we see that $G(K/L)$ is a normal subgroup of

$$G(K/F) = \sigma G(K/L) \sigma^{-1} = G(K/L) \quad \forall \sigma \in G(K/F)$$

$$\Leftrightarrow G(K/\sigma(L)) = G(K/L) \quad \forall \sigma \in G(K/F)$$

$$\Leftrightarrow \sigma(L) = L \quad \forall \sigma \in G(K/F) \text{ by the previous theorem.}$$

Claim (i) :

Let L be a normal extension of F . Then $G(K/L)$ is a normal subgroup of $G(K/F)$.

Proof :

$F \subseteq L \subseteq K$, L/F is normal $\Rightarrow L$ is a splitting field of some polynomial $f(x)$ over F and if σ is any element of $G(K/F)$,

$\sigma: L \rightarrow K$ is an F -isomorphism of L into K

by Lemma,

Let $f(x)$ be a polynomial in X over a field F and let K be a splitting field of $f(x)$ over F . If a field L is an extension of F and $\sigma: K \rightarrow L$ is any F -isomorphism of K into L . Then $\sigma(K) = K$.

i.e.) $\sigma(L) = L \quad \forall \sigma \in G(K/F)$

By the remark made above this

$\Rightarrow G(K/L)$ is a normal subgroup of $G(K/F)$.

Hence claim (i) is proved.

Claim (ii) :

Suppose $G(K/L)$ is a normal subgroup $G(K/F)$. Then L is a normal extension of F .

Proof :

As K/F is a finite separable extension and $F \subseteq L \subseteq K$.

Let L/F is a finite, separable extension.

So,

$L = F(\alpha)$ for some $\alpha \in L$.

Also

$G(K/L)$ is a normal subgroup of $G(K/F)$.

By hypothesis

$$\Rightarrow \sigma(L) = L \quad \forall \sigma \in G(K/F)$$

(by the remark made in the beginning)

Consider the polynomial,

$$g(x) = \prod_{\sigma \in G(K/F)} (x - \sigma(\alpha))$$

Then $\sigma \in L$ and $\sigma(L) = L \quad \forall \sigma \in G(K/F)$

$$\Rightarrow \sigma(\alpha) \in L \quad \forall \sigma \in G(K/F)$$

So that $g(x) \in L[x]$

By an argument which is familiar.

We have $g(x) = g \quad \forall \sigma \in G(K/F)$

So that $g(x) \in F[x]$

and $L = F(\alpha) = F(\sigma_1(\alpha), \sigma_2(\alpha), \dots, \sigma_n(\alpha))$

If $G(K/F) = \{\sigma_1, \sigma_2, \dots, \sigma_n\}$

$\Rightarrow L$ is a splitting field of $g(x)$ over F .

Hence L is a normal extension of F .

This proves claim (ii)

Thus we have proved (i).

To prove (ii) :

Here we are assuming that $F \subseteq L \subseteq K$.

And L is a normal extension of F .

So that L/F is a Galois extension of F .

For all $\sigma \in G(K/L)$

$\sigma : K \rightarrow K$ we have $\sigma(L) = L$.

If we write $\sigma^*(x) = \sigma(x) \quad \forall x \in L$

then $\sigma^* : L \rightarrow L$ is an F -isomorphism,

onto ($\because \sigma^*(L) = \sigma(L) = L$)

So that

$$\sigma^* \in G(L/F)$$

Thus

If we write $\phi(\sigma) = \sigma^*$

We have a map

$$\phi : G(K/F) \rightarrow G(L/F)$$

If $\sigma \ell \in G(K/F)$

$$(\ell \sigma)^*(x) = (\sigma \ell)(x)$$

$$= \sigma(\ell(x))$$

$$= \sigma^*(\ell(x))$$

$$\Rightarrow \sigma^* \ell^*(x) = (\sigma^* \ell^*)(x) \quad \forall x \in L$$

$$\Rightarrow \sigma^* \ell^* = (\sigma \ell)^*$$

$$\Rightarrow (\sigma \ell)^* = \sigma^* \ell^*$$

$$\phi(\sigma \ell) = \phi(\sigma) \phi(\ell)$$

ϕ is a group homomorphism.

$$\sigma \in \text{Ker } \phi \Leftrightarrow \sigma^* = \text{Id}_L \Leftrightarrow x = \text{Id}_L(x)$$

$$\Leftrightarrow \sigma^*(x) = \sigma(x)$$

$$\forall x \in L \Leftrightarrow \sigma \in G(K/L)$$

So that $\text{Ker } \phi = G(K/L)$.

[Note : As $G(K/L) = \text{Ker } \phi$ is a normal subgroup of $G(K/F)$. This gives another proof of claim (i) above.]

By the fundamental theorem on group homomorphism, we have,

$$\text{Im } \phi \cong G(K/F)/G(K/L),$$

So order of,

$$O(\text{Im } \phi) = \frac{O(G(K/F))}{O(G(K/L))} = \frac{[K:F]}{[K:L]}$$

(by theorem 1, since K/F and K/L are Galois extension).

$$= [F:L] = O(G(L/F))$$

$$\text{As } \text{Im } \phi \subseteq G(L/F)$$

$$\therefore O(\text{Im } \phi) = O(G(L/F))$$

$$\Rightarrow \text{Im } \phi = G(L/F)$$

So that ϕ is onto.

$$\text{We have } G(L/F) \cong \frac{G(K/F)}{G(K/L)}$$

This proves (ii) and Completes the proof of the theorem.

Example :

Let $f(x) = x^3 - 2 \in \mathbb{Q}[x]$

Then its splitting field is $K/\mathbb{Q}$.

Where $K = \mathbb{Q}(\sqrt[3]{2}, \omega)$. Where $\omega = \frac{-1+i\sqrt{3}}{2}$ $K/\mathbb{Q}$ is a Galois extension of $\mathbb{Q}$.

And $G = G(K/\mathbb{Q})$ is of order 6.

As $x^3 - 2$ is irreducible over $\mathbb{Q}$ with roots $\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}$. These three elements are conjugate elements.

Also ω, ω^2 are conjugate elements as they are the roots of the polynomial x^2+x-1 . Which is irreducible over $\mathbb{Q}$. So if $\sigma \in G$, σ maps $\sqrt[3]{2}$ into one of $\{\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}\}$ and σ maps ω into one of $\{\omega, \omega^2\}$ so that there are 6 possibilities.

- 1) $\text{Id} = \sigma_1: \sqrt[3]{2} \rightarrow \sqrt[3]{2}$
 $\omega \rightarrow \omega$
- 2) $\phi = \sigma_2: \sqrt[3]{2} \rightarrow \sqrt[3]{2} \cdot \omega$
 $\omega \rightarrow \omega$
- 3) $\phi^2 = \sigma_3: \sqrt[3]{2} \rightarrow \sqrt[3]{2} \cdot \omega^2$
 $\omega \rightarrow \omega$
- 4) $\psi = \sigma_4: \sqrt[3]{2} \rightarrow \sqrt[3]{2}$
 $\omega \rightarrow \omega^2$
- 5) $\phi\psi = \sigma_5: \sqrt[3]{2} \rightarrow \sqrt[3]{2} \cdot \omega$
 $\omega \rightarrow \omega^2$
- 6) $\psi\phi = \sigma_6: \sqrt[3]{2} \rightarrow \sqrt[3]{2} \cdot \omega^2$
 $\omega \rightarrow \omega^2$

As $(\phi\psi, (\sqrt[3]{2}), \neq \psi\phi(\sqrt[3]{2}))$, we have $\phi\psi \neq \psi\phi$. As $\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6$ are 6 distinct elements of G and G is a group of order 6, we conclude that $G = \{\sigma_1, \sigma_2, \dots, \sigma_6\}$ and G is non-commutative. So $G \simeq S_3$, the symmetric group as 3 symbols. The subgroups of G are (i) G , (ii) $\{\text{Id}, \phi, \phi^2\}$ (iii) $\{\text{Id}, \psi\}$ (iv) $\{\text{Id}, \phi, \psi\}$ and $\{\text{Id}, \psi\phi\}$ (vi) $\{\text{Id}\}$. The corresponding fixed fields of these subgroups are respectively.

(i) $\mathbb{Q}/\mathbb{Q}$ (ii) $\mathbb{Q}(\omega)/\mathbb{Q}$ (iii) $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ (iv) $\mathbb{Q}(\omega^2, \sqrt[3]{2})$ (v) $\mathbb{Q}(\omega\sqrt[3]{2})/\mathbb{Q}$ and $\mathbb{K}/\mathbb{Q}$ respectively of the six subgroups only these in (i), (ii) and (vi) are normal subgroups of G and the corresponding subfields are normal extension of $\mathbb{Q}$.

Note :

Before we state the next theorem we consider the following. Suppose K_1, K_2 are two subfields of a field L . Then K_1, K_2 denotes the set

$$K_1 K_2 = \left\{ \frac{\sum_{i=1}^n a_i b_i}{\sum_{j=1}^m c_j d_j} \mid a_i, c_i \in K_1; b_i, d_i \in K_2; \right. \\ \left. n \geq 1; m \geq 1 \text{ not fixed and } \sum_{j=1}^m c_j d_j \neq 0 \right\}$$

We note that $K_1 K_2$ is a subfield of L , $K_1 K_2 \supseteq K_1$, $K_1 K_2 \supseteq K_2$ and $K_1 K_2$ is in fact, the smallest subfield of L containing both K_1 and K_2 .

Theorem :

Let K_1/F be a Galois extension and Let K_2/F be any extension. Where K_1, K_2 are subfields of some field L . Then $K_1 K_2/K_2$ is a Galois extension and $G(K_1 K_2/K_2)$ is isomorphic to a subgroup of $G(K_1/F)$.

Proof :

(i) If K_1/F is a finite separable extension $\Rightarrow K_1 = F(\alpha)$ for some $\alpha \in K_1$.

If $m(x)$ is the minimal polynomial of α over F .

Then $m(x)$ has no repeated roots.

It is clear that $K_1 K_2 = K_2(\alpha)$

So that,

$K_1 K_2$ is a finite extension of K_2 .

If $f(x)$ is the minimal polynomial of α over K_2 .

Then $m(x) \in K_2[x]$ and

$m(\alpha) = 0 \Rightarrow f(x)/m(x)$

$\Rightarrow f(x)$ has no repeated root.

Hence α is separable over K_2 .

So that

$K_1 K_2 = K_2(\alpha)$ is a separable extension of K_2 .

(ii) K_1/F is a normal extension $\Rightarrow K_1$ is a splitting field of some polynomial $g(x)$ over F .

∴ $K_1 = F(\alpha_1, \alpha_2, \dots, \alpha_n)$

where

$$\alpha_1, \alpha_2, \dots, \alpha_n \in K_1$$

and are roots of $g(x)$.

$$\text{Now } g(x) \in F[x] \subseteq K_2[x]$$

$$\begin{aligned} \text{and } K_1 K_2 &= K_2 \cdot F(\alpha_1, \dots, \alpha_n) \\ &= K_2(\alpha_1, \dots, \alpha_n) \end{aligned}$$

$\Rightarrow K_1 K_2$ is a splitting field of the polynomial $g(x)$ over K_2 .

Hence $K_1 K_2$ is a normal extension of K_2 .

Thus we have shown that $K_1 K_2$ is a finite, normal and separable extension of K_2 .

$\therefore K_1 K_2 / K_2$ is a Galois extension.

$$\text{As } K_1 \subseteq K_1 K_2 \quad \forall \sigma \in G(K_1 K_2 / K_2)$$

$$\text{Let } \sigma^*(x) = \sigma(x) \in K_1, \quad \forall x \in K_1$$

Since K_1 / F is normal.

$$\text{Then for } a \in F \subseteq K_2$$

$$\text{We have } \sigma^*(a) = \sigma(a) = a$$

$\therefore \sigma^*$ is an F -homomorphism of K_1 into K_1 .

$$\therefore \sigma \text{ is 1-1} \Rightarrow \sigma^* \text{ is 1-1.}$$

As K_1 is a vector space over F .

$$\text{And } \sigma^*: K_1 \rightarrow K_1 \text{ is an } F\text{-linear map.}$$

$$\sigma^* \text{ is 1-1} \Rightarrow \sigma^* \text{ is onto.}$$

$$\text{So that } \sigma^* \in G(K_1 / F)$$

Thus we have a map.

$$\phi: G(K_1 K_2 / K_2) \rightarrow G(K_1 / F)$$

$$\text{defined by } \phi(\sigma) = \sigma^*$$

This is clearly a group-homomorphism.

$$\sigma \in \text{Ker } \phi \Leftrightarrow \sigma^* = \text{Id}_{K_1} \Leftrightarrow \sigma|_{K_1} = \text{Id}$$

$$\text{But } \sigma \in G(K_1 K_2 / K_2) \Rightarrow \sigma(a) = a \quad \forall a \in K_2$$

$$\text{So } \sigma|_{K_1} = \text{Id} \Leftrightarrow \sigma(a) = a \quad \forall a \in K_1$$

$$\Leftrightarrow \sigma(a) = a \quad \forall a \in K_1 K_2$$

$$\Leftrightarrow \sigma = \text{Identity element of } G(K_1 K_2 / K_2)$$

$$\text{So that } \text{Ker} \phi = \{\text{Id}\}$$

So

$$\phi: G(K_1 K_2 / K_2) \rightarrow G(K_1 / F) \text{ is 1-1}$$

Hence $G(K_1 K_2 / K_2)$ is isomorphic to $\text{Im} \phi$.

Which is a subgroup of $G(K_1 / F)$.

This completes the proof.

Theorem :

Let K/F be any finite extension where F is a finite field. Then K/F is a Galois extension and $G(K/F)$ is cyclic.

Proof :

As K is finite. Ch of K is positive. Say P and so K is of order P^n for some $n \geq 1$.

Also K is a splitting field of $x^{P^n} - x$ over the field p of p elements.

And so K is a splitting field of $x^{P^n} - x$ over subfield F also.

So K/F is a finite, normal extension.

As F is a finite, it is a perfect field and So K/F is separable.

So K/F is a Galois extension.

Let order of F be q with $[K:F]=m$

So that $G(K/F)$ is of order m .

As $q=p^r$ where $r=[F:p]$

We have,

$$(a+b)^q = (a+b)^p = a^p + b^p = a^{p^r} + b^q$$

$$\text{and } (ab)^q = a^q b^q.$$

If we write $\sigma(a) = a^q \quad \forall a \in K$

Then $\sigma: K \rightarrow K$ is a ring homomorphism

Which is 1-1.

As σ is 1-1 and K is finite.

$\therefore \sigma$ is onto, so that σ is an automorphism of K .

Also $a^q = a \quad \forall a \in F$ as order of $F = q$

$\Rightarrow \sigma(a) = a \quad \forall a \in F \Rightarrow \sigma$ is an F -automorphism of K .

$\therefore \sigma \in G(K/F)$ and

$$O(G(K/F)) = m$$

To show that G is cyclic it is enough if we prove that σ is of order m .

$$(i) \quad \sigma^m(a) = a^{q^m} = a \quad \forall a \in K$$

$$\therefore O(K) = q^m$$

$$[As [K:F] = m \text{ and } O(F) = q]$$

Hence $\sigma^m = \text{identity element of } G(K/F)$.

So order of $\sigma \in G(K/F)$ is K with $1 \leq K \leq m$.

(ii) To prove that $K = m$. As K is a finite field. Its multiplicative group of non-zero elements is cyclic.

Let it be generated by C .

$$\text{So that } O(C) = q^m - 1$$

$$\text{Now } \sigma^K = \text{Identity} \Rightarrow \sigma^K(x) = x. \quad \forall x \in K$$

$$\Rightarrow C = \sigma^K(C) C^{q^K} \quad \text{As } C \neq 0.$$

$$\text{We have } C^{q^K - 1} = 1 \text{ with } 1 \leq K \leq m$$

But multiplicative order of

$$C = q^m - 1 \Rightarrow q^K - 1 \geq q$$

$$\Rightarrow K \geq m \Rightarrow K = m.$$

So that

$$O(\sigma(G(K/F))) \text{ is } K = m.$$

$$\text{And } O(G(K/F)) = m$$

This $\Rightarrow$ that $G(K/F)$ is cyclic being generated by σ .

This completes the proof.

Remark (iii) :

We next give a proof of the theorem that the field of all complex numbers is algebraically closed based on (i) the fundamental theorem of Galois theory (ii) some results in group theory and the following two results.

(iii) If $f(x) = a_0 + a_1x + \dots + a_nx^n$ is a polynomial of odd degree n over the field of all real numbers then $f(x)$ has atleast one real root.

(Proof : Let us suppose that $a_n = 1$. Then $f(x) \rightarrow -\infty$ as $x \rightarrow -\infty$ and $f(x) \rightarrow +\infty$ as $x \rightarrow +\infty$. So there exist real numbers a, b with ab such that $f(a) < 0$ and $f(b) > 0$. As $f(x)$ is a continuous function of x on $[a, b]$ and $f(a) < 0 < f(b)$, by the intermediate value theorem, $\exists$ a real number C with $a < C < b$ such that $f(C) = 0$).

So if $f(x)$ is an irreducible polynomial of odd degree over the reals, then $\deg f = 1$.

Remark (iv) :

If C denotes the field of the all complex numbers that there is no field extension K/C of degree 2. Let, if possible K/C be an extension of degree 2.

Then $K = C(\alpha)$ for some $\alpha \in K$ with minimal polynomial $m(x)$ of degree $= [K:C] = 2$ over C .

$$\text{So } m(x) = x^2 + ax + b \in C[x]$$

$$\alpha^2 + a\alpha + b = 0$$

$$\Rightarrow \alpha = \frac{-a \pm \sqrt{a^2 - 4b}}{2}$$

$$\text{Let } a^2 - 4b = p + iq \text{ where } p, q \text{ are real.}$$

Claim :

$\exists$ a complex number $z = x + iy$ such that $z^2 = p + iq$

If $z = x + iy$, where x, y are real. Then we have only to find x, y such that

$$p + iq = (x + iy)^2 = x^2 - y^2 + 2i(xy)$$

$$\text{i.e.) such that } x^2 - y^2 = p, 2xy = q$$

$$(x^2 - y^2)^2 = (x^2 - y^2)^2 + (2xy)^2 = p^2 + q^2 \text{ and as } p^2 + q^2 \geq 0$$

$$\text{We have } x^2 + y^2 = \pm \sqrt{p^2 + q^2}$$

$$\text{exists then } x^2 = \frac{\sqrt{p^2 + q^2} + p}{2} \geq 0 \text{ \&}$$

$$y^2 = \frac{\sqrt{p^2 + q^2} - p}{2} \geq 0$$

$$(\because \sqrt{p^2 + q^2} \geq \sqrt{p^2} = |p| \geq p)$$

So that there exist real numbers x, y such that

$$z^2 = p + iq = \sqrt{a^2 - 4b}$$

$$\text{Hence } \alpha = \frac{-a \pm (x + iy)}{z} \in \mathbb{C}$$

This is $\Rightarrow \Leftarrow$. Since $z = [K:\mathbb{C}]$

$$= [C(\alpha):\mathbb{C}] \Rightarrow \alpha \in \mathbb{C}$$

This contradiction proves the required result.

Theorem :

The field $\mathbb{C}$ of all complex numbers is algebraically closed.

Proof :

Let $K/\mathbb{C}$ be any algebraic extension.

$$[C:\mathbb{R}] = 2$$

So there exists an extension $N/\mathbb{R}$ which is a finite normal extension of $\mathbb{R}$ with $N \supseteq K \supseteq \mathbb{C}$.

N is a Galois extension of $\mathbb{R}$.

And so $G = G(N/\mathbb{R})$ is a finite group of even order.

$$\begin{aligned} \text{Because } O(G(N/\mathbb{R})) &= [N:\mathbb{R}] = [N:\mathbb{C}][C:\mathbb{R}] \\ &= [N:\mathbb{C}] \times 2 \text{ is an even integer.} \end{aligned}$$

So we have $O(G) = 2^{m \times n}$ for some integer m, n with $m \geq n \geq 1$ and n is odd.

Claim (i) :

$n=1$. As $2^m/O(G)$, by sylow theorem, G contains a subgroup H . (say) of order 2^m .

Let L denote the fixed field of H .

So that $[N:L] = O(H) = 2^m$ and

$$[L:\mathbb{R}] = \frac{[N:\mathbb{R}]}{[N:L]} = \frac{2^m \cdot n}{2^m} = n$$

As $\text{Ch of } R = 0$. L is a separable extension of R .

And L is a simple extension of R .

(say) $L = R(\alpha)$. If $m(x)$ is the minimal polynomial of α over R .

Then $\deg m(x) = [R(\alpha):R] = [L:R] = n$ is odd.

By the remark (ii) above, this $\Rightarrow n=1$.

Hence the claim (i) is proved.

$\therefore O(G) = 2^m \cdot I$ for some $m \geq 1$.

Claim (ii) :

$$N = C$$

As N/R is a Galois extension and $R \supseteq C \supseteq N$.

We have N/C is a Galois extension.

If $G_1 = G(N/C)$. Then G_1 is a subgroup of $G = G(N/R)$.

We claim that $G_1 = \{\ell\}$

Which will imply that $N = C$.

Suppose not

Then $O(G) = 2^m \Rightarrow O(G_1) = 2^K$, for some $K \geq 1$

And this $G_1 \Rightarrow$ contains a subgroup G_2 of order 2^{K-1} .

Let L be the fixed field of G_2 .

Then $C \subseteq L \subseteq N$, $[N:C] = O(G_1) = 2^K$.

$$[N:L] = O(G_2) = 2^{K-1}$$

So that
$$[L:C] = \frac{[N:C]}{[N:L]} = 2$$

$\therefore L$ is a field extension of degree 2 over C . But by the remark (iv) above, C has no extension of degree 2. Hence $G_1 = \{\ell\} \Rightarrow N=C$. As $C \subseteq K \subseteq N$. And $N=C$.

We have $K = C$

Thus we see that C has no finite extension except.

Hence C is algebraically closed.

This proves the theorem.

APPLICATION OF GALOIS THEORY

Notation :

Let K be a field of characteristic p and m a positive integer. We write $[m, p] = 1$ if either of the following conditions is satisfied.

- (i) $p = 0$ and m arbitrary.
- (ii) $p > 0$ and m and p are coprime.

Cyclic extensions :**Definition :**

Any root of the polynomial $f(x) = x^n - 1 \in F[x]$ in some extension field of F is called an n^{th} root of unity.

If ℓ is an n^{th} root of unity, $f(\ell) = 0$ and $f'(\ell) = n\ell^{n-1} \neq 0$ as that ℓ is a simple root. Thus all the n^{th} roots of unity are distinct.

Theorem :

The n^{th} roots of unity form a cyclic group for multiplication.

Proof :

Let $\ell_1, \ell_2, \dots, \ell_n$ be the distinct n^{th} roots of unity in some splitting field of $x^n - 1 \in F[x]$.

Then $\{\ell_1, \ell_2, \dots, \ell_n\}$ is clearly an abelian group G for multiplication.

$$\ell_i^{n+1} = 1$$

If $\ell_i, \ell_j \in G$.

$$\text{Then } (\ell_i \ell_j)^n = \ell_i^n \ell_j^n = 1.$$

$$(\ell_i^{-1})^n = (\ell_i^n)^{-1} = 1.$$

$$\therefore \ell_i \ell_j = \ell_j \ell_i, \quad i \neq j.$$

Let t = exponent of G .

$$\text{Then } \ell_i^t = 1, \quad 1 \leq i \leq n.$$

and $x^t - 1 \in F[x]$ has at most t roots.

Hence $t = n$.

$\therefore G$ has an element of order n .

Hence G is cyclic.

Definition :

Any generator of the cyclic group of n^{th} roots of unity is called a primitive n^{th} root of unity. Clearly there are $\phi(n)$ primitive n^{th} roots of unity, where $\phi(n)$ is the number of positive integers less than n and relatively prime to n .

Note (i) :

ℓ is a primitive n^{th} root of unity $\Rightarrow \ell^n = 1$. and $\ell_m \neq 1$ for all integers m with $1 \leq m \leq n-1$. Let ℓ be a primitive n^{th} root of unity, So that the order of the element ℓ in the multiplicative group G is n . We know that an element ℓ^k of G is of order $n \Leftrightarrow K$ is prime to n . Hence the number of primitive n^{th} roots of unity $= \phi(n)$. Where ϕ is Euler's totient function.

Note (ii) :

If $\text{Ch of } f = p \geq 0$ and $(\ell, n) = 1$ we have seen that there exists at least one primitive n^{th} root of unity. Suppose $p \geq 1$ and $(\ell, n) > 1$ i.e., p/n . Then we assert that there cannot exist a primitive n^{th} root of unity. For if $n = m$ where m is a positive integer and $\ell^n = 1$,

Then

$$\begin{aligned} 0 &= \ell^{mp-1p} \\ &= (\ell^m - 1)^p \text{ (as ch of } F = P \Rightarrow P^m - 1 = 0). \end{aligned}$$

$$\Rightarrow \ell \text{ is an } m^{\text{th}} \text{ root of unity with } 1 \leq m = n/p < n.$$

Hence, if $p \leq 1$ and p/n , then there does not exist any primitive n^{th} root of unity. It is for this reason that we assume that $(n, p) = 1$.

Theorem :

Let ℓ be a primitive n^{th} root of unity in some extension of a field F . Then $F(\ell)/F$ is a Galois group which is isomorphic to a subgroup of the multiplicative group of units in the ring $\mathbb{Z}/(n)$. So $G(F(\ell)/F)$ is an abelian group.

Proof :

If ℓ is a primitive n^{th} root of unity. Then the set of all n^{th} roots of unity $= \{1, \ell, \ell^2, \ell^3, \dots, \ell^{n-1}\}$. $K = F\{1, \ell, \dots, \ell^{n-1}\} = F(p)$ is a splitting field of ℓ over F .

So that $F(\ell)$ is a normal extension of F .

If $m(x)$ is the minimal polynomial of ℓ over F .

Then $m(x)/(x^n-1)$ and x^n-1 has distinct roots $\Rightarrow m(x)$ has no repeated roots.

So ℓ is separable over F .

So that $F(\ell)/F$ is a separable extension.

Hence K/F is a Galois extension.

It $\sigma \in G(K/F)$.

Then $(\sigma(\ell))^n = \sigma(\ell^n) = \sigma(1) = 1$.

$\Rightarrow \sigma(\ell)$ is an n^{th} root of unity. Also $\sigma(\ell)$ is a primitive n^{th} root of unity.

$\therefore$ If $\sigma(\ell)$ is of order.

Then $1 \leq k \leq n$ and $1 = (\sigma(\ell))^k = \sigma(\ell^k)$.

$\Rightarrow \ell^k = 1 \Rightarrow n = \text{order of } \ell \leq k$.

$\Rightarrow k = n$.

So that order of $\sigma(\ell) = n$.

So $\sigma(\ell) = \ell^k$ for some integer k with $(k, n) = 1$.

So that $\bar{k}$ is a unit in the ring $Z/(n)$.

It $H =$ multiplicative group of units of $Z/(n)$.

We have a mapping $\phi : G(K/F) \rightarrow H$ given by $(\sigma) = \bar{k}$.

$\therefore \sigma(\ell) = \ell^k$

Now $\sigma(\ell) = \ell^k$ and

$\sigma(\ell) = \ell^1$

Multiplicative order of ℓ is $n = \bar{k} - \bar{\ell}$ in $Z/(n)$.

So that ϕ is well - defined.

It

$\sigma_1(\ell) = \ell^k$ and $\sigma_2(\ell) = \ell^1$.

Then

$(\sigma_1\sigma_2)(\ell) = \sigma_1(\ell)\sigma_2(\ell)$

$$= \sigma_1(\sigma_2(\ell)) = \sigma_1(\ell^1) = (\sigma_1(\ell))^1.$$

$$= (\ell^k)^\ell = \ell^{k\ell}.$$

$$\phi(\sigma_1\sigma_2) = \overline{k\ell} = \overline{k} \cdot \overline{\ell} = \phi(\sigma_1) \cdot \phi(\sigma_2).$$

So that ϕ is a group homomorphism.

$$\sigma \in \ker \phi \Leftrightarrow \phi(\sigma) = T \Leftrightarrow$$

$$\sigma(\ell) = \ell \Leftrightarrow \sigma(x) = x \quad \forall x \in F(\ell)$$

($\therefore \sigma$ is an F - isomorphism)

$$\Leftrightarrow \sigma = \text{Identity map.}$$

$$\ker \phi = (\text{Id})$$

$$\Rightarrow \phi : G(K/F) \rightarrow H \text{ is 1 - 1.}$$

Thus $G(K/F)$ is isomorphic to $\text{Im} \phi$.

Which is sub group of units of $Z/(n)$.

Hence the proof is complete.

Definition :

An extension K/F is called a cyclic extension if it is a Galois extension with cyclic Galois group.

Corollary :

Let ℓ be primitive P_1^{th} root of unity, P_1 prime. Then $F(\ell)/F$ is a cyclic extension.

Proof :

If $K = F(\ell)$. Then K/F is Galois extension with $G(K/F)$ isomorphic to a subgroup of the multiplicative group (z/q) all non-zero elements of the finite field $z/(q)$.

As the group $(z/q)^k$ is cyclic and every subgroup of a cyclic group is cyclic.

We have $G(K/F)$ is cyclic.

Hence the Proof.

Theorem :

Let F be a field to $\text{ch } P \geq 0$ and let n be a positive integer with $(n, p) = 1$. Suppose F contains all the n^{th} roots of unity. Let k be a splitting field of $f(x) = x^n - a \in F[x]$ with $a \neq 0$. If β is a root of $f(x)$, then $K = F(\beta)$ and K/F is cyclic extension. If n is prime either $K = F$ or $[K:F] = n$.

Proof :

Let $\{\ell, \ell^2, \dots, \ell^{n-1}, \ell^n = 1\}$ be the set of all n^{th} roots of unity in F . If β is one root of $x^n - a$.

β is a root of this equation for $i = 1, \dots, n$.

$$\begin{aligned}\text{So } K &= \text{splitting field of } x^n - a \text{ over } F = F(\beta_1(\beta_1 \dots \ell^{n-1} \ell)) \\ &= F(\beta) \text{ since } \ell \in F.\end{aligned}$$

It $m(x)$ is the minimal polynomial of β over F .

We have $m(x)/(x^n - a)$

As $a \neq 0$. We have $\beta \neq 0 \Rightarrow x^n - a$ has n distinct roots $\Rightarrow m(x)$ has no repeated roots.

$\Rightarrow K/F$ is separable.

Hence K/F is a finite separable and normal extension.

$\therefore K/F$ is a Galois extension.

Let $G = G(K/F)$

If $\sigma \in G$.

Then $\sigma(\beta) = \ell^k \beta$.

for some integer β .

and $\sigma(\beta) = \ell^L \beta$.

$$\Leftrightarrow \ell^k = \ell^L.$$

$$\Leftrightarrow k = L \pmod{n}$$

It $\sigma_1, \sigma_2 \in G$ and

$$\sigma_1(\beta) = \ell^k \beta, \sigma_2(\beta) = \ell^L \beta.$$

Then

$$\begin{aligned}(\sigma_1 \sigma_2)(\beta) &= \sigma_1(\sigma_2(\beta)) = \sigma_1(\ell^L \beta) = \sigma_1(\ell^L) \sigma_1(\beta) \\ &= \ell^1 \cdot \ell^k \beta = (\ell^{k+L}) \beta. \\ (\because \ell^L \in F \Rightarrow \sigma(\ell^L) &= \ell^L)\end{aligned}$$

Thus,

If we write $\phi(\sigma) = \bar{k}$.

When ever

$$\sigma(\beta) = \ell^k \beta.$$

Then ϕ is a well - defined map and is a group homomorphism.

$$\sigma \in \ker \phi \Leftrightarrow \phi(\sigma) = \text{Identity map}$$

$$\Leftrightarrow \sigma(\beta) = \beta \Leftrightarrow \sigma(x) = x \quad \forall x \in k$$

$$\Leftrightarrow \sigma = \text{Id} \quad (\because \sigma \text{ is an } F\text{-isomorphism})$$

Hence $\ker \phi = \text{Id}$.

And

$\phi : G \rightarrow (z/(n), +)$ is a group homomorphism which is 1-1.

As $(z/(n), +)$ is cyclic.

$\therefore G \cong \text{Im} \phi$, and so G isomorphic

To a cyclic group.

Hence K/F is a cyclic extension.

If n is a prime, $z/(n)$ being of order a prime has no subgroup other than (0) and itself.

So $[K:F] = \text{order of } G = 1 \text{ or } n$.

$\Rightarrow$ either $K = F$ or $[K:F] = n$.

This completes the proof of the Thm.

The following is a converse of above thm.

Theorem :

Let K be a field of char p , m a prime and K contain all the m^{th} roots of unity. Let L/K be a cyclic extension s.t $(L:K) = m$. Then $\exists \omega \in k$ s.t L is the splitting field of $x^m - \omega$ over K .

Proof :

L/F in a cyclic extension.

So it is a Galois extension.

Since $(L:K) = m$, it is a finite separable extension.

So L/K is a simple extension.

ie) $\exists \beta \in L$ s.t $L = K(\beta)$.

Let $f(x)$ be the minimal polynomial of β over K .

Then $\deg f(x) = m$.

β is a root of $f(x)$. L/K is Galois.

$\therefore f(x)$ splits into linear factors in K .

Let $f(x) = (x - \beta_1)(x - \beta_2) \dots (x - \beta_m)$

Where we take $\beta_1 = \beta$.

L/K is cyclic $\Rightarrow G(L/K)$ is a cyclic group.

Let σ be a generator of $G(L/K)$.

Since order of G is m .

We note that σ cannot fix β .

Also since $\sigma(\beta_1)$ is a root, we can assume w.l.g that

$$\sigma(\beta) = \beta_{i+1}, i = 1 \dots m-1,$$

$$\sigma(\beta_m) = \beta_1 = \beta.$$

Let ℓ be the primitive m^{th} root of unity. Define for $1 \leq k \leq m$.

$$\alpha_k = \sum_{i=0}^{m-1} \ell^{ik} \beta_{i+1}.$$

(α_k are called lagrange resolvent)

$$\alpha_m = \sum_{i=0}^{m-1} \ell^{im} \beta_{i+1} = \sum_{i=0}^{m-1} \beta_{i+1} = \sum_{i=1}^m \beta_i.$$

$\sum \beta_i$ being the sum of the roots of $f(x)$ is in K .

$$\therefore \alpha_m \in K.$$

Now

$$\begin{aligned} \sum_{k=1}^m \alpha_k &= \sum_{k=1}^m \left(\sum_{i=0}^{m-1} \ell^{ik} \beta_{i+1} \right) \\ &= \sum_{i=0}^{m-1} \left(\sum_{k=1}^m \ell^{ik} \right) \beta_{i+1} \end{aligned}$$

$$= m\beta.$$

$$\sum_{k=1}^m \alpha_k \notin K$$

Since $\beta \notin K$.

But $\alpha_m \in K$.

∴ For some $k, 1 \leq k \leq m-1, \alpha_k \notin K$.

Consider,

$$\sigma(\alpha_k) = \sigma\left(\sum_{i=0}^{m-1} \ell^{ik} \beta_{i+1}\right)$$

$$= \sum_{i=0}^{m-1} \sigma(\ell^{ik}) \sigma(\beta_{i+1})$$

$$= \sum_{i=0}^{m-2} \ell^{ik} \beta_{i+2} + \ell^{k(m-1)} \beta_1$$

$$= \sum_{i=0}^{m-2} \ell^{ik} \beta_{i+2} + \ell^{k(m-1)} \beta_1$$

$$= \sum_{i=0}^{m-2} \ell^{ik} \beta_{i+2} + \ell^{-k} \beta_1$$

$$= \ell^{-k} \left(\sum_{i=0}^{m-2} \ell^{ik+k} \beta_{i+2} + \beta_1 \right)$$

$$= \ell^{-k} \left(\sum_{i=0}^{m-2} \ell^{(i+1)k} \beta_{i+2} + \beta_1 \right)$$

$$= \ell^{-k} \left(\sum_{i=0}^{m-2} \ell^{ik} \beta_{i+1} + \beta_1 \right)$$

$$= \ell^{-k} \left(\sum_{i=0}^{m-2} \ell^{ik} \beta_{i+1} \right)$$

$$= \ell^{-k} \alpha_k.$$

$$\sigma(\alpha_k) = \ell^{-k} \alpha_k \quad \alpha_k \notin K.$$

Now,

$$\sigma(\alpha_k^m) = (\sigma(\alpha_k))^m$$

$$= (\ell^{-k} \alpha_k)^m = \alpha_k^m$$

But

$$\sigma^m(\alpha_k) = (\alpha_k^m)$$

$$\circ \sigma(\alpha_k^m) = \alpha_k^m.$$

Put $\omega = \alpha_k^m$. Then $\sigma(\omega) = \omega$

Let $\ell \in G(L/K)$.

$$\circ \ell = \sigma^1 \text{ as } \sigma \text{ is a generator of } G(L/K).$$

$$\ell(\omega) = \sigma \ell(\omega) = (\sigma \dots \sigma(\omega)) \dots$$

$$= \omega$$

$$\ell(\omega) = \omega, \quad \forall \ell \in G(L/K)$$

$$\Rightarrow \omega \in \text{fixed field of } G(L/K) = K.$$

$$\circ \omega = \alpha_k^m \in K.$$

L is the splitting field of $x^m - \omega$.

$\alpha_k \in L$ is a root of $x^m - \omega$.

The other roots are $\ell \alpha_k, \ell^2 \alpha_k, \dots, \ell^{m-1} \alpha_k$.

Where ℓ is the primitive m^{th} root of 1.

K contains $\ell^i, 0 \leq i \leq m-1$ and $K \subset L \Rightarrow \ell^i \in L, 0 \leq i \leq m-1$.

$$\alpha_k \in L, \quad i \alpha_k \in L, 0 \leq i \leq m-1.$$

$$\circ K(\ell \alpha_k, \ell^2 \alpha_k, \dots, \ell^{m-1} \alpha_k) \subset L.$$

$$K(\alpha_k) \subset L.$$

$$\circ [K(\alpha_k):K]/[L:K]$$

$$\circ [L:K] = [L:K(\alpha_k)][K(\alpha_k):K]$$

$$\circ [L:K] = m \text{ a prime number}$$

$$\circ [K(\alpha_k):K] = 1 \text{ or } m.$$

$$\text{It is 1, } K(\alpha_k) = K \Rightarrow \alpha_k \in K \text{ (not true)}$$

$$\circ [K(\alpha_k):K] = m.$$

$$[L:K(\alpha_k)] = 1 \Rightarrow L = K(\alpha_k).$$

$K(\alpha_k)$ is the splitting field of $x^m - \omega$.

ie) L is the splitting field of $x^m - \omega$.

Cor :

Let $\text{char } k \neq 2$ and L/K an extension with $[L:K] = 2$. Then $\exists \alpha \in L$ s.t $\alpha^2 \in K$ and $L = K(\alpha)$

Proof :

$$\text{char } k \neq 2 \Rightarrow [L:K] = 2,$$

$$P = \text{Char}(k)$$

$+1, -1$ are the square root of unity and $\in K$.

$$[L:K] = 2 \Rightarrow \dim_K L = 2.$$

So L has a basis square $[1, \alpha]$ over K .

$$L = K(1, \alpha)$$

$$= K(\alpha)$$

$$[K(\alpha):K] = 2$$

$\Rightarrow$ deg of the minimal polynomial of $\alpha = 2$.

α is algebraic and $1, \alpha, \alpha^2$ in L .

We can find scalars $c_0, c_1, c_2 \in K$.

$$c_0 + c_1 \alpha + c_2 \alpha^2 = 0.$$

$$c_2 \neq 0.$$

We have

$$b_0 + b_1 \alpha + b_2 \alpha^2 = 0$$

∴ The minimal polynomial of α is $b_0 + b_1 \alpha + b_2 \alpha^2 = (x - \alpha)(x - \beta)$.

β is the other root.

$$\alpha + \beta = -b_1.$$

$$\alpha \beta = b_0.$$

$$b_0 \in K \subset L, \quad \alpha \in L \Rightarrow \beta \in L.$$

∴ L/K is a normal extension finite extension.

$$\beta \neq \alpha.$$

$$f'(x) = 2x + b_1$$

$$f'(\alpha) = 2\alpha + b_1 \neq 0$$

α is a multiple root

∴ L/K is separable extension of finite extension.

∴ L/K is a Galois group of order 2 is cyclic.

Exercise :

- 1) Let K/F be a cyclic extension and L a field such that $F \subset L \subset K$. Show that K/L is cyclic and if L/F is normal, L/F is cyclic.
- 2) Let K/F be cyclic extension. show that There in a unique field L such that $F \subset L \subset K$ such that $[L:F] = d$, for each divisor d of $[K:F]$.

Solvability by Radicals :

We discuss in this section an important application of Galois Theory. This concerns the solution of polynomial equations by radicals, ie) expressing the roots of the polynomial in terms of the coefficients using the field operations and the operation of taking square roots, cube roots and so on.

Definition :

Let $\text{ch } F = P \geq 0$. A finite extension K/F is called a simple radical extension if $K = F(\alpha)$, with $\alpha^n \in F$ and $(n, P) = 1$.

Examples :

Let $F = \mathbb{Q}$ and ℓ be a primitive n^{th} root of unity. Then $F(\ell)/F$ is a simple radical extension.

Definition :

An extension K/F is called a radical extension if it can be obtained as a tower of simple radical extensions.

i.e.) There exist K_i/F ($1 \leq i \leq m$) such that $K_0 = F \subset K_1 \subset \dots \subset K_m = K$ and that K_i/K_{i-1} are simple radical extensions.

The following are clear from the definitions.

Note :

- (i) A simple radical extension, as well as a radical extensions, is separable.
- (ii) If K/L and L/F are radical extensions then K/F is a radical extension.
- (iii) If K_1/F and K_2/F are radical extensions, contained in a field K , K_1K_2/F is a radical extension.

Proof of (iii) :

K_1/F is radical extensions of $\Rightarrow F = L_0 \subseteq L_1 \subseteq \dots \subseteq L_k = K_1$ where L_i/L_{i-1} is a simple radical extension.

consider $L_i = L_{i-1}(\alpha_i)$ with $\alpha_i^{n_i} \in L_{i-1} \quad \forall i = 1, 2, \dots, k$

$$\begin{aligned} K_2 &= K_2F = K_2L_0 \subseteq K_2L_1 \subseteq \dots \subseteq K_2L_k \\ &= K_2K_1 \text{ where } K_2L_{i-1} = K_2(L_{i-1}(\alpha_i)) \\ &= (K_2(L_{i-1}))\alpha_i \text{ with } \end{aligned}$$

$\alpha_i^{n_i} \in L_{i-1} \subseteq K_2L_{i-1} \Rightarrow K_2L_1/K_2L_{i-1}$ is a simple radical extension for each i .

Thus K_2K_1/K_2 is a radical extension.

As K_2/F is a radical extension.

We have K_2K_1/F is a radical extension.

Theorem : (i)

Let K/F be a radical extension. Then there $\exists$ a field L s.t $L \supseteq K$ and s.t L/F is a Galois radical extension.

Proof :

K/F is a radical extension $\Rightarrow K/F$ is a separable extension $\Rightarrow K/F$ is a simple extension say $K = F(\alpha)$ for some $\alpha \in K$.

Let $m(x) \in F[x]$ be the minimal polynomial of α over F .

Let L be a splitting field of $m(x)$ s.t $L \supseteq K$

Then $L = F(\alpha_1, \alpha_2, \dots, \alpha_n)$ where $\alpha_1 = \alpha$ and $\alpha_2, \dots, \alpha_n$ are the roots of $m(x)$.

As $m(x)$ is irreducible over F . $\forall i$ with, $1 \leq i \leq n$.

$\exists$ an F - isomorphism $\sigma_i : F(\alpha_i) = K \rightarrow F(\alpha_i) = K$. (say) so K/F is a radical extension.

$\Rightarrow K_i/F$ is a radical extension. $\forall i$

Now

$K_1 K_2 \dots K_n / F$ [by note (iii)] a radical extension.

But $K_1 K_2 \dots K_n = F(\alpha_1, \alpha_2, \dots, \alpha_n) = L$.

So that L/F is a radical extension.

Now

$\alpha_1 = \alpha$ is separable over F .

$\Rightarrow$ each α_i is separable over F .

$\Rightarrow L = F(\alpha_1, \dots, \alpha_n)$ is separable over F .

As L is a splitting field of some polynomial F .

$\therefore L/F$ is a normal extension.

Hence L/F is a Galois extension which is also a radical extension.

Theorem (ii) :

If K/F be a Galois radical extension. Then $G(K/F)$ is a solvable group.

Proof :

By definition, there exist subfields $F = K_0 \subset K_1 \subset K_2 \dots \subset K_m = K$ with $K_{i+1} = K_i(\beta_i)$, $\beta_i^{n_i} = a_i \in K_i$, $(n_i, p) = 1 \quad \forall i$.

$$m-1$$

$$\text{Let } n = \prod_{i=0}^{m-1} n_i.$$

Then $(n, p) = 1$.

Let K be the splitting field of the separable polynomial $f(x) \in F[x]$.

If $L \supset K$ is a splitting field of $\phi(x) = (x^n - 1)f(x) \in F[x]$, it is also a splitting field of $\phi(x)$ over K .

Since $\phi(x)$ is a separable polynomial. L/F is a Galois extension.

Let L^1 be the subfield of L generated by F and the roots of $x^n - 1 \in F[x]$.

Let L_i ($0 \leq i \leq m$) be the subfield of L generated by L^1 and K_i .

Then $L_0 = L^1 F = L^1$, $L^m = L^1 K_m = L$ and $L_{i+1} = L_i(\beta_i)$ as $K_{i+1} = K_i(\beta_i)$ ($0 \leq i \leq m-1$).

Since L^1 contains all n^{th} root of unity, it contains all n^{th} roots of unity $\forall i$.

Hence by theorem, Assume that F contains all n^{th} roots of unity and K a splitting of $f(x) = x^n - \alpha \in F[x]$. If β is a root of $f(x)$, Then $K = F(\beta)$ and K/F is a cyclic extension. If n is prime, either $K = F$ or $[K:F] = n$.

L_{i+1}/L_i is a cyclic extension ($0 \leq i \leq m-1$).

Also L^1/F is a cyclic extension.

We claim that $G = G(L/F)$ is solvable.

Let G_i be the subgroup of G having L_i as fixed field ($0 \leq i \leq m$).

Then $G_0 = G(L/L_1) \supset G_1 \supset \dots \supset G_m = \{\ell\}$.

Since L_{i+1}/L_i is normal.

$\therefore G_{i+1}$ is a normal subgroup of G_i and G_i/G_{i+1} is isomorphic to the galois group $G(L_{i+1}/L_i)$, which is cyclic.

Now G/G_0 is abelian by theorem Let ℓ be a primitive n^{th} root of unity. Then $F(\ell)/F$ is a galois extension with the galois group isomorphic to a subgroup of the multiplicative group of prime residue classes modulo n . Thus G has a normal series with abelian quotients.

$\Rightarrow G$ is a solvable group. Since $G(K/F)$ can be identified with a quotients group of $G = G(L/F)$.

Hence $G(K/F)$ is solvable.

The following Theorem is the converse of Theorem (ii).

Theorem (iii) :

Let K/F be a galois extension of degree n , $(n, P) = 1$, such that $G = G(K/F)$ is a solvable group then there exists a radical extension L/F such that $K \subset L$.

Proof :

The proof is by induction on $n = 0$ (G). If $n=1$, there is nothing to prove. Assume $n > 1$.

Then $\exists$ a normal subgroup G_1 of G such that G/G_1 is cyclic of prime order by lemma, If G be a finite group. then G is solvable $\Leftrightarrow$ for every composition series of G , then quotients are cyclic of prime order.

Let K_1 be the fixed field of G_1 .

Then K/K_1 and K_1/K are Galois extension with Galois groups G_1 and G/G_1 respectively.

Let $m = 0(G/G_1)$ so that $(m, p) = 1$ as m/n .

Let N be a splitting field of $x^m - 1$ over K .

$\circ N_1$ the subfield of N generated by F and the root of $x^m - 1$.

Then $K_1 N_1 / N_1$ is a Galois extensions, by lemma, Let K_1 / F be a Galois extension and K_2 / F any extension. Then $K_1 K_2 / K_2$ is a Galois extension and $G(K_1 K_2 / K_2)$ is isomorphic to a subgroup of $G(K_1 / F)$.

And $G(K_1 N_1 / N_1)$ is isomorphic to a subgroup of $G(K_1 / F)$.

Since m is prime, $G(K_1 N_1 / N_1)$ is of order 1 or m .

$\circ$ It is a cyclic group.

Since N_1 contains all m^{th} roots of unity. $K_1 N_1 / N_1$ is a simple radical extensions.

By Theorem,

Let n be a prime and assume that F contains all n^{th} roots of unity.

Let K/F be a cyclic extension with $[K:F] = n$. Then there exists some $(\gamma \in F)$ such that K is a splitting field of $x^n - \gamma \in F[x]$.

Since K/K_1 is a Galois extension.

$KN_1 / K_1 N_1$ is a Galois extension with $G(KN_1 / K_1 N_1)$ isomorphic to a subgroup of $G(K/K_1) = G_1 \subset G$.

Since G is solvable.

$G(KN_1 / K_1 N_1)$ is solvable and its order r is less than $n = 1(G)$, with $(r, \ell) = 1$.

By induction,

There exists an extension $L \supset KN_1$ such that $L/K_1 N_1$ is a radical extension.

Since K_1N_1/N_1 is a simple radical extension and N_1/F is a simple radical extension.

It follows that L/F is a radical extension and $L \supset K$.

This proves the Theorem.

Definition :

Let $f(x) \in F[x]$. Then $f(x)$ is said to be solvable by radicals if its splitting field is a subfield of some radical extension of F .

Note (i) :

Let $f(x) = g(x)h(x) \in F[x]$. Let K be a splitting field of b . So that $K = F(\alpha_1, \dots, \alpha_n)$ where $\alpha_1, \dots, \alpha_n$ are the roots of $b(x)$. Suppose that $\alpha_1, \dots, \alpha_r$ are the roots of $g(x)$ and $\alpha_{r+1}, \dots, \alpha_n$ are the roots of $h(x)$ then $K_1 = F(\alpha_1, \dots, \alpha_r)$ and $K_2 = F(\alpha_{r+1}, \dots, \alpha_n)$ are splitting fields of g, h respectively over F and $K = K_1K_2$.

Claim :

f is solvable by radicals over $b \iff g, h$ are both solvable by radicals

(i) $\Rightarrow$ by hyp $K \subseteq L$ where L/K is a radical extension with $L \supseteq K$. As $L_1 \supseteq K_1$ and $L_2 \supseteq K_2$.

We see that g, h are solvable by radicals.

(ii) $\Leftarrow$ By hyp. $\exists$ a radical extensions $L_1/F, L_2/F$ with $L_1 \supseteq K_1, L_2 \supseteq K_2$, and we may suppose that both L_1 and L_2 are contained in some field.

(Say an algebraic closure of F containing K_1, K_2).

Then L_1L_2 is a radical extension of F . and $L_1L_2 \supseteq K_1K_2 = F$.

$\therefore f$ is solvable by radicals over F .

Note (ii) :

From note (i) it follows that $f(x) \in F[x]$ is solvable by radicals over $F \iff$ each irreducible factor of $f(x) \in F[x]$ is solvable by radicals over F .

Theorem (iv) :

Let $f(x) \in F[x]$, K a splitting field of $f(x)$, $[K:F] = n$ and $(n, p) = 1$. Then K/F is a Galois extension. $G(K/F)$ is solvable iff $f(x)$ is solvable by radicals over F .

Proof :

Part I :

As K is a splitting field of a polynomial $f(x)$ over F .

We see that K/F is a finite normal extension.

To show that K/F is a finite normal extension.

To show that K/F is a Galois extension.

We have only to show that it is a separable extension.

i.e.) that the minimal polynomial of any element α of K has no repeated root.

Let α be any element of k and let $m(x) \in F[x]$ be the minimal polynomial of α over F .

It $m = \text{degree of } m(x) \text{ over } F$.

Then $m = [F(\alpha):F]$ is a factor of $[K:F] = n$.

$\therefore m/n$ and $(n,p) = 1 \Rightarrow (m,p) = 1$.

This implies that $m(x)$ has no repeated root.

Then $m(x) = g(x^p)$ for some $g(y) \in F[y]$.

If $g(y) = a_0 + a_1 y + \dots + a_k y^k$ with $a_k \neq 0$

Then $m(x) = g(x^p) = a_0 + a_1 x^p + \dots + a_k x^{kp}$, is of degree $m = kp \Rightarrow p/m$.

$\Rightarrow \Leftarrow$

Since $(m,p) = 1$.

So α is separable over F .

This is true for all $\alpha \in k$ and so K/F is a separable extension. This proves that K/F is a Galois extension.

Now suppose that $G(K/F)$ is solvable by theorem (iii).

There exists a radical extension L/F with $L \supseteq K$.

Hence $f(x)$ is solvable by radicals over F .

Part II :

Conversely,

Let us suppose that $f(x)$ is solvable by radicals.

Then there exists a radical extension L/F with $L \supseteq K$.

By theorem (i),

We may assume without loss of generality that L/F is a radical Galois extension.

Hence by theorem (ii),

$G(L/F)$ is a solvable group. As $F \subseteq K \subseteq L$ and K/F is a normal extension.

We have

$$G(K/F) = \frac{G(L/F)}{G(L/K)}.$$

So that $G(K/F)$, being a homomorphic image of the solvable group $G(L/F)$ is itself a solvable group.

This proves the second part and completes the proof of the theorem.

Remark :

The condition $(n, p) = 1$ is satisfied if $(m!, p) = 1$, where $m = \deg f(x)$.

In particular, it is always, satisfied over a field of char.

Definition :

Let $f(x) \in F[x]$ be a separable polynomial and K a splitting field of $f(x)$. Then $G(K/F)$ is called the Galois group of the polynomial $f(x)$.

Suppose $f(x)$ is irreducible with roots $\alpha_1, \alpha_2, \dots, \alpha_n \in K$, a splitting field of $f(x)$. If $\sigma \in G(K/F) = G$, then $\sigma(\alpha_1), \dots, \sigma(\alpha_n)$ are also roots of $f(x)$ and since $f(x)$ is separable, $\sigma(\alpha_1), \sigma(\alpha_2), \dots, \sigma(\alpha_n)$ coincide with $\alpha_1, \alpha_2, \dots, \alpha_n$ in some order.

ie) σ is a permutation of the n roots $\alpha_1, \alpha_2, \dots, \alpha_n$. Thus we have a map $\phi : G(K/F) \rightarrow S_n$ which is clearly a group homomorphism with $\ker \phi = \{1\}$. Thus G is isomorphic to a subgroup of S_n . Thus the group of any irreducible polynomial of degree n can be looked upon as a subgroup of the symmetric group S_n .

Lemma :

Let $\text{char } F = p \neq 2, 3$ and $f(x) \in F[x]$ with $\deg f(x) \leq 4$. Then $f(x)$ is solvable by radicals.

Proof :

We may assume that $f(x)$ is irreducible. Since $\deg f(x) \leq 4$, $(4!, p) = 1$ as $p \neq 2, 3$.

If K is a splitting field of $f(x)$ and $[K:F] = m$ then $(m, p) = 1$ as $m/4!$ now $G(K/F)$ is isomorphic to a subgroup of $S_n (n \leq 4)$.

Since S_n is solvable for $n \leq 4$.

$\therefore G(K/F)$ is solvable.

Hence $f(x)$ is solvable by radicals.

Examples:

- 1) Let $F = \mathbb{C}$, the field of all complex number. If $f(x) \in F[x]$, and K is a splitting field of $f(x)$ over F , then $K = F$, so that $G(K/F) = \{e\}$, As F is algebraically closed.
- 2) Let $F = \mathbb{R}$, the field of all real numbers. If $F(x)$ is any irreducible polynomial over F then $\deg f \leq 2 \Rightarrow$ group of $F(x)$ over $\mathbb{R}$ is solvable by radicals. Hence every polynomial with real coefficients is solvable by radicals over $\mathbb{R}$.

This is no longer true if we replace the real number field by the rational number field. We shall show that there exists an irreducible $f(x) \in \mathbb{Q}[x]$ of degree 5 whose group is S_5 .

Since S_5 is not solvable, $f(x)$ will not be solvable by radicals over $\mathbb{Q}$.

Lemma :

Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial of degree p, p prime. Assume that $f(x)$ has exactly two non-real roots over the complex number field. Then the group of $f(x)$ is S_p .

Proof :

Let $K/\mathbb{Q}$ be a splitting field of $F(x) \in \mathbb{Q}[x]$ such that $K \subseteq \mathbb{C}$.

Then $K/\mathbb{Q}$ is a galois extension and the group $G = G(K/\mathbb{Q})$ is a subgroup of S_p .

If $\alpha \in K$ is root of $f(x)$.

Then

$$[F(\alpha):F] = \deg f(x) = p.$$

$$\Rightarrow P/[K:F] \Rightarrow P/O(G).$$

By caucly's theorem in group theory,

G contains an element σ of order p . As $\sigma \in G \subseteq S_p$ and order of $\sigma = p$ a prime. σ is p cycle.

Claim :

G contains a transposition. By hypothesis $f(x)$ has exactly 2 non real roots α_1, α_2 (say) Let $\alpha_3, \alpha_4, \dots, \alpha_p$ be the remaining (real) roots of $f(x)$.

As $f(x) \in \mathbb{Q}[x]$ has real coefficients its non real roots occur in complex conjugate pairs.

$$\circ \quad \bar{\alpha}_1 = \alpha_2 \text{ and } \bar{\alpha}_2 = \alpha_1.$$

Let $\ell : K \rightarrow \mathbb{C}$ be the complex conjugation.

Then

$$\begin{aligned} \ell(\alpha_1) &= \bar{\alpha}_1 = \alpha_2, \\ \text{and } \ell(\alpha_2) &= \bar{\alpha}_2 = \alpha_1, \\ \ell(\alpha_i) &= \alpha_i \quad \forall i = 3, \dots, p \end{aligned}$$

So that

$$\begin{aligned} \ell(k) &= \ell(\mathbb{Q}(\alpha_1, \alpha_2, \dots, \alpha_p)) \\ &= \mathbb{Q}(\alpha_2, \alpha_1, \alpha_3, \dots, \alpha_p) = k. \end{aligned}$$

If we restrict the codomain of ℓ of K .

We get

$\ell : K \rightarrow K$ is a $\mathbb{Q}$ - isomorphism and $(K:\mathbb{Q})$ is finite.

$\circ \ell$ is onto

so that ℓ is a $\mathbb{Q}$ - automorphism of K .

$$Z \in G(F/S) = G.$$

$$\text{As } \ell(\alpha_1) = \alpha_2, \ell(\alpha_2) = \alpha_1 \text{ and}$$

$$\ell(\alpha_i) = \alpha_i \text{ for } i = 3, \dots, p.$$

we see that ℓ is a transposition of G .

G contains a p - cycle and a transposition.

$\circ S_p$ is generated by a cycle and transposition.

Hence $G = S_p$.

This proves the lemma.

Corollary :

The polynomial $f(x) = x^5 - 6x + 3 \in \mathbb{Q}[x]$ is not solvable by radicals.

Proof :

$f(x)$ is irreducible by Eisenstein's criterion. It is easy to verify that $f(x)$ has exactly 5 non-real roots by observing that $y = f(x)$ meets the x -axis exactly at 3 points using maxima, minima. Hence the group of $f(x)$ is S_5 which is not a solvable group.

ie) $f(x)$ is not solvable by radicals.

we now prove that the general polynomial of n th degree is not solvable by radicals for $n \geq 5$

Let F be a fixed field and $K = F(x_1, \dots, x_n)$ the field of rational functions in $x_1, x_2, \dots, x_n$ over F . ie) the quotient field of the polynomial ring $F[x_1, \dots, x_n]$ the group $G = S_n$ acts on K by setting

$$\sigma(x_i) = x_{\sigma(i)} \text{ and } \sigma|_F = \text{Id}.$$

Thus for any rational function f/g .

$$\sigma \left(\frac{f(x_1, \dots, x_n)}{g(x_1, \dots, x_n)} \right) = \frac{f(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)})}{g(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)})}$$

Let L be the fixed field of G . Then L is called the fixed field of symmetric rational functions. The following are clearly elements of L .

$$a_1 = x_1 + x_2 + \dots + x_n$$

$$a_2 = \sum_{i < j} x_i x_j$$

$$a_3 = \sum_{i < j < k} x_i x_j x_k$$

$$\dots \dots \dots$$

$$\dots \dots \dots$$

$$a_n = x_1 x_2 \dots x_n$$

these $a_1, \dots, a_n$ are called elementary symmetric functions. Thus $F(a_1, a_2, \dots, a_n)$ is a subfield of L . We prove that these two fields coincide.

FINITE FIELDS

Let F be a finite field. Then $\text{Ch } F = p > 0$ and F contains a subfield $F^1 \cong \mathbb{Z}_p$. Moreover the extension F/F^1 is finite. If $[F:F^1] = n$, then F is isomorphic to $\mathbb{Z}_p^n$ as $\mathbb{Z}_p$ -vector spaces. In particular F has p^n elements. Thus the number of elements in a finite field is always a power of its characteristic.

A field having finite number of elements is called a finite field or a Galois field.

Example :

$$1) \quad \frac{\mathbb{Z}}{2^{\mathbb{Z}}} = \{\bar{0}, \bar{1}\}$$

$$\frac{\mathbb{Z}}{3^{\mathbb{Z}}} = \{\bar{0}, \bar{1}, \bar{2}\}$$

$$\dots \dots \dots$$

$$\dots \dots \dots$$

$$\frac{\mathbb{Z}}{p^{\mathbb{Z}}} = \{\bar{0}, \bar{1}, \dots, \overline{(p-1)}\}$$

$$\frac{\mathbb{Z}}{(2^{1123} - 1)^{\mathbb{Z}}} \cdot 2^{1123} - 1 \text{ is a prime.}$$

(verified by computer)

2) Let F be a finite field

Let F have m elements

$(F, +)$ is an abelian group with m elements.

If $x \in F$, $mx = x + \dots + x$ m times $= 0$

(because any G map with n element, $x^n = \ell$, by lagrange's theorem).

☞ Characteristic of F has to be a prime p .

☞ F contains a subfield isomorphic to $\frac{\mathbb{Z}}{p^{\mathbb{Z}}}$.

F is a vector space over $\frac{\mathbb{Z}}{p^{\mathbb{Z}}}$.

$$\left[F: \frac{Z}{p^Z} \right], \text{ finite.}$$

$$\text{Let } \left[F: \frac{Z}{p^Z} \right] = n.$$

Let $\ell_1, \ell_2, \dots, \ell_n$ be a basis for F over $\frac{Z}{p^Z}$.

$$\circ F = \left\{ a_1 \ell_1 + a_2 \ell_2 + \dots + a_n \ell_n, a_1, \dots, a_n \in \frac{Z}{p^Z} \right\}$$

$\circ |F| = \text{the no. of elements in } F = p^n.$

$\circ x^{p^n} - x$ can have at most p^n roots.

$\circ F$ is precisely the set of all roots of $x^{p^n} - x$.

$\circ F$ is the splitting field of $x^{p^n} - x$ over $\frac{Z}{p^Z}$

$\circ q = p^n$

$F_q = \text{finite field with } q \text{ elements.}$

1) Let F be a field with p^n elements.

$(F, +)$ is an abelian group s.t. $px=0 \forall x \in F$.

$\{F \setminus \{0\}, \cdot\}$ is an abelian group with $p^n - 1$ elts.

$$\forall a \in F \setminus \{0\}, a^{p^n-1} = 1 \quad \circ a \cdot a^{p^n-1} = a$$

$$\text{i.e.) } a^{p^n} = a$$

$\circ a$ is a root of the polynomial $x^{p^n} - x$ over $\frac{Z}{p^Z}$.

Every element of F is a root of $x^{p^n} - x$

$\circ |F| = p^n.$

2) Consider $\frac{Z}{p^Z}$. This is a field with p -elements.

Let $n \in \mathbb{N}$. Consider the polynomial $x^{p^n} - x$ over $\frac{\mathbb{Z}}{p^z}$. Let E be a splitting field for

$$x^{p^n} - x \text{ over } \frac{\mathbb{Z}}{p^z}.$$

We already know that E is a finite extension of $\frac{\mathbb{Z}}{p^z}$.

∴ E is a finite field. In $E[x]$, $x^{p^n} - x$ splits into linear factors.

Step (i) :

Let α be a root of $x^{p^n} - x$ in E . Then α is not a repeated root.

$$\begin{aligned} x^{p^n} - x &= x^{p^n} - x - (\alpha^{p^n} - \alpha) \\ &= x^{p^n} - \alpha^{p^n} - (x - \alpha) \\ &= (x - \alpha)^{p^n} - (x - \alpha) \end{aligned}$$

$$x^{p^n} - x = (x - \alpha) \left((x - \alpha)^{p^n - 1} - 1 \right)$$

$$\therefore (x - \alpha)^2 \times x^{p^n} - x$$

∴ α is not a repeated root.

Step (ii) :

$$\text{Let } F = \left\{ \alpha \in E : \alpha \text{ is a root of } x^{p^n} - x \right\}$$

By step (i), $|F| = p^n$.

If

$$\begin{aligned} \alpha, \beta &\in F \quad (\alpha + \beta)^{p^n} - (\alpha + \beta) \\ &= \alpha^{p^n} + \beta^{p^n} - \alpha - \beta \\ &= \alpha^{p^n} - \alpha + \beta^{p^n} - \beta \\ &= 0 + 0 \end{aligned}$$

∴

$$\alpha + \beta \in F$$

$$\alpha - \beta \in F \quad (\alpha\beta)^{p^n} = \alpha^{p^n} \cdot \beta^{p^n} = \alpha\beta$$

$$\alpha\beta \in F$$

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

$$\alpha^{-1} \in F$$

∴ F is a subfield of E.

$$\frac{z}{p^z} \subset F$$

Let $a \in \frac{z}{p^z}$

$$a^p = a$$

$$a^{p^2} = (a^p)^p = a^p = a$$

$$\dots \dots \dots$$

$$\dots \dots \dots$$

$$\dots \dots \dots$$

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

$$a \in F$$

∴ F is the splitting field of $x^{p^n} - x$ over $\frac{z}{p^z}$.

$$F = E.$$

Lemma :

Let F be a finite field with q elements and suppose $F \subset K$ where K is also a finite field. Then K has q^n elements where $n=[K:F]$

Proof :

K is a vector space over F.

Since K is finite it is certainly finite dimensional as a vector space over F.

Suppose that $[K:F] = n$.

Then K has a basis of n elements over F. Let such a basis be $\vartheta_1, \vartheta_2, \dots, \vartheta_n$.

Then every element in K has a unique representation in the form $\alpha_1 \theta_1 + \dots + \alpha_n \theta_n$ where $\alpha_1, \alpha_2, \dots, \alpha_n$ are all in F .

Thus the number of elements in K is the number of $\alpha_1 \theta_1 + \alpha_2 \theta_2 + \dots + \alpha_n \theta_n$ as the $\alpha_1, \alpha_2, \dots, \alpha_n$ range over F .

Since each coefficient can have q values K must. Clearly have q^n elements.

Theorem :

If F is a finite field, then $O(F) = p^n$ for some prime p and an integer $n \geq 1$.

Proof :

Let P be the prime subfield of F .

Since F is finite. So in p .

$$\circ \quad p \cong \frac{Z}{\langle p \rangle} \text{ for some prime } p.$$

$$\text{But} \quad \frac{Z}{\langle p \rangle} \cong \{0, 1, \dots, p-1\} \text{ mod } p = F_p$$

$$\Rightarrow \quad p \cong F_p$$

$$\text{Since} \quad p \subseteq F, \text{ we can regard } F_p \subseteq F$$

Now,

F is a vector space over F_p

$$\circ \quad F \text{ is finite } [F:F_p] = n = \text{finite}$$

Let $\{u_1, u_2, \dots, u_n\}$ be a basis of F/F_p .

$$\text{Then} \quad F = \{\alpha_1 u_1 + \dots + \alpha_n u_n / \alpha_i \in F_p\}$$

Now each α_i can be chosen in p ways.

$$\sum \alpha_i u_i = \sum \beta_i u_i \Rightarrow \alpha_i = \beta_i$$

$$\circ \quad O(F) = p^n$$

This proves the theorem.

Theorem :

Let p be a prime and $n \geq 1$ be an integer. Then there exists a field with p^n elements.

Proof :

Let $f(x) = x^q - x \in F_p[x]$, $q = p^n$.

Let F be a minimal splitting field of $f(x)$ over F_p .

Then $F = F_p$ (zeros of f in F)

Let $S = \{\text{zeroes of } f \text{ in } F\}$

Now $f' = qx^{q-1} - 1 = -1$ as $\text{Char } F = p \Rightarrow q-1 = p^n-1 = 0$.

Therefore $(f, f') = 1$

$\Rightarrow$ all zeroes of f in F are simple and so distinct.

$\therefore O(S) = q$

Now $O \in S \Rightarrow S \neq \emptyset$.

Also $a, b \in F_q \Rightarrow a^q = a, b^q = b \Rightarrow (a \pm b)^q = a^q \pm b^q$
 $= a \pm b$

$(ab)^q = a^q \cdot b^q = ab$

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

$\Rightarrow a \pm b, ab, ab^{-1} \text{ (if } b \neq 0) \in S$.

Thus S is a subfield of F .

Let $a \in F_p$

Then $a^{p-1} = 1 \Rightarrow a^p = a$

$\Rightarrow a^{p^n} = a \Rightarrow a^q = a$

$\Rightarrow a$ is a zero of f in $F \Rightarrow a \in S \Rightarrow F_p \subseteq S$.

So S is a field containing F_p and S .

But F is the smallest field containing F_p and S .

$\Rightarrow F \subseteq S$. Also $S \subseteq F$

$\therefore S = F \Rightarrow O(F) = O(S) = q$.

Problems :

1) Show that $x^m - 1$ divides $x^n - 1$ over a field F iff m divides n .

Solution :

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

The $x^n - 1 = x^r \left(\sum_{i=0}^{K-1} x^{im} \right) (x^m - 1) + (x^r - 1)$

$$\circ x^{m-1}/x^{n-1} \text{ iff } x^r-1 = 0$$

$$\text{Also } x^r-1 = 0 \text{ iff } r = 0$$

$$\text{So } x^{m-1}/x^{n-1} \text{ iff } m/n.$$

$$2) \text{ Show that } x^{p^m} - x / x^{p^n} - x \text{ if } m/n.$$

Solution :

Let

$$n = mu$$

$$p^n - 1 = p^{mu} - 1$$

$$= (p^m)^u - 1$$

$$= (p^m - 1) (\text{integer})$$

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

By above problem

$$x^{p^{m-1}} - 1 / x^{p^{n-1}} - 1$$

$$\Rightarrow x^{p^m} - x / x^{p^n} - x$$

Theorem :

Every finite extension of a finite field is Galois.

Proof :

Let K be a finite extension of a finite field R . Then K is also finite field. So, $\text{Char. } K = \text{Char } R = p$ for some prime p .

$$\text{Let } O(R) = p^m, O(K) = p^n$$

Now, K is a minimal splitting field of $x^{p^n} - x$ over $F_p \Rightarrow K/F_p$ is finite normal

Also F_p is finite $\Rightarrow F_p$ is perfect

$\Rightarrow$ every algebraic extension of F_p is separable.

$\Rightarrow K/F_p$ is separable $\Rightarrow K/F_p$ is Galois.

Now, $F_p \subseteq R \subseteq K$ and K/F_p is Galois

$\Rightarrow K/R$ is Galois.

This proves the theorem.

Theorem :

Let F be a finite field. Then $\exists$ an irreducible polynomial of any given degree n over F .

Proof :

Now $F^{(n)}$ is a field of n -tuples.

We can regard F as a subfield of $F^{(n)}$.

Let $E = F^{(n)}$

Then $[E:F] = n$

Let $E^* = \langle \alpha \rangle$

Then $E = F(\alpha)$

$\therefore n = [E:F] = [F(\alpha):F] = \deg \text{Irr}(F, \alpha)$

$\Rightarrow p(x) = \text{Irr}(F, \alpha)$ is an irreducible polynomial of degree n over F .

Theorem :

Let G be a group of F_p -automorphisms of F_q . Then G is a cyclic group generated by Frobenius map of order n . Where $q=p^n$.

Proof :

Let $\theta: F_q \rightarrow F_q$ s.t.

$$\theta(b) = b^p$$

Then θ is called Frobenius map.

Since $\text{Char } F_p = \text{Char } F_q = p$

$\therefore \theta$ is a homomorphism.

Also θ is 1-1.

Since F_q is finite. θ is onto.

If $b \in F_p$

Then $b^p = b \Rightarrow \theta(b) = b \forall b \in F_p$

So θ is an F_p -automorphism of F_q .

$\Rightarrow \theta \in G$

By Artin's theorem,

$$\theta(G) = [F_q:F_p] \text{ as } F_p \text{ is the fixed field of } G.$$

$$\Rightarrow O(G) = n$$

$$\text{We show that } O(\theta) = n$$

$$\text{Let } \theta^r = I, \text{ Let } F_q^* = \langle a \rangle$$

$$\text{Then } a^{q-1} = 1 \Rightarrow a^q = a \Rightarrow a^{p^n} = a$$

$$\text{Now } \theta^r = I \Rightarrow \theta^r(a) = a \Rightarrow a^{p^r} = a \Rightarrow a^{p^{r-1}} = 1$$

$$\Rightarrow O(a)/p^r - 1 \Rightarrow q - 1/p - 1$$

$$\Rightarrow p^n - 1/p^r - 1$$

$$\Rightarrow p^n - 1 \leq p^r - 1 \Rightarrow n \leq r$$

$$\text{Also } \theta^n(b) = b^{p^n} = b \quad \forall b \in F_q \Rightarrow \theta^n = I$$

$$O(\theta) = n \Rightarrow G = \langle \theta \rangle$$

Theorem :

Any two finite fields with the same number of elements p^n are F_p -isomorphic.

Proof :

Let F_1, F_2 be finite fields such that $O(F_1) = p^n = O(F_2)$.

By theorem,

Let F be a finite field of order p^n .

Then F is a minimal splitting field of $x^{p^n} - x$ over F_p .

$\therefore F_1, F_2$ are minimal splitting fields of $f(x) = x^{p^n} - x$ over F_p .

$\Rightarrow F_1, F_2$ are F_p -isomorphic.

By theorem,

Let F be a finite field of order p^n . Then F is a minimal splitting field of $x^{p^n} - x$ over F_p .

Shows that there is unique field of order $q=p^n$ upto an isomorphism.

It is denoted by $GF(p^n)$ or $Gp(q)$ or F_q .

Theorem :

Let F be a finite field of order p^n . Then F is a minimal splitting field over F_p .

Proof :

We can regard F as an extension of F_p .

Let $q = p^n$

Now $F^* = \langle \alpha \rangle$

$$O(\alpha) = O(F^*) = q-1$$

$$\text{Also } \alpha^{q-1} = 1 \Rightarrow \alpha^q = \alpha$$

$\Rightarrow$ elements of F are zeros of $f(x) = x^q - x$ over F_p .

So $f(x)$ splits in F .

$$\therefore f(x) = x(x-\alpha)\dots\dots(x-\alpha^{q-1})$$

$\Rightarrow$ minimal splitting field of f over F_p is $F_p(\alpha, \alpha^2, \dots, \alpha^{m-1}, 1, 0) = F_p(F) = F$

Hence the theorem.

Theorem :

Let F be a field with p^n elements.

Then F has a subfield K with p^m elements iff m divides n .

Proof :

Suppose K is a subfield of F

Then K can be regarded as an extension of F_p such that $[K:F_p] = m$

III^{ly} F can be regarded as an extension of F_p such that $[F:F_p] = n$

$$\text{Now } [F:F_p] = [F:K][K:F_p] \Rightarrow m \text{ divides } n.$$

Conversely,

Let F be a field such that $O(F) = p^n$.

Suppose m/n

Now F is a minimal splitting field of $x^{p^n} - x$ over F_p .

Let $f(x) = x^{p^n} - x$ and $g(x) = x^{p^m} - x$

by problem show that $x^{p^m} - x / x^{p^n} - x$ if m/n .

$$\Rightarrow g(x)/f(x)$$

Consider $F^1 = \{\text{zeros of } g(x) \text{ in } F\}$

Then F^1 is a subfield of F .

Since $g(x)$ has p^m distinct zeros, F^1 is a subfield of F with p^m elements.

If K is another subfield of F such that $O(K) = p^m$.

Then $O(K) = O(F^1) = p^m$.

$$\Rightarrow K, F^1 \text{ are } F_p\text{-isomorphic.}$$

Thus, there is exactly one subfield of F (upto isomorphism) with p^m elements.

This proves the theorem.

Theorem :

Let F be a finite field. Then F^* , the set of non zero element of F forms a cyclic group under multiplication in F .

Proof :

Now F^* is an abelian group under multiplication.

Let $\alpha \in F^*$ be an element of maximum order m .

By lemma, Let G be a finite abelian group under multiplication.

Let $\alpha \in G$ be of maximum order. then $O(\beta)/O(\alpha) \forall \beta \in G$

$$\therefore O(\beta)/m \quad \forall \beta \in F^*$$

$$\begin{aligned} \text{So, } m = O(\beta)r &\Rightarrow \beta^m = \beta^{O(\beta)r} = 1 \quad \forall \beta \in F^* \\ &\Rightarrow \beta \text{ satisfies } x^m - 1 \text{ over } F. \end{aligned}$$

Since F can't have more than m zeros of $x^m - 1$, $O(F^*) \leq m$.

But $\alpha \in F^*$ and $O(\alpha) = m \Rightarrow 1, \alpha, \alpha^2, \dots, \alpha^{m-1}$ are distinct elements of F^* .

$$\Rightarrow O(F^*) \geq m \Rightarrow O(F^*) = m = O(\alpha)$$

$$\Rightarrow F^* = \langle \alpha \rangle$$

The generators of F^* are called primitive elements of F .

Theorem :

Let F be a finite field with $q=p^n$ elements considered as an extension over z_p . Then F is a splitting field of $x^{p^n} - x \in z_p[x]$.

Proof :

$F^* = F - \{0\}$ is a cyclic group of order $q-1$. In particular every $\alpha \in F^*$ satisfies $\alpha^{p^n-1} = 1$, and every element of F satisfies

$$\alpha^{p^n} = \alpha$$

∴ The elements of F are the roots of the polynomial $f(x) = x^{p^n} - x \in z_p[x]$. Since $f(x)$ is a separable polynomial with at most p^n roots.

∴ F has p^n distinct elements. F is a splitting field of $x^{p^n} - x \in z_p[x]$.

Exercises :

- Find the generators of the cyclic group of non-zero elements of the following finite fields.
(i) z_{19} (ii) z_{29}
- Show that $x^{p^n} - x$ is the product of all monic irreducible polynomials in $z_p[x]$ of degree d dividing n .
- Let F be a field of $\text{Char } p > 0$. Give an example to show that the map $a \rightarrow a^p$ need not be an automorphism of F if F is an infinite field.

MODEL QUESTION PAPER

M.Sc. - 1 Year

Paper - I : ALGEBRA

HOURS : 3

MAX. MARKS = 100

PART A

Answer 4 out of 8

(4×10 = 40)

1. (a) Define a group and prove that if $(ab)^2 = a^2b^2$ for all $a, b \in G$ then G is abelian.
(b) H and K are subgroups of a group G , then prove that HK is a subgroup iff $HK = KH$.
2. (a) If H and K are normal subgroups of a group then HK is also a normal subgroup (prove!).
(b) A homomorphism $\phi: G \rightarrow G^1$ is 1-1 iff $\text{Ker } \phi = \{0\}$. Prove!
3. (a) If P is a p -sylow subgroup of a group G then show that $N(N(P)) = N(P)$.
(b) A group G is solvable iff $G^{(K)} = \{e\}$ for some integer K . Prove this!
4. (a) Show that the only ideals of a field are $\{0\}$ & itself.
(b) Define prime and maximal ideals and give one example for each.
5. (a) State and prove the division algorithm in $F[x]$.
(b) State and prove Gauss Lemma.
6. (a) Show that $V_2 + V_3$ is algebraic over $\mathbb{Q}$.
(b) Show that every finite extension is algebraic.
7. (a) Find the splitting field of the polynomial $x^2 + x + 1$ over $\mathbb{Q}[x]$.
(b) If K/F is finite and L/K is finite then prove that L/F is also finite.
8. Show that every finite field is perfect.

PART B

Answer any three

(3×20 = 60)

9. (a) State and prove Lagrange's theorem in the case of finite groups.
(b) A subgroup N of G is normal in G iff $gN = Ng$ for all $g \in G$. (Prove)