Advanced Abstract Algebra

M.A./M.Sc. Mathematics (Previous)
Paper-I

Directorate of Distance Education
Maharshi Dayanand University
ROHTAK – 124 001
## Contents

<table>
<thead>
<tr>
<th>Unit</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unit I</td>
<td>5</td>
</tr>
<tr>
<td>Unit II</td>
<td>49</td>
</tr>
<tr>
<td>Unit III</td>
<td>62</td>
</tr>
<tr>
<td>Unit IV</td>
<td>76</td>
</tr>
<tr>
<td>Unit V</td>
<td>128</td>
</tr>
</tbody>
</table>
ADVANCED ABSTRACT ALGEBRA

Max. Marks : 100
Time : 3 Hours

Note: Question paper will consist of three sections. Section I consisting of one question with ten parts of 2 marks each covering whole of the syllabus shall be compulsory. From Section II, 10 questions from each unit. The candidate will be required to attempt any seven questions each of five marks. Section III, five questions to be set, one from each unit. The candidate will be required to attempt any three questions each of fifteen marks.

Unit I
Groups, Subgroups, Lagrange’s theorem, Normal subgroups, Quotient groups, Homomorphisms, Isomorphism Theorems, Cyclic groups, Permutations, Cayley’s Theorem, Simplicity of $A_n$ for $n \geq 5$.

Unit II

Unit III

Unit IV

Unit V
Normal extensions, Perfect fields, finite fields, algebraically closed fields, Automorphisms of extensions, Galois extensions, Fundamental theorem of Galois theory. Solution of polynomial equations by radicals. Isolvability of the general equation of degree 5 by radicals.
**Unit-I**

**Definition**
A non-empty set of elements $G$ is said to form a **group** if in $G$ there is defined a binary operation, called the product, denoted by $\cdot$, such that:

1. $a, b \in G \Rightarrow a \cdot b \in G$ (closed)
2. $(associative \ \text{law})$
3. $\exists$ an element $e \in G$ such that $a \cdot e = e \cdot a = a$ (the existence of an identity element in $G$)
4. $\exists a^{-1} \in G$ such that $a \cdot a^{-1} = a^{-1} \cdot a = e$ (The existence of an identity element in $G$)

**Example 1:**

Let $G$ be the set of nonsingular $2 \times 2$ matrices over rational numbers $\mathbb{Q}$.

1. Let $a = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$ and $b = \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix}$ be two non-singular $2 \times 2$ matrices over $\mathbb{Q}$.

   Now $a \cdot b$ under matrix multiplication is again $2 \times 2$ matrix over $\mathbb{Q}$ and $\det(a \cdot b) = (\det a) \cdot (\det b) \neq 0$, as $\det a \neq 0$, $\det b \neq 0$.

2. We know that matrix multiplication is always associative. Therefore, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in G$.

3. $\exists e = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in G$ such that $a \cdot e = e \cdot a = a$ for all $a \in G$.

4. If $a \in G$, say $a = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$, then $a^{-1} = \begin{bmatrix} \frac{1}{a_{11}a_{22} - a_{12}a_{21}} & -\frac{a_{12}}{a_{11}a_{22} - a_{12}a_{21}} \\ -\frac{a_{21}}{a_{11}a_{22} - a_{12}a_{21}} & \frac{1}{a_{11}a_{22} - a_{12}a_{21}} \end{bmatrix}$.
\[ a, a^{-1} = a, \quad \frac{1}{2} \text{adj} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = I = e \]

similarly, \[ a^{-1}, a = I = e \]

\[ \therefore a^{-1} \in G \]

Thus \( G \) is a group.

Note that \( a, b \neq b, a \quad \forall a, b \in G \). In fact, let

\[
\begin{pmatrix} 1 & 7 \\ 2 & 3 \end{pmatrix} \neq \begin{pmatrix} 1 & 3 \\ 3 & 1 \end{pmatrix} = b, a
\]

**Definition**

A group \( G \) is said to be abelian (or commutative) if \( a, b = b, a \quad \forall a, b \in G \). Therefore, example 1 gives us a noncommutative group with infinite number of elements in it, since elements are taken from \( Q \), rational numbers which are infinite.

**Definition**

The number of elements in a group \( G \) is called the order of \( G \). Denote it by \( O(G) \). When \( g \) has finite number of elements, \( G \) is called a finite group.

**Example 2:**

\[
G = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}
\]

\[ G \] is again a set of \( 2 \times 2 \) matrices with entries in \( Z \), integers, but containing only four elements.

Let \( e = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, a = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, b = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, c = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \]

we can verify \( a^2 = b^2 = c^2 = e = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = I \),

and \( a b = c = ba, ac = b = ca, bc = a = cb \).

It can be easily verified that \( G \) is a group under matrix multiplication. Thus \( G \) is an abelian group containing four elements only (Note that entries are from \( Z \)).

Therefore, \( G \) is a finite abelian group.

**Remarks:**

In this example every element of \( G \) is its own inverse i.e. \( a = a^{-1}, b = b^{-1}, c = c^{-1}, e = e^{-1} \).
2. In example 1, \[ a = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}, \quad b = \begin{bmatrix} 5 & 6 \\ 7 & 8 \end{bmatrix} \]

Note that \[ a^{-1} b^{-1} = \begin{bmatrix} -3 & -2 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} -4 & -3 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = e. \]

3. In a group \( G \), we can prove that \( (ab)^{-1} = b^{-1}a^{-1} \) \( \forall a, b \in G \),

\[ (ab)^{-1} = a^{-1}b^{-1} = a e = a^{-1} = e \]

Similarly \( (b^{-1}a^{-1})(ab) = e \).

Hence \( (a b)^{-1} = b^{-1}a^{-1} \)

This rule can be extended to the product of \( n \) elements, we note that

\[ b_{n} a_{n-1} a_{n-2} \ldots a_{2} a_{1} \in G, 1 \leq i \leq n \]

**Example 3:**

If every element of a group \( G \) is its own inverse (i.e. \( a^{2} = e \) for all \( a \in G \)), then \( G \) is abelian. We note that

\[ a^{2} \in G \Rightarrow a \in G \Rightarrow a^{2} = e \]

and \( \forall a, b \in G \),

\[ ab = ba, \quad ab \in G \]

\[ = b^{-1}a^{-1} \]

\[ = b \quad a. \]

**Definition:**

A group \( G \) is said to be cyclic if every element of it is a power of some given element in it. This given element is said to generate or a generator of the group \( G \). Thus \( G \) is cyclic if \( \exists a \in G \) such that \( x = a^{n}, n \in \mathbb{Z} \). It is denoted by \( G = \langle a \rangle = \{ a^{n} : n \in \mathbb{Z} \} \)

**Remarks 1:**

A cyclic group is necessarily abelian but the converse is not true.

Let

\[ xy = a^{n} a^{m} = a^{n+m} = a^{m+n} = a^{m} a^{n} = yx \quad \forall x, y \in G. \]

Thus a cyclic group \( G \) is abelian. But example 2 shows that every abelian group is not cyclic. Every element of \( G \) in example 2 can not be written as power of either \( a, b \) or \( c \) in it, verify it.
Problem 1:
Let G be a non-empty set closed under an associative product, which has left identity e and left inverse for all elements of g. Show that G is a group.

Proof:
Let a ∈ G and let b such that ba = e. Now

\[ b \cdot a \cdot b = (b \cdot a) \cdot b = e \cdot b = b \] ........................(i)

such that c \( b = e \)

Hence \( c \cdot (b \cdot a) = c \cdot b = e \) from (i)

\[ \Rightarrow \ b \cdot a \cdot b = e \]

\[ \Rightarrow \ a \cdot b = e \]

\[ \therefore b \] is also right inverse of a.

Further,

\[ a \cdot e = a \cdot (b \cdot a) = (a \cdot b) \cdot a = e \cdot a = a \]

Hence e is right identity also

Thus G is a group.

Subgroups

Let H be a non-empty subset of the group G such that

1. \( a \cdot b \in H \) \( \forall a, b \in H \)

We prove that H is a group with the same law of composition as in G.

Proof:
H is closed under multiplication from (1). All elements of H are from G and associative law holds in G, therefore, multiplication is associative in H also.

Let a \in H, then \( a^{-1} \) from (2) and so from (1), \( a \cdot a^{-1} = e \), i.e. \( e = a \cdot a^{-1} \).

which implies, identity law holds in H, (2) gives inverse law in H. Thus H is a group. H is called a subgroup of G. Thus a nonempty subset of a group G which is a group under the same law of composition is called a subgroup G. Note that e, the identity element G is also the identity of H.

A group G is called nontrivial if G \( \neq \) \( \langle e \rangle \). A nontrivial group has at least two subgroups namely G and \( \langle e \rangle \). Any other subgroup is called a proper subgroup.

Definition:
Let b, a \in G, b is said to be Conjugate of a \in G, if such that \( b = x^{-1} \cdot ax \).

Problems:
1. Let a \in G, let \( C_{G}(a) = \{ x \in G: x^{-1} \cdot ax = a \} \)
   Prove that \( C_{G}(a) \) is a subgroup of G.

2. is a subgroup of G.

3. Find the centre of the group \( GL(2, \mathbb{R}) \) of nonsingular 2 x 2 matrices over real numbers.
Solutions:

1. \( C_g \neq \phi \), because \( e \in C_g(a) \).

   Let \( x, y \in C_g(a) \). Then

   \[
   \begin{align*}
   d^{-1} \cdot d^{-1} &= xax^{-1} \\
   &= x^{-1}ax^{-1} \\
   &= d^{-1}a d^{-1} \\
   &= e \\
   &= a
   \end{align*}
   \]

   \( \Rightarrow x^{-1} \in C_g \) \( \subseteq G \)

2. Let \( x, y \in Z(G) \).

   From above

   \[
   \begin{align*}
   x^{-1}y^{-1} &= x^{-1}ax^{-1} \\
   &= e \\
   &= a
   \end{align*}
   \]

   \( \Rightarrow xy \in C_g \) \( \subseteq G \)

   hence

   Thus \( Z(G) \) is a subgroup.

3. Let \( x = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{centre of } GL(2, \mathbb{R}) \)

   \[
   \begin{align*}
   x &= \begin{pmatrix} a & b \\ c & d \end{pmatrix} \\
   &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\
   &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}
   \end{align*}
   \]

   \( \therefore \) \( x \) commutes with all non-singular 2 x 2 matrices. So in particular \( x \) commutes with
(1) and (2) gives
\[
\begin{pmatrix}
    a & b \\
    c & d \\
\end{pmatrix}
\begin{pmatrix}
    a+b & b+di \\
    c+e & d+fi \\
\end{pmatrix}
\]
Hence \(c = 0, a = d\)

Similarly, gives
\[
\begin{pmatrix}
    a & b \\
    c & d \\
\end{pmatrix}
\begin{pmatrix}
    a & b \\
    c & d \\
\end{pmatrix}
\]

Hence \(b = 0\).

Therefore \[x = \begin{pmatrix}
    a & 0 \\
    0 & a \\
\end{pmatrix}
\text{ where } a \neq 0, a \in R\]

is a scalar matrix and so commutes with all 2 x 2 matrices, (nonsingular or not) Hence \(Z(GL(Z, R))\), the center of \(GL(2, R)\) Consists of all nonzero scalar matrices.

**Remark:**

This can be generalised that the center of \(GL (n, R)\), the general linear group of nonsingular \(n \times n\) matrices over \(IR\), consists of all nonzero scalar matrices.

**Coset of a subgroup H in G:**

Let \(G\) be a group and \(H\) be a subgroup of \(G\). For any \(a \in G\), \(Ha = \{ha / h \in H\}\). This set is called right coset of \(H\) in \(G\). As \(e \in H\), so \(a = e \cdot a \in Ha\). Similarly \(aH = \{ah / a \in H\}\) is called left coset of \(H\) in \(G\), containing \(a\).

**Some simple but basic results of Cosets:**

Lemma 1: Let \(H\) be a subgroup of \(G\) and let \(a, b \in G\).

Then
1. \(a \in Ha\)
2. \(Ha = H \iff a \in H\)
3. Either two right cosets are same or disjoint i.e. \(Ha = Hb\) or
4. \(Ha = Hb \iff b = a^{-1} \in H\)
5. i.e. there is one-one correspondence between two right Cosets

**Proof:**

1. \(a = ea \in Ha \quad \exists e \in H\)
2. Let \(, \text{ Now } h \quad \text{ due to closure in } H\).
UNIT-I

1. Let H be any element of H. Since H, we get a⁻¹ and h a⁻¹. Hence h = he = h (a⁻¹ a)
   = (h a⁻¹)a. So. Thus H = Ha.

3. Suppose Ha € Hb let x € Ha Hb

   Then x = h₁ a and x = h₂ b, for some h₁, h₂ € H.

   Thus

   Ha = H e a € H, a € H.

4. Ha = Hb ⇔ H = Hba⁻¹ ⇔ b a⁻¹ ∈ H, from (2)

5. Define f: Ha → Hb by ha → hb ∀ h ∈ H.

   ∴ f is one-one. By definition it is obvious that f is onto.

   We again visit example 2, G = {e, a, b, c}

   There are three proper subgroups of G, H₁ = {e, a}, H₂ = {e, b}, H₃ = {e, c}

   order of each Hᵢ, i = 1, 2, 3, is 2. Hence O (Hᵢ) | O (G) = 4, i.e., /Hi/ divides /G/.

   Now we are ready to prove a theorem called Lagrange’s Theorem.

   Theorem 1. Lagrange’s Theorem (1770): /H/ divides |G|.

   If G is a finite group and H is a subgroup of G, then /H/ divides /G/. Moreover, the number of distinct right left

   cosets of H in G is

   Proof:

   Since G is a finite group, we have finite number of distinct right cosets of H in G, say Ha₁, Ha₂,............., Haᵢ.

   Now for each a in G, We have Ha = Haᵢ for some i. By property (i) of Lemma 1, a ∈ Ha. Hence, each element of G belongs to one of Cosets Haᵢ, i.e.

   By property (3) of lemma 1,

   Haᵢ ∩ Haⱼ = φ,

   for i ≠ j.

   ∴ |G| = |Ha₁| + |Ha₂| +...|Haᵢ| for each i.

   (Because f: H → Haᵢ defined by h → haᵢ is one-one & onto).
Therefore we get
\[ |G| = |H| + |H| + \ldots + |H| \]
\[ \text{i.e. } |G| = r|H| \]

**Warning:**
Let \( G \) be a finite group of order 12. We may think that it has subgraps of order 12, 6, 4, 3, 2, 1 but no others. Converse of Lagrange's theorem is false. 6|12 but there exists a group of order 12 which does not have a subgroup of order 6. We shall give this example some time later.

The number of right (or left) cosets of a subgroup \( H \) in a group \( G \) is called the **index** of a subgroup \( H \) in the group \( G \). This number is denoted by \( |G:H| \). When \( G \) is finite, by Lagrange's theorem, we have \( |G:H| = \frac{|G|}{|H|} \).

We can say:
\[ |G| = |H| \times \text{index of } H \text{ in } G. \]

**Corollary 1:**
\[ |a| \text{divides } |G| \]
In a finite group, the order of each element of the group divides the order of the group.

**Proof:**
\[ |a| = 0 \implies a \neq e \text{ and } G \text{ is prime. Hence the corollary.} \]

**Corollary 2:**
Groups of Prime order are cyclic.

**Proof:**
\[ a^{\text{order of } G} = 1 \quad \text{and } G \text{ is prime. Hence } a^{\text{order of } G} = |G| \]
Therefore \( \langle a \rangle \leq G \Rightarrow G = \langle a \rangle \text{ i.e., } G \text{ is cyclic.} \)

**Corollary 3:**
\[ a^{|G|} = e. \]
Let \( G \) be a finite group, and let \( a \in G \). Then

**Proof:**
\[ |G| = |a|n, \text{ } n \text{ is a positive integer, by Corollary 1.} \]

\[ \text{Hence } a^{|G|} = a^{|H|n} = e^n = e \]

Corollary 4: (Fermat’s Little Theorem):
For every integer $a$ and every prime $p$, $a^p \equiv a \pmod{p}$.

Proof:
By division algorithm, $a = pm + r$, $0 \leq r < p$. Hence
$a \equiv r \pmod{p}$. The result will be proved if we prove $r^p \equiv r \pmod{p}$. If $r = 0$, the result is trivial. Hence
which forms a group under multiplication module $o$ $p$. Therefore by corollary 3,
$r^{p-1} = 1$. Thus $r^p \equiv r \pmod{p}$.

Normal Subgroups
If $G$ is a group and $H$ is a subgroup of $G$, it is not always true that $aH = Ha$,

Definition:
A subgroup $H$ of a group $G$ is called a normal subgroup of $G$ if $aH = Ha$ for every $a$ in $G$. This is denoted by $H \triangleleft G$.

Warning:
$H \triangleleft G$ does not indicate $ah = ha$

$H \triangleleft G$ means that if , then $\exists$ some $h_1 \in H$ such that

A subgroup $H$ of $G$ is normal in $G$ if and only if $\forall x \in G$,

$\forall a \in G$.

Factor Groups (or Quotient Groups):
Let $H \triangleleft G$. The set of right (or left) cosets of $H$ in $G$ is itself a group. This group is called the factor group of $G$ by $H$ (or the quotient group of $G$ by $H$).

Theorem 2:
Let $G$ be a group and $H$ a normal subgroup of $G$. The set $G/H = \{Ha \mid a \in G\}$ forms a group under the operation $(Ha)(Hb) = Hab$.

Proof:
We claim that the operation is well defined. Let $Ha = Ha_1$ and $Hb = Hb_1$.

Then $a_1 = h_1a$ and $b_1 = h_2b$, $h_1, h_2 \in H$.

Therefore, $Ha_1b_1 = Hh_1a_1h_2b = Ha_1h_2b = aHh_2b = aHb = Hab$

(In proving this we used $Ha = H$ and $H \triangleleft G$).

Further $He = H$ is the identity and $Ha^{-1}$ is the inverse of $Ha$, $\forall a \in G$.

$(Ha)(He) = Hae = Ha$, and $HaH^{-1} = Ha^{-1} = He = H$.
Thus is a group.

**Theorem 3: Theorem.**

Let $G$ be a group and let $Z(G)$ be the center of $G$. If is cyclic, then $G$ is abelian.

**Proof:**

we claim we show that $g^{-1}Z \subseteq Z g \subseteq g G$, $g \in G$.

let $x \in Z$ then

$$g^{-1}xg = g^{-1}g x = x \in Z$$

Hence $g^{-1}xg \in Z g \subseteq g G$, $\forall x \in Z$.

Therefore, $g^{-1}Z \subseteq Z g \subseteq g G$.

We can now form a factor group

Let $G/Z \cong \langle x/1, y/1, g/1 \rangle$ is cyclic.

Let $a, b \in G$. To show $ab = ba$

hence

$$a Z \cong x^n Z, \quad b Z \cong x^m Z$$

and $b Z \cong x^m Z, \quad a \cong x^n Z$, where $n, m$ are integers.

Thus $a \in a Z \Rightarrow a = x^n y$ for some $y \in Z$.

and $b = x^m t$ for some $t \in Z$.

Now

$$= b a$$

We often use it as: If $G$ is not abelian, then is not cyclic.
Definition: Group Homomorphism
Let \( f \) be a mapping from a group \( G \) to a group \( G \) defined by
\[
f(a, b) = f(a) f(b), \quad a, b \in G.
\]
\( f \) is called homomorphism of groups.

Definition: Kernel of a Homomorphism
Let \( f : G \rightarrow G \) be a group homomorphism and \( e \) be the identity of \( G \). Then Kernel of \( f \) denoted by \( \ker f \) is defined by
\[
\ker f = \{ x \in G : f(x) = e \}.
\]
We note that \( \ker f \subseteq G \). (It is easy to show that \( \ker f \) is a subgroup of \( G \))

Let \( x \) be any element of \( \ker f \). Then
\[
f(x^{-1}) f(x) = f(x f(x^{-1})) = f(e) = e
\]
( Any homomorphism of groups carries identity of \( G \) to identity of \( \overline{G} \) )

Explanation:
\[
f(x e) = f(x) f(e) \in \overline{G}
\]
So by cancellation property in \( \overline{G} \), we have \( e = (e) \).

Hence
\[
\Rightarrow g^{-1} x g \in \ker f \forall g \in G, \forall x \in \ker f \Rightarrow \ker f \overline{G}.
\]
Lemma 2:

Let be a homomorphism of $G$ into $G$, then

1. $(e) = e$, the identify element of $G$.

2. $f(x^n) = (f(x))^n \forall x \in G$

Proof:

(1) is proved above

(2) $\varepsilon = f(b^{-1} \cdot d \cdot x^{-1} \cdot i = f(b \cdot g \cdot d \cdot i)$

$\Rightarrow (f(x))^{-1} \varepsilon = (f(x))^{-1} f(x) f(x^{-1}) \text{ in } G$

$\Rightarrow (f(x))^{-1} = \varepsilon f(x^{-1}) = f(x^{-1}) \forall x \in G$

Example 4:

$G = \text{GL}(2, R)$; group of nonsingular $2 \times 2$ matrices over reals and $R^*$ be the group of nonzero real number under multiplication. Then

$f: G = \text{GL}(2, R) \longrightarrow R^*$ defined by

$A \quad (A) = \det A$

Then $(AB) = \det(AB) = \det A \det B = (A) (B)$

Hence is a homomorphism

$\iff A \in \text{SL}(2, R)$, the group of nonsingular $2 \times 2$ matrices over $R$, whose determinant is 1. Therefore, $\ker f$

Theorem 4: (Fundamental Theorem of Group Homomorphism)

Let $G$ be a group homomorphism with $K = \ker f$. Then

$G/K \cong f(G)$

i.e. $G/\ker(f) \cong \text{Image}(f)$

($\cong$: Isomorphic, when is homomorphism, 1–1 and onto).
**Proof:**
Consider the diagram

\[
\begin{array}{ccc}
G & \xrightarrow{f} & \tilde{G} \\
\downarrow & \searrow & \downarrow \\
K & \xrightarrow{f} & G/K
\end{array}
\]

where

The above diagram should be completed to

\[
\begin{array}{ccc}
G & \xrightarrow{f} & \tilde{G} \\
\downarrow & \searrow & \downarrow \\
K & \xrightarrow{f} & G/K
\end{array}
\]

We shall use

\[
\begin{array}{ccc}
Kg & \xrightarrow{f} & Kf \\
\downarrow & \searrow & \downarrow \\
Kg & \xrightarrow{f} & Kf
\end{array}
\]

to complete the previous diagram.

Define \( \tilde{f}(Kg) = f(g), \quad \forall \text{ coset } Kg \in \overline{G/K} \)

\( \tilde{f} \) is well defined: Let \( Kg = Kg_1, g_1, g_2 \in G \)

Then \( g_1 = kg_2, k \in \ker \tilde{f} = K \), and

\[
f(g_1) = f(kg_2) = f(k)f(g_2) = \tilde{f}(g_2) = f(g_2)
\]

is a homomorphism since

\[
\tilde{f}(Kg_1 Kg_2) = \tilde{f}(Kg_1 g_2) = f(g_1, g_2) = f(g_1)f(g_2)
\]

(\( \Theta \) \( f \) is a homomorphism).
\[ f \] is 1–1 since \( f(\begin{pmatrix} g_1 & \cdot & \cdot \\ \cdot & g_2 & \cdot \\ \cdot & \cdot & \cdot \end{pmatrix}) = f(\begin{pmatrix} g_1 & \cdot & \cdot \\ \cdot & g_2 & \cdot \\ \cdot & \cdot & \cdot \end{pmatrix}) \Rightarrow f(g_1) = f(g_2) \), hence \( f(g_1) f(g_2)^{-1} = e \) and \( f(g_1^{-1} g_2) = e \) (\( \Theta \bar{f} \) is a homo).

So \( g_1 g_2^{-1} \in K = \ker f \), which shows that \( kg_1 = kg_2 \). Thus \( f \) is 1–1. By definition \( \bar{f} \) is onto. Hence \( \bar{f} \) is homomorphism. So \( \frac{G}{K} \cong f(G) \subseteq G \).

**Consider Again Example 4:**

\[ f : GL_n(R) = GL(n,R) \rightarrow R^* \]

A

\[ f(AB) = \det(AB) = \det(A) \det(B) \]

So \( f \) is a homomorphism.

the identity of \( R^* \).

\[ \iff A \in SL_n(R) = SL(n,R), \text{the subgroup of } \text{of all } n \times n \text{ matrices with determinant 1}. \]

By above fundamental homomorphism theorem, we get

\[ \frac{GL(n,R)}{\ker f} \cong \text{Im}(f) \]

i.e \( \frac{GL(n,R)}{SL(n,R)} \cong \text{Im}(f) \)

But \( f \) is onto, since for

\[ A = \begin{pmatrix} a_{11} & \cdot & \cdot \\ \cdot & \ddots & \cdot \\ \cdot & \cdot & a_{nn} \end{pmatrix} \in GL(n,R) \text{ such that } f(A) = \det A = a \]

Hence \( \frac{GL(n,R)}{SL(n,R)} \cong R^* \)

**Theorem 5 (First Isomorphism Theorem)**

Let \( G \) be a group with normal subgroup \( N \) and \( H \) such that \( N \subseteq H \)

Then and
Define \( f : \frac{G}{N} \rightarrow H \) by

\[ N a \mapsto H a \]

is well-defined, since \( Na = Nb \) for we get . Since \( N \subseteq H \), thus gives and so

\( Ha = Hb \). \( f \) is a homomorphism:

the identity of

\[ a \in H \]

Hence ker . As ker \( f \triangleq \frac{G}{N} \), so \( \frac{H}{N} \triangleq \frac{G}{N} \).

The fundamental homomorphism theorem for groups implies that

\[ \frac{G}{N} \]

\[ \ker f \equiv \text{Im} f = \frac{G}{N} \]

\[ \frac{H \cap N}{N} \]

\[ H \equiv \frac{G}{N} \]

\[ a \in H \cap N \]

**Theorem 6 (Second Isomorphism Theorem)**

Let \( G \) be a group, and let \( N \triangleq G \), let \( H \) be any subgroup of \( G \). Then \( HN \) is a subgroup of \( G \), and

**Proof:**

Define \( f : H \rightarrow N \) by a \( \mapsto \)

is a homomorphism since

\[ a \in \ker f \iff f(a) = N \], the identity element of \( HN \) and a \( H \)

So
The arbitrary element of $\frac{HN}{N}$ is $NaN$ but $a \in H \subseteq G$ and $aNa = Na$, hence $NaN = NNa = Na$.

Therefore, $f$ is onto. Now by fundamental homomorphism theorem for groups, we get

\[ \frac{H}{H \cap N} \cong \frac{HN}{N} \]

Some results about cyclic groups: we prove the following results:

**Theorem 7:**

Let $g$ be a cyclic group

1. If $G$ is infinite, then $G \cong \mathbb{Z}$

2. If $G$ is finite with $n$ elements, then $G \cong \mathbb{Z}/\langle n \rangle$

**Proof:**

1. Let $g = \langle a \rangle$ be infinite cyclic group.

Define $f : \mathbb{Z} \rightarrow g$ by $n$.

$f$ is a homomorphism, since

$f$ is onto: since $G = \langle a \rangle$, so for any $x = a^n$ for some integer $m$,

Hence $f(m) = a^n = x \Rightarrow f$ is onto $f$ is 1–1: Let $m \equiv n$, with $f$ is onto, since $G = \langle a \rangle$.

Then multiplying by $a^{-m} = e$ and since $a$ is not of finite order, we must have $m = n$.

Hence every infinite cyclic group is isomorphic to additive group of integers.

2. Let $G$ be a finite group with $n$ elements,

Define $f : \mathbb{Z}/\langle n \rangle \rightarrow G$ by $[m]$.

$f$ is well-defined. We should show that if $a^k = a^m \Rightarrow a^{k-m} = e \Rightarrow n|k-m \Rightarrow k \equiv m \pmod{n}$.

$f$ is onto, since $G = \langle a \rangle$.

is 1–1: let then as above Then as above

Also

$\therefore f$ is an isomorphism. Hence every finite cyclic group of order $n$ is isomorphic to additive group of integers module $n$. 
**Theorem 8.** Let $H$ be a subgroup of a cyclic group $<a>$ and $m$ is the least positive integer such that $a^m \in H$. If $a^n \in H$, then $m|n$.

**Proof.** By division algorithm, we have

$$n = qm + r, \ q, r \in \mathbb{Z}, \ 0 \leq r < m$$

Therefore,

$$a^r = a^{qm+r} = a^q(a^m)^r$$

$$= a^n (a^m)^{-1} \in H$$

Hence $r = 0$, otherwise it will contradict the fact that $m$ is the least positive integer such that $a^m \in H$. Therefore

$$n = q^m$$

and so $m|n$. This completes the proof.

Let $G = <a>$ be a cyclic group generated by $a$. Then $a^{-1}$ will also be a generator of $G$. In fact, if $a^m \in G$, $m \in \mathbb{Z}$, then

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

The question arises which of the elements of $G$ other than a and $a^{-1}$ can be a generator of $G$. We consider the following two cases:

(i) $G$ is an infinite cyclic group
(ii) $G$ is a finite group.

We discuss these cases in the form of the following theorems:

**Theorem 9.** An infinite cyclic group has exactly two generators.

**Proof.** Let $a$ be a generator of an infinite cyclic group $G$. Then $a$ is of infinite order and

$$G = \{ \ldots, a^{-r}, \ldots, a^{-1}, e, a, a^2, \ldots \}$$

Let $a^t \in G$ be another generator of $G$, then

$$G = \{ \ldots, a^{-2t}, a^{-1}, e, a^t, a^{2t}, \ldots \}.$$ 

Since $a^{t+1} \in G$, therefore

$$a^{t+1} = a^n$$

for some integer $r$.

Since $G$ is infinite, this implies

$$t+1 = rt$$

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

which holds only if $t = 1 \pm 1$. Hence there exist only two generators $a$ and $a^{-1}$ of an infinite cyclic group $<a>$.

**Theorem 10.** Let $G = <a>$ be a cyclic group of order $n$. Then $a^m \in G$, $m \leq n$ is a generator of $G$ if and only if $\gcd(m, n) = 1$.

**Proof.** Let $H$ be a subgroup of $G$ generated by $a^m (m \leq n)$. If $\gcd(m, n) = 1$, then there exist two integers $u, v$ such that

$$um + vn = 1$$

$$\Rightarrow a^{um+vn} = a$$

$$\Rightarrow a^m . a^v = a$$

$$\Rightarrow (a^m)(a^n)^v = a$$

$$\Rightarrow (a^m)^u = a \ (\Theta (a^n)^v = e)$$

$$\Rightarrow a \in H (\Theta (a^m)^u \in H)$$

$$\Rightarrow G \subseteq H.$$ 

But, by supposition, $H \subseteq G$.

Hence $G = H = <a^m>$, that is, $a^m$ is a generator of $G$.

Conversely, let $a^m (m \leq n)$ be a generator of $G$. Then

$$G = \{ a^{mn} : n \in \mathbb{Z} \}.$$ 

Therefore, we can find an integer $u$ such that
\[ a^{\mu} = a \]
\[ a^{\mu - 1} = e \]
\[ \Rightarrow \quad O(a) \mid (\mu - 1) \]
\[ \Rightarrow \quad n \mid (\mu - 1) \]

Hence, there exists an integer \( v \) such that
\[ nv = \mu - 1 \]
\[ \Rightarrow \quad \mu - nv = 1 \]
\[ \Rightarrow \quad \gcd(m, n) = 1 . \]

This completes the proof of the theorem.

**Theorem 11.** Every subgroup \( H \) of a cyclic group \( G \) is cyclic.

**Proof.** If \( H = \{ e \} \), then \( H \) is obviously cyclic. So, let us suppose that \( H \neq \{ e \} \). If \( a^\lambda \in H \), then \( a^\lambda \in H \).

So, we can find a smallest positive integer \( m \) such that \( a^m \in H \). Therefore
\[ < a^m > \subseteq H \quad \text{(i)} \]

Moreover,
\[ a^\lambda \in H \Rightarrow \lambda = qm, \ q \in \mathbb{Z} \]

Therefore
\[ a^\lambda = a^{qm} \]
\[ = (q^m)^d \in < a^m > \]
\[ \Rightarrow \quad < a^\lambda > \subseteq < a^m > \]
\[ \Rightarrow \quad H \subseteq < a^m > \quad \text{(ii)} \]

It follows from (i) and (ii) that
\[ H = < a^m > \]
And hence \( H \) is cyclic.

**Theorem 12.** Let \( G = < a > \) be a cyclic group of order \( n \) and \( H \) be a subgroup of \( G \) generated by \( a^m \), \( m \leq n \). Then
\[ O(H) = \frac{n}{\gcd(m, n)} \]

**Proof.** We are given that
\[ H = < a^m > \]

Let \( \gcd(m, n) = d \), then we can find an integer \( q \) such that
\[ m = qd \]
\[ \Rightarrow \quad a^m = a^{qd} \]

But \( a^{qd} \in < a^d > \), where \( < a^d > \) is a subgroup generated by \( a^d \). Therefore
\[ a^m \in < a^d > \]
\[ \Rightarrow \quad H = < a^m > \subseteq < a^d > \quad \text{... (i)} \]

Since \( \gcd(m, n) = d \), we can find \( u, v \in \mathbb{Z} \) such that
\[ d = un + vm \]
\[ \Rightarrow \quad a^d = a^{un + vm} \]
\[ = a^{un} \cdot a^{vm} \]
\[ = a^{vm} (\Theta a^{un} = e) \]

But \( a^{vm} \in < a^m > = H \). Therefore
\[ a^d \in H \]
\[ \Rightarrow \quad < a^d > \subseteq H \quad \text{... (ii)} \]
From (i) and (ii), we have
\[ H = \langle a^d \rangle \]
\[ \Rightarrow O(H) = O(\langle a^d \rangle) \]

But
\[ O(\langle a^d \rangle) = \frac{n}{d} \quad (\Theta(a^d) \frac{n}{d} = e) \]

Hence
\[ O(H) = \frac{n}{\gcd(m,n)} , \]
which completes the proof of the theorem.

**Theorem 13.** Any two cyclic groups of the same order are isomorphic.

**Proof.** Let G and H be two cyclic groups of the same order. Consider the mapping
\[ f : G \rightarrow H \]
defined by
\[ f(a^r) = b^r \]
Then f is clearly an homomorphism. Also,
\[ f(a^r) = f(a^s) \Rightarrow b^r = b^s , \]
If G and H are of infinite order, then
\[ r = s \]
and so \( a^r = a^s \).
If their order is finite, say n, then
\[ B^r = b^s \Rightarrow b^{r-s} = e \]
\[ \Rightarrow n \mid (r-s) \]
\[ \Rightarrow nu = r-s , \quad u \in Z \]
\[ \Rightarrow a^{r-s} = a^{nu} \]
\[ = (a^n)^u = e \]
\[ \Rightarrow a^r = a^s . \]
Hence f is 1–1 mapping also. Therefore, \( G \cong H \).

**Theorem 14.** Every isomorphic image of a cyclic group is again cyclic.

**Proof.** Let \( G = \langle a \rangle \) be a cyclic group and let H be its image under isomorphism f. The elements of G are given by
\[ G = \{ \ldots , a^{-r} , \ldots , a^{-3} , a^{-2} , a^{-1} , a , a^2 , a^3 , \ldots , a^r , \ldots \} \]
Let be an arbitrary element of H. Since H is isomorphic image of G, there exists \( a^r \in G, r = 0, 1, \ldots \) Such that \( b = f(a^r) \). Since f is homomorphism, we have
\[ b = f(a)f(b)f(\ldots f(c))^r \]
\[ = (f(a))^r \]
Thus H is generated by f(a) and hence is cyclic.
Permutations:

Let $S$ be a non-empty set. A permutation of a set $S$ is a function from $S$ to $S$ which is both one-to-one and onto.

A permutation group of a set $S$ is a set of permutations of $S$ that forms a group under function composition.

Example 5:

Let

Define a permutation $\sigma$ by

This 1–1 and onto mapping can be written as

Define another permutation

$\phi(1) = 3, \phi(3) = 2, \phi(2) = 1, \phi(4) = 4$

Then

The multiplication is from right to left.

We see $(\phi \sigma)(1) = \phi(\sigma(1)) = \phi(2) = 1$, and

Example 6: Symetric Groups

Let $S_3$ denote the set of all one-to-one function from {1, 2, 3} to itself. Then $S_3$ is a group of six elements, under composition of mappings. These six elements are

$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \alpha^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$
Note that $\alpha \beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \beta \alpha$

Hence $S_3$, the group of 6 elements, called symmetric group which is non-abelian. This is the smallest finite non-abelian group, since groups of order 1, 2, 3, 5 are of prime order, hence cyclic and, therefore, they are abelian. A group of order 4 is of two types up to isomorphism, either cyclic or Klein 4-group, given in example 2.

**Cycle Notation**

Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 1 & 6 & 5 & 2 \end{pmatrix}$

This can be seen as:

In cycle notation $\sigma$ can be written as

Therefore from example 6:

It has 4 proper subgroups:

and

so $A_3$ is a subgroup of $S_3$ of index 2. It can be easily verified that $A_3 \triangleleft S_3$. In fact, it can be generalised, that every subgroup of index 2 is a normal subgroup in its parent group. is called alternating group.
Example. Let

\[
\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \text{and} \quad \beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}
\]

be two permutations belonging to \( S_3 \). Then

\[
\alpha \circ \beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}
\]

\[
= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}
\]

and

\[
\beta \circ \alpha = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}
\]

Thus \( \alpha \circ \beta = \beta \circ \alpha \). Hence \( \alpha \) and \( \beta \) commute with each other.

But the **composition of permutations is not always commutative**. For example, if we consider

\[
\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}
\]

then

\[
\beta \circ \alpha = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}
\]

and

\[
\alpha \circ \beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}
\]

Hence

\( \alpha \circ \beta \neq \beta \circ \alpha \).

**Definition.** Let \( S \) be a finite set, \( x \in S \) and \( \alpha \in S_n \). The **\( \alpha \) fixes \( x \)** if \( \alpha(x) = x \) otherwise \( \alpha \) moves \( x \).

**Definition.** Let \( S = \{x_1, x_2, \ldots, x_n\} \) be a finite set. If \( \sigma \in S_n \) is such that

\[
\sigma(x_i) = x_{i+1}, \quad i = 1,2,\ldots, k-1
\]

\[
\sigma(x_k) = x_1
\]

and

\[
\sigma(x_j) = x_j, \quad j \neq 1, \ 2,\ldots, k;
\]

then \( \sigma \) is called a **cycle of length \( k \)**. We denote this cycle by

\[
\sigma = (x_1x_2\ldots x_k)
\]

Thus, the **length of a cycle is the number of objects permuted**.

For example, \( \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix} \in S_3 \) is a cyclic permutation because

\[
f(a) = b, \quad f(b) = c, \quad f(c) = a.
\]
In this case the length of the cycle is 3. We can denote this permutation by \((a \ b \ c)\).

**Definition.** A cyclic permutation of length 2 is called a **Transposition**.

For example, \(\begin{pmatrix}1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}\) is a transposition.

**Definition.** Two cycles are said to be disjoint if they have no object in common.

**Definition.** Two permutations \(\alpha, \beta \in S_n\) are called disjoint if
\[
\alpha(x) = x \Rightarrow \beta(x) \neq x \\
\alpha(x) \neq x \Rightarrow \beta(x) = x
\]
for all \(x \in S\).

In other words, \(\alpha\) and \(\beta\) are disjoint if every \(x \in S\) moved by one permutation is fixed by the other.

Further, if \(\alpha\) and \(\beta\) are disjoint permutations, then \(\alpha\beta = \beta\alpha\). For example, if we consider
\[
\alpha = \begin{pmatrix}1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \beta = \begin{pmatrix}1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}
\]
then \(\alpha\beta = \beta\alpha\).

**Definition.** A permutation \(\alpha \in S_n\) is said to be regular if either it is the identity permutation or it has no fixed point and is the product of disjoint cycles of the same length.

For example,
\[
\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 5 & 6 & 4 \end{pmatrix} = (1 \ 2 \ 3)(4 \ 5 \ 6)
\]
is a regular permutation.

**Theorem 15.** Every permutation can be expressed as a product of pairwise disjoint cycles.

**Proof.** Let \(S = \{x_1, x_2, \ldots, x_n\}\) be a finite set having \(n\) elements and \(f \in S_n\). If \(f\) is already a cycle, we are through. So, let us suppose that \(f\) is not a cycle. We shall prove this theorem by induction on \(n\).

If \(n = 1\), the result is obvious. Let the theorem be true for a permutation of a set having less than \(n\) elements. Then there exists a positive integer \(k < n\) and distinct elements \(y_1, y_2, \ldots, y_k\) in \(\{x_1, x_2, \ldots, x_n\}\) such that
\[
f(y_1) = y_2 \\
f(y_2) = y_3 \\
\ldots \\
\ldots \\
f(y_{k-1}) = y_k \\
f(y_k) = y_1
\]
Therefore \((y_1, y_2, \ldots, y_k)\) is a cycle of length \(k\). Next, let \(g\) be the restriction of \(f\) to
\[
T = \{x_1, x_2, \ldots, x_n\} - \{y_1, y_2, \ldots, y_k\}
\]
Then \(g\) is a permutation of the set \(T\) containing \(n-k\) elements. Therefore, by induction hypothesis,
\[
g = \alpha_1 \alpha_2 \ldots \alpha_m,
\]
where \(\alpha_1, \alpha_2, \ldots, \alpha_m\) are pairwise disjoint cycles. But
\[ f = (y_1 \ldots y_k) \circ g = (y_1 \ldots y_k) \alpha_1 \alpha_2 \ldots \alpha_m \]

Hence, every permutation can be expressed as a composite of disjoint cycles.

For example, let
\[
\begin{pmatrix}
1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\
6 & 4 & 7 & 2 & 5 & 1 & 8 & 9 & 3 
\end{pmatrix}
\]
be a permutation. Here 5 is a fixed element. Therefore, \((5)\) is a cycle of length 1. Cycles of length 2 are \((1 \ 6)\) and \((2 \ 4)\) whereas \((3 \ 7 \ 8 \ 9)\) is a cycle of length 4. Hence
\[
f = (5) \ (1 \ 6) \ (2 \ 4) \ (3 \ 7 \ 8 \ 9)
\]

**Theorem 16.** Symmetric group \(S_n\) is generated by transpositions, i.e., every permutation in \(S_n\) is a product of transpositions.

**Proof.** We have proved above that every permutation can be expressed as the composition of disjoint cycles. Consider the \(m\)-cycle \((x_1, x_2, \ldots, x_m)\). A simple computation shows that
\[
(x_1 x_2 \ldots x_m) = (x_1 x_m) \ldots (x_1 x_3) (x_1 x_2),
\]
that is, every cycle can be expressed as a product of transposition. Hence every permutation \(\alpha \in S_n\) can be expressed as a product of transpositions.

**Remark.** The above decomposition of a cycle as the product of transposition is not unique. For example,
\[
(1 \ 2 \ 3) = (1 \ 3) \ (1 \ 2) = (3 \ 2) (3 \ 1)
\]
However, it can be proved that the number of factors in the expression is always **even** or always **odd**.

**Definition.** A permutation is called **even** if it is a product of an even number of transpositions.

Similarly, a permutation is called **odd** if it is a product of odd number of transpositions.

Further,
(i) The product of two even permutations is even.
(ii) The product of two odd permutations is even.
(iii) The product of one odd and one even permutation is odd.
(iv) The inverse of an even permutation is an even permutation.

**Theorem 17.** If a permutation is expressed as a product of transpositions, then the number of transpositions is either even in both cases or odd in both cases.

**Proof.** Let a permutation \(\sigma\) be expressed as the product of transpositions as given below:
\[
\sigma = \alpha_1 \alpha_2 \ldots \alpha_r = \beta_1 \beta_2 \ldots \beta_s
\]
This yields
\[
e = \alpha_1 \alpha_2 \ldots \alpha_r \beta_s^{-1} \beta_{r+1}^{-1} \\
= \alpha_1 \alpha_2 \ldots \alpha_r \beta_s \beta_{s-1} \ldots \beta_2 \beta_1,
\]
since inverse of transposition is the transposition itself. The left side, that is, identity permutation is even and therefore the right hand should also be an even permutation. Thus \(r+s\) is even which is possible if \(r\) and \(s\) are both even or both odd. This completes the proof of the theorem.
Theorem 18. The set of all even permutations in $S_n$ is a normal subgroup. Further $O(A_n) = \frac{|n|}{2}$.

Proof. Let $A_n$ be the subset of $S_n$ consisting of all even permutations. Since
(i) the product of two even permutations is an even permutation.
(ii) the inverse of an even permutation is an even permutation,
it follows that $A_n$ is a subgroup of $S_n$.

To prove that $A_n$ is a normal subgroup of $S_n$, we proceed as follows:
Let $W$ be the group of real numbers 1 and $-1$ under multiplication. Define
$$f : S_n \rightarrow W$$
by
$$f(\alpha) = 1 \quad \text{if } \alpha \text{ is an even permutation}$$
$$f(\alpha) = -1 \quad \text{if } \alpha \text{ is odd permutation}$$
Then it can be verified that $f$ is homomorphism of $S_n$ of $W$. The kernel (null space) of $f$ is given by
$$K = \{ \alpha \in S_n : f(\alpha) = eW = 1 \}$$
$$= \{ \alpha \in S_n : f(\alpha) = 1 \}$$
$$= \{ \alpha : \alpha \text{ is even} \}$$
$$= A_n .$$
Thus $A_n$, being the kernel of a homomorphism is a normal subgroup of $S_n$.
Moreover, by Isomorphism Theorem,
$$\frac{S_n}{A_n} \cong W.$$ 
Therefore,
$$O(W) = O\left( \frac{S_n}{A_n} \right)$$
$$= \frac{O(S_n)}{O(A_n)}$$
But $O(W) = 2$, therefore,
$$2 = \frac{O(S_n)}{O(A_n)}$$
or
$$O(A_n) = \frac{O(S_n)}{2} = \frac{|n|}{2}$$
This completes the proof of the theorem.

Definition. The normal subgroup of $A_n$ formed by all even permutation in $S_n$ is called the Alternating Group of degree $n$.

We have shown above that order of $A_n$ is $\frac{|n|}{2}$. 
Theorem 19:
Cayley’s Theorem
Every finite group is isomorphic to a group of permutations.

Proof:
Let \( G \) be any group. We must get a group \( G \) of permutations such that it is isomorphic to \( G \).
For any \( g \) in \( G \), Define a function

\[
\phi_g(x) = g^{-1}x 
\]

Claim: \( \phi_g \) is a permutation on \( G \).
\( \phi_g \) onto: Let \( x \) be any element of \( G \). So \( \exists g^{-1}x \in G \) such that

\[
\phi_g(g^{-1}x) = g(g^{-1}x) = (gg^{-1})x = x.
\]

\( \phi_g \) is one-one:
Let \( \phi_g(x) = \phi_g(y) \) so \( gx = gy \); hence

\[
x = y.
\]

Now, Let

Claim:

is a group of permutations under composition of mappings.

\[
= g(hx)
\]

Hence \( \phi_g \phi_h = \phi_{gh} \forall g, h \in G \).

\[
\phi_g(\phi_h)(x) = \phi_{gh}(x) = \phi_{gh}(x)
\]

\[
= \phi_{gh}(x)
\]

\[
= \phi_g(\phi_{ht}(x))
\]

\[
= \phi_g(\phi_{ht}(x))
\]
\( = \phi_{g} \bigcirc (\phi_{h} \phi_{i}) (x) \xi \)

(associative)

\( \phi_{e} \) is the identity and \( \phi_{g^{-1}} = (\phi_{g})^{-1} \)

\[ \phi_{g} \phi_{e} = \phi_{ge} = \phi_{g} \ \forall \ g \in G, \text{ and} \]

\[ \phi_{g} \phi_{g^{-1}} = \phi_{gg^{-1}} = \phi_{e}, \text{ hence } (\phi_{g})^{-1} = \phi_{g^{-1}} \]

Thus \( \overline{G} = \mathfrak{H}_{g} : g \in G \xi \) is a group of permutations.

Define \( \psi : \)

\[ g \rightarrow \phi_{g} \ \forall \ g \in G \]

i.e. \( \psi \)

If \( g = h \), then \( \psi \) is trivial, so \( \psi \) is a function.

**\( \psi \) is one-to-one:**

If \( g = h \) then \( \phi_{g} (e) = \phi_{h} (e) \) or \( g e = h e \) i.e.

\[ \psi (g) = \psi (h) \quad g = h, \text{ i.e. } \psi \text{ is one-one.} \]

by definition of \( \psi \),

\( \psi \) is onto.

\( \psi \) is a homomorphism:

\[ \psi \quad \psi \quad \psi \]

Hence \( \psi \) is an isomorphism and so

**Remark:**

\( \overline{G} \) is called **left regular representation** of \( g \).

**Simplicity of \( A_{n} \) for**

**Definition:**

A group is **simple** if its only normal subgroups are the identity subgroup and the group itself.

The first non abelian simple groups to be discovered were the alternating groups \( A_{5} \).

The simplicity of \( A_{5} \) was known to Galois and is crucial in showing that the general equation of degree 5 is not solvable by radicals.

**Theorem 20.**

The alternating group \( A_{n} \) is simple if \( n \geq 5 \).
For proving this we shall need a simple fact about 3 – cycles in $A_n$.

**Lemma 3:**

$A_n$ is generated by cycles of length 3 (3 – cycles) if $n \geq 3$.

**Proof.**

Every even permutation is the product of an even number of 2 – cycles. Since $(a, b) (a, c) = (a, b, c)$ and $(a, b) (c, d) = (a, b, c) (a, d, c)$, an even permutation is also a product of 3 – cycles. Further, 3 – cycles are even and thus belong to $A_n$.

(Here we have taken product from left to right).

**Proof of Theorem:**

Suppose it is false and there exists a proper nontrivial normal subgroup $N$.

Assume that a 3 – cycle $(a', b', c')$ is another 3 – cycle and such that

$$\pi = \begin{pmatrix} a & b & c \\ a' & b' & c' \end{pmatrix}$$

$$\pi^{-1} (a, b, c) \pi = \begin{pmatrix} a' & b' & c' \\ a & b & c \end{pmatrix}$$

$\Theta \pi \in S_n$, so $\pi$ may be odd, hence we replace it by even permutation

where $e, f$ differ from $a', b', c'$ without disturbing the conjugacy relation (here we use the fact $n \geq 5$).

Hence $(a', b', c')$ and $N = A_n$ by above lemma 3. Therefore, $N$ cannot contain a 3 – cycle.

Assume now that $N$ contains a permutation where disjoint cyclic decomposition involves a cycle of length at least 4, say

Then $N$ also contains

$$\pi' = b, a_2, a_3, g \pi b, a_2, a_3 \xi$$

Hence $N$ contains $\pi^{-1} \pi'$

$$= \begin{pmatrix} a & a_3 & a_4 & a_5 \\ a & a_2 & a_3 & a_4 \end{pmatrix} \begin{pmatrix} a & a_3 & a_4 \\ a & a_1 & a_4 \end{pmatrix} = (a_2, a_4, a_1): \text{ Note that other cycles cancel here.}$$
This is impossible. So nontrivial elements of N must have cyclic decomposition involving cycles of length 2 or 3. Moreover, such elements can not involve just one 3-cycle – otherwise by squaring we would contain a 3-cycle in N.

Assume that N contains a permutation \( \pi = (a, b, c) (a', b', c') \) – (with disjoint cycles). Then N contains

\[
\xi (a', c, b') (a, b, c) (a', b', c') = (a', b', c) = (a', a, b) (c, c', b') \xi
\]

Hence N contains which is impossible. Hence each element of N is a product of an even number of disjoint 2-cycles.

If then N contains for all c unaffected by \( \pi \).

Hence N contains

It follows that if then

\[
\xi (a', a, c, b', c') \xi (a, a, c, b, c') \xi
\]

But then N will also contain

\[
\pi = (a_2, b_2) (a_2, b_4) \pi (a_2, b_1) (a_2, b_2)
\]

\[
= (a_1, a_2) (a_3, b_1) (b_2, b_3) (a_4, b_4) \pi \pi' = (a_1, a_2, b_2) (a_3, b_3, b_1)
\]

which is final contradiction.

Hence \( A_n \) is simple for \( n \geq 5 \).

As promised earlier, to give an example that converse of Lagrange’s theorem is false:

**Example 7:**
The elements of \( A_4 \), the alternating group of degree 4, are

(1),

(12) (34), (13) (24), (14) (23),

(123), (123)²,

(124), (124)²,

(134), (134)²,

(234), (234)²

Which are 12 in number.

\( A_4 \) has 3 cyclic sub-groups of order 2.
A₄ has 4 cyclic subgroups of order 3.

The Klein’s four – group V₄:

is a normal subgroup of A₄.

Each

But Nᵢ is not normal subgroup of A₄ i.e.

Hence Normality is not a transitive relation i.e.

A ∆ B, B ∆ C ⇒ A ∆ C in genral.

Converse of Lagrange’s Theorem:

but A₄ does not contain a subgroup of order 6.

Suppose ∃ a subgroup H in A₄ of order 6. Then [A₄ : H] = 2 ⇒ H ∆ A₄

So we consider a quotient group \( A₄ / H \).

(123), (124), (134), (234), (132), (142), (143), (243) are elements of A₄.

\( \Theta \left| A₄ / H \right| = 2 \), \( (123) H g = H \), the identity of

\( \Rightarrow (123)^2 H = H \Rightarrow (132) H = H \)

\( \Rightarrow (132) \in H \)

Similarly, we can show

(123), (124), (132), (134), (142), (143), (234), (243) are elements of H. Therefore H contains 8 elements, which is absurd.

\( \Rightarrow A₄ \) has no subgroup of order 6, although \( 6 \) \( \left| A₄ \right| \).

Examples:

1. If there exists two relatively prime positive integers m and n such that \( a^m b^m = b^m a^m \) and \( a^n b^n = b^n a^n \), \( \forall a, b \in \text{a group } g \), then g is abelian.

Solution:

To show \( ab = ba \), \( \forall a \). As m, n are relatively prime positive integers, therefore, \( mx + ny = 1 \) for some
Integers \( x \) and \( y \). Note that \( x \) and \( y \) both cannot be +ve integers because if 1 in R.H.S. Let \( x \) be a +ve integer and \( y \) be -ve integer. Hence

\[
ab = a^{mx-ny} b^{mx-ny}
\]

\[
= a^{\frac{mx}{b}} \left( b^{mx} \right)^{-\frac{ny}{b}}
\]

\[
= a^{\{d^{in} d\}^{\frac{mx}{b}}}
\]

\[
= \begin{cases} 
\varepsilon^{a^y}, b^y \in G \end{cases}
\]

**Claim:**

\( g_1^{m} g_2^{n} = g_2^{n} g_1^{m} \neq g_1 g_2 \in G \neq \)

**Consider**

**Caution:**

We can not write \( mx \) times, if \( x \in N, x \) is -ve integer. Here \( mx \) is a+ve integer as

\[
= \begin{cases} 
\varepsilon^{a^y}, b^y \in G \end{cases}
\]

Also \( d^{m} g_2^{n} i^{-ny} = \{d^{m} g_2^{n} i^{-ny}\}^{-l} \)

\[
= \{d^{m} g_2^{n} i^{-ny}\}^{-l} \text{ from above}
\]

as \( ny \in N.\)

\[
\therefore d^{m} g_2^{n} i^{-ny} = d^{m} g_2^{n} i^{-ny}
\]

Hence from (1) and (2) we get

\[
\Rightarrow \quad \forall g_1, g_2 \in G, \ 
eq \ \ \ (3)
\]
Therefore,

\[
ab = \begin{align*}
&= d^{i^m} d^{i^n} d^{i^m} d^{i^n} d^{a^x}, \quad b^y \in G \\
&= d^{i^m} d^{i^n} d^{i^m} d^{i^n} d^{b^x}, \quad a^y \in G \\
&= d^{i^n} d^{i^m} d^{i^n} d^{i^m} d^{a^m b^m} = b^m a^m \neq a, \quad b \in G \\
&= \quad \begin{cases} a & \\
& b \ a \\
& a \ b
\end{cases} \quad \text{is ab} = \text{ba} \quad \text{and} \quad a, \quad b \in g.
\]

(2) (Groups of units modulo n)

Let n be a positive integer. The set of units modulo n is an abelian group under multiplication of congruence classes. The group \( \mathbb{Z}_n^* \) is finite and \( |\mathbb{Z}_n^*| = \phi(n) \), the Euler's phi-function.

**Special Case: \( \mathbb{Z}_8^* \)**

| Multiplication table in \( \mathbb{Z}_8^* \) |
|------------------|--|--|--|--|
| \([1]\) | \([3]\) | \([5]\) | \([7]\) |
| \([1]\) | \([1]\) | \([3]\) | \([5]\) | \([7]\) |
| \([3]\) | \([3]\) | \([1]\) | \([7]\) | \([5]\) |
| \([5]\) | \([5]\) | \([7]\) | \([1]\) | \([3]\) |
| \([7]\) | \([7]\) | \([5]\) | \([3]\) | \([1]\) |

\( \mathbb{Z}_n^* = \{[1], [3], [5], [7]\} : \text{Set of units (invertible elements) modulo 8, } [3] [3] = [9] \equiv [1] \mod 8 \)

\( [5] [5] = [25] \quad [1], [7] [7] = [49] \quad [1]. \)

\( \phi(8) = 4. \)

(3) \( = \{[1], [2], [4], [7], [8], [11], [13], [14]\} \)

Set of units modulo 15.

<table>
<thead>
<tr>
<th>( x_{15} )</th>
<th>([1])</th>
<th>([2])</th>
<th>([4])</th>
<th>([7])</th>
<th>([8])</th>
<th>([11])</th>
<th>([13])</th>
<th>([14])</th>
</tr>
</thead>
<tbody>
<tr>
<td>([1])</td>
<td>([1])</td>
<td>([2])</td>
<td>([4])</td>
<td>([7])</td>
<td>([8])</td>
<td>([11])</td>
<td>([13])</td>
<td>([14])</td>
</tr>
<tr>
<td>([2])</td>
<td>([2])</td>
<td>([4])</td>
<td>([8])</td>
<td>([14])</td>
<td>([1])</td>
<td>([7])</td>
<td>([11])</td>
<td>([13])</td>
</tr>
<tr>
<td>([4])</td>
<td>([4])</td>
<td>([8])</td>
<td>([11])</td>
<td>([13])</td>
<td>([2])</td>
<td>([14])</td>
<td>([7])</td>
<td>([11])</td>
</tr>
<tr>
<td>([7])</td>
<td>([7])</td>
<td>([14])</td>
<td>([13])</td>
<td>([4])</td>
<td>([11])</td>
<td>([2])</td>
<td>([1])</td>
<td>([8])</td>
</tr>
<tr>
<td>([8])</td>
<td>([8])</td>
<td>([11])</td>
<td>([2])</td>
<td>([14])</td>
<td>([4])</td>
<td>([13])</td>
<td>([14])</td>
<td>([7])</td>
</tr>
<tr>
<td>([11])</td>
<td>([11])</td>
<td>([7])</td>
<td>([14])</td>
<td>([2])</td>
<td>([13])</td>
<td>([1])</td>
<td>([8])</td>
<td>([4])</td>
</tr>
<tr>
<td>([13])</td>
<td>([13])</td>
<td>([11])</td>
<td>([7])</td>
<td>([1])</td>
<td>([14])</td>
<td>([8])</td>
<td>([4])</td>
<td>([2])</td>
</tr>
<tr>
<td>([14])</td>
<td>([14])</td>
<td>([13])</td>
<td>([11])</td>
<td>([8])</td>
<td>([7])</td>
<td>([4])</td>
<td>([2])</td>
<td>([1])</td>
</tr>
</tbody>
</table>
O(7) = 4, as $7^1 = 7$, $7^2 = 4$, $7^3 = 28 \equiv 13$, $7^4 = 91$.

O(1) = 1, O(2) = 4, O(4) = 2, O(8) = 4, O(13) = 4, O(14) = 2.

**Note:** To get calculation easier:

We do not calculate $13$, $13^2$, $13^3$, $13^4$

We calculate as follows:

- $13 \equiv -2 \pmod{15}$
- $13^2 \equiv (-2)^2 = 4$
- $13^3 = 13 \times 13 \equiv 4(-2) = -8$
- $13^4 \equiv -8 	imes -2 = 1 \pmod{15}$

Q.1. Show that the set of all $2 \times 2$ matrices over reals of the form

\[
\begin{pmatrix}
1 & 0 \\
0 & 1
\end{pmatrix}
\]

forms a group under matrix multiplication. Find all elements that commute with element

\[
\begin{pmatrix}
2 & 0 \\
1 & 0
\end{pmatrix}
\]

Q.2. Let $S = \mathbb{R} - \{-1\}$. Define $*$ on $S$ by $a * b = a + b + ab$. Show that $(S, *)$ is a group.

Q.3. Find the inverse of $\begin{pmatrix}2 & 0 \\ 1 & 0\end{pmatrix}$ in $\text{GL}(2, \mathbb{Z}_{11})$.

Q.4. For any elements $a$ and $b$ from a group and any integer $n$, prove that $(a^{-1}ba)^n = a^{-1}b^n a$.

Q.5. Show that the set $\{[5], [15], [25], [35]\}$ is a group under multiplication modulo 40. What is the identity element of the group?

Q.6. Construct Cayley table $\mathbb{Z}_x 12$.

Q.7. For any pair of real numbers $a \neq 0$ and $b$, define a function $f_{a,b}$ as follows:

\[f_{a,b}(x) = ax + b\]

1. Prove that $f_{a,b}$ is a permutation of $\mathbb{R}$

\[\mathbb{C}: f_{a,b} \in S_n\]

2. Prove that

3. Prove that $f_{a,b}^{-1} = f_{b,-a}$

4. Show that $g = \bigcap_{a,b} f_{a,b}$, $a, b \in R, a \neq 0$ is a group (a subgroup of $S_n$).

Q.8. For each integer $n$, define $f_n$ by

1. Prove that for each integer $n$, $f_n$ is a permutation of $\mathbb{R}$.

2. Prove that $f_n^{-1} = f_{-n}$.

3. Prove that $g = \bigcup_{f_n, n \in \mathbb{Z}}$ is subgroup of $S_n$.

4. Prove that $g$ is cyclic. Find a generator of $g$. 
Q.9. Show that the set of all matrices of the form where is an abelian group under matrix multiplication.

Q. 10. Show that $G = \{f_1, f_2, f_3, f_4\}$ where $f_1(x) = x$, $f_2(x) = -x$, $f_3(x) = -x^2$, and $f_4(x) = -\frac{1}{x}$ for $x \in R$, is a group under composition of functions. Is this abelian?

(Construct Cayley table)

Example 4.

In a group $G$, for three consecutive integers $i$ for all $a, b \in gG$. Show that $g$ is an abelian group.

Solution:

Let

\[ abg' = a^{i+1}b^{i+1} \quad (1) \]

\[ i \in Z \quad (2) \]

\[ bg' = bgb' \]

\[ = ab' \quad (3) \]

\[ = b'ab \]

\[ \Rightarrow b'a = ab' \quad (4) \]

Similarly

\[ abg' = a^{i+2}b^{i+2} \]

\[ \Rightarrow b'^{i+1}a = ab'^{i+1} \]

\[ \Rightarrow b'^{i+1}a = ab'^{i+1} \]

\[ \Rightarrow b'a = ab' \]

\[ \Rightarrow ba = ab \quad \forall a, b \in G. \]

Example 5.

Let $G$ be a group and has the order $mn$, $m$ and $n$ are relatively prime. Show that $x$ can be expressed uniquely as the product of two commutative elements $b$ and $a$ of $g$ of orders $m$ and $n$ respectively.

Solution:

\[ x = x^1 = x^{mt\cdot ns} \]

\[ = x^{mt}x^{ns} \]
Put \( a = x^{m_1} \), \( b = x^{n_1} \)

Then \( x = ab = ba \) \( x^{m_1+n_1} = x^{n_1+m_1} \) must have order \( n \).

Thus \( d_i \) has order \( n \), since \( (m, n) = 1 \) (if \( o(a) = n \), \( o(a') = m \) and \( (n, r) = d \), then \( m = n/d \))

Similarly \( x^{n_1} \) has order \( m \). Hence
\[
o(a) = n, \ o(b) = m
\]

**Uniqueness:**

Let \( x = a_1b_1 = b_1a_1 \).
\[
o(a_1) = n, \ o(b_1) = m.
\]
Then \( ab = a_1b_1 \)

Now \( (ab)^{m_1} = (a_1b_1)^{m_1} \)

\[
(1) \quad a_1b_1 = b_1a_1, \ ab = ba \zeta
\]

but \( o(b_1) = o(b) = m \)

Hence (1) \( \Rightarrow a^{m_1} = a_1^{m_1} \)

\[
\Rightarrow a^{l-n_1} = a_1^{l-n_1} \zeta \Rightarrow (a^{m_1} + n_1) = l \zeta
\]

\[
\Rightarrow a = a_1.a_1^{-n_1}.a^{n_1}
\]

\[
\Rightarrow a = a_1.a_1^{-n_1} e \zeta o(a) = n \zeta
\]

\[
\Rightarrow a_1.a_1^{-n_1}.a^{n_1} = a_1
\]

\[
\Rightarrow a = a_1 \zeta o(a) = n \zeta
\]

Now \( ab = a_1b_1 \) and \( a = a_1 \Rightarrow b = b_1 \)

**Example 5.**

Find the generators of the following finite cyclic groups:

1. \( G = \langle a \rangle, \ o(G) = 13 \)
2. \( G = \langle a \rangle, \ o(G) = 12 \)
Solutions.

1. Generators of G are \(a, a^2, a^3, a^4, a^5, a^6, a^7, a^8, a^9, a^{10}, a^{11}, a^{12}\), because 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, are relatively prime to 13. Number of generators = \(\phi(n) = \phi(13) = 12\) \(\implies \phi(p) = p - 1\) \(\mathbb{C}\)

2. Generators of G are \(a, a^5, a^7, a^{11}\), as 1, 5, 7, 11 are relatively prime to 12.

Example 6.

If \(a^{-1}ba = b^n\), then prove that \(a^{-m}b^s a^m = b^{sm}\). Hence deduce that if \(o(a) = 31\), then \(o(b) = 31\).

Solution.

\[
a^{-1}ba = b^n \Rightarrow a^{-1}(a^{-1}ba)a = a^{-1}b^n a
\]
\[
= a^{-2}ba = a \cdot a^{-1} = b^{n^{-1}} \Rightarrow a^{-2}ba^2 = b^{n^2}
\]

Given \(a^{-1}ba = b^2 \Rightarrow n = 2\)

\[
\Rightarrow b^s = b^2 \Rightarrow b = b^{32} \text{ (if } s = 1\}
\]

\[
\Rightarrow b^{31} = 1 \Rightarrow o(b) = 31
\]

Q.11. Give an example for each of the following:

(i) Finite non-abelian group.
(ii) Infinite non-abelian group.
(iii) Abelian group but not cyclic.
(iv) Finite non-abelian group which has only one normal subgroup.
(v) Finite non-abelian group which has all its subgroup normal.
(vi) Finite cyclic group.
(vii) Infinite cyclic group.

Example 7

Let \(G = \mathbb{Z}_n\) \(\implies a \neq 0\)

i. Show that g is a group under composition of mapping.

ii. Let . Show that
iii. \( N = \mathbb{N}_{a,b} \in G \xi \) show that

**Solution.**

Let \( \tau_{a,b}, \tau_{c,d} \in G. \)

\[
= a(cx + d) + b
\]

\[
= \psi x \in R
\]

\[
= \Rightarrow \quad \tau_{a,b} \circ \tau_{c,d} = \tau_{ac, ad + b} \in G \quad \Theta \quad ac \neq o \text{ in } R \xi
\]

\[
= \tau_{a(bf), a(cf + d)} + b
\]

\[
= \tau_{a,b} \circ \tau_{c,f + d}
\]

\[
= \tau_{a,b} \circ \tau_{c,f + d} \circ \tau_{f,l} \quad \psi
\]

\[
b, d, l \in R
\]

For identity element:

\[
\Rightarrow ac = 1, ad + b = 0
\]

\[
\therefore c = \frac{b}{a}, d = -a^{-1}b (\Theta + a \in R)
\]

Hence \( \tau_{1,0} \in G \) such that \( \tau_{a,b} \circ \tau_{1,0} = \tau_{al, at+b} = \tau_{a,b} \quad \forall \quad \tau_{a,b} \in G. \)

Hence \( \tau_{1,0} = e, \) the identity of G.

For inverse element:

\[
\Rightarrow ac = 1, ad + b = 0
\]

\[
\therefore \quad \tau_{c,d} = \tau_{a^{-1}, -a^{-1}b} \text{ is the right inverse of } \tau_{a,b}
\]

\[
\therefore G = \mathbb{M}_{a,b} | a \neq 0 R \text{ is a group.}
\]

(ii) \( H = \)

From above H is a subgroup of G.

To show \( \forall \quad \tau_{c,d} \in G \) \( \forall \)
L.H.S. =

\[ \tau_{(ca), (c'b + d)} = \tau_{a, -ad + cb + d} \in H \]

(iii) from (i) and (ii).

**Example 8.**

Let \( G \) be a group in which, for some integer \( n > 1 \), \( (ab)^n = a^n b^n \) for all \( a, b \in G \). Show that

i. is a normal subgroup of \( G \).

ii. is a normal subgroup of \( G \).

iii. \( \forall a, b \in G \).

iv. \( \forall a, b \in G \).

**Solution:**

(i) First we show \( G^{(n)} \) is a subgroup of \( G \).

Let

Now \( ab^{-1} = x^n(y^n)^{-1} = x^n(y^{-1})^n = (xy^{-1})^n \in G \), \( x, y \in g \)

is a subgroup of \( g \).

To show \( G^{(n)} \triangleleft G \).

i.e. To show \( az^{-1}a^{-1} \in G^{(n)} \), \( \forall a \in G, \forall z \in G^{(n)} \Rightarrow z = x^n, x \in G \).

\[ az^{-1}a^{-1} = ax^n a^{-1} = (ax^{-1})^n \] \( \exists \ n \) is an integer \( > 1 \)

(ii) To show \( G^{(n-1)} \) is a subgroup of \( G \).

Let \( a, b \in G^{(n-1)}, \) then \( a = x^{n-1}, b = y^{n-1}, x, y \in G \).

\[ ab^{-1} = x^{n-1}(y^{n-1})^{-1} = x^{n-1}(y^{-1})^{n-1} = (y^{-1}x)^{n-1} \in G^{(n-1)} \in G \]

is a subgroup of \( G \).

\[ e b g = a^n b^n \] \( \forall a, b \in G \), for some integer \( n > 1 \).
abab-------ab = a^n b^n

⇒ a b g' b = a^n b^n
⇒ b g' = a^{n-1} b^{n-1} j

To show \( G^{(n-1)} \trianglelefteq G \).

i.e. To show \( a z a^{-1} \in G^{(n-1)}, \forall a \in G, \forall z \in G^{(n-1)} \)

Let \( z = x^{(a^{-1})}, x \in G \)

Now \( a z a^{-1} = axa^{-1} a^{-1} = d a x a^{-1} i^{-1} \in G^{(n-1)} \) \( \text{d} a x a^{-1} \in G \)

⇒ \( G^{(n-1)} \trianglelefteq G \).

(iii) To show \( a^{n-1} b^n = b^n a^{n-1} \neq a, b \in G \)

Also

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

(iv) To show

\( d a x a^{-1} i^{(n-1)} = e \neq a, b \in G \)

L.H.S. =

\[ = \{ d a^{-1} b^{-1} i^{(n-1)} a^{n-1} \} \ o b g' = a^{n-1} b^{n-1} \text{ from above} j \]

\[ = d a^{-(n-1)} b^{-1} a^{n-1} i' \]

\[ = \]
Example 9.

Let $S$ be a semi-group. If for all 

$$x^2 y = y = yx^2 \quad \forall \ xy \in S.$$ (1)

$$\Rightarrow x^2 x = x = xx^2$$

$$\Rightarrow x^3 = x \quad \forall \ x \in S.$$ (2)

Also$$\forall \ x, \ y \in S.$$ (3)

Now from (3) and (1)

$$= \quad \forall$$

$$= \quad \forall$$

$$= \quad \forall$$

$$= \quad \forall$$

$$= \quad \forall$$

$$= \quad \forall$$

$$= \quad \forall$$

Q.12.

1. Show that is not cyclic group.

2. Show that is a cyclic group.

Find its all generators.

Q.13. If in the group $G$, $a^5 = e$, $aba^{-1} = b^2$

for some $\forall$

Q.14. If $G$ has no nontrivial subgroups, show that $G$ must be finite of prime order.

Q.15. If $G$ is a group and $H$ is a subgroup of index 2 in $G$, prove that $H$ is a normal subgroup of $G$.

Q.16. If $N$ is a subgroup of $G$ and $H$ is any subgroup of $G$, prove that $NH$ is a subgroup of $G$.

Q.17. If $N$ and $M$ are normal subgroups of $G$, prove that $NM$ is also a normal subgroup of $G$.

Q.18. In Q17, if $\forall\ x \in N, \ y \in M$. show that $xy = yx$.

Q.19. If $H$ is a normal cyclic subgroups of a group $G$, show that every subgroup of $H$ is normal in $G$. 

Q.20. Show that Normality is not a transitive relation in a group $G$. Let $H, K, G$ be subgroups of $G$ with $H \trianglelefteq K \trianglelefteq G \Rightarrow H \trianglelefteq G$. 

Q.21. Show that $S_n$ is generated by $(12)$ and $(1, 2, 3, \ldots, n)$. 

Q.22. Find the product of 

(1) $(12)(123)(12)(23)$ 
(2) $(125)(45)(1, 6, 7, 8, 9)(15)$ 

Q.23. Which of the following are even or, odd permutations: 

(1) $(123)(13)$, 
(2) $(12345)(145)(15)$, 

Q.24. Prove that the cyclic group $Z_4$ and the Klein four-group are not isomorphic. 

Q.25. Show that the group is isomorphic to the group if all are of the form 

$$
\begin{pmatrix}
1 & 0 \\
0 & 1
\end{pmatrix},
\begin{pmatrix}
1 & 1 \\
0 & 1
\end{pmatrix}
$$

$\text{Example 10.}$

Let $H$ be a subgroup of $G$ and $N$ a normal subgroup of $G$. Show that $H \cap N$ is a normal subgroup of $H$. 

$\text{Solution:}$

Let $x$ be any element of $H$ and $h$ be any element of $H$. 

$$x \in H, h \in H \Rightarrow hxh^{-1} \in H, N \trianglelefteq G, h \in H \subseteq G \Rightarrow hxh^{-1} \in N$$

$\therefore hxh^{-1} \in H \cap N$ 

$\text{Example 11.}$

Let $H$ be a subgroup of a group $G$, let 

Prove that 

(i) $N(H)$ is a subgroup of $G$ 

(ii) $H \trianglelefteq N \trianglelefteq \Omega$ 

(iii) $N(H)$ is the largest subgroups of $G$ in which $H$ is normal. 

(iv) 

$\text{Solution:}$ 

(i) Let $g_1, g_2 \in N \trianglelefteq \Omega$
To show

Now $b_{i}d_{j}^{-1}d_{i}^{-1} = d_{j}^{-1}H_{g_{i}}^{-1}H_{g_{j}}^{-1} = g_{i}Hg_{j}^{-1} = H \Rightarrow g_{i}Hg_{j}^{-1} \subseteq N(H)$

Hence $N(H)$ is a subgroup of $G$.

(ii) Let $g \in N(H)$, $x \in H$.

To show $gxg^{-1} \in H$.

$g \in N(H) \Rightarrow gHg^{-1} = H \Rightarrow gHg^{-1} \subseteq H \Rightarrow gxg^{-1} \in H$ $\exists x \in H$\(\ni\)

$\Rightarrow H \Delta N \ni \zeta$

(iii) Let $K$ be any subgroup $G$ and $H$ be a normal of $K$, we must show that

(1)

(2) $H \Delta K$, Hence $kx^{-1} \in H \forall k \in H \subseteq G \Rightarrow k \in N(H) \Rightarrow K \subseteq N(H)$

(iv) From (ii) and (iii) $\Rightarrow N(H) = G$. Also $N(H) = G$ and $N(H) = \{g \in G \mid gHg^{-1} = H\} \Rightarrow H \Delta G$

**Example 12**

Given any group of $G$. Let $U$ be the smallest subgroup of $G$ which contains $U$. Such group is called the subgroup generated by $U$.

(i) If $\forall u \in U$, show that .

(ii) Let $U = \{x^{-1}y^{-1} \mid x, y \in G\}$, In this case is usually written as , called the commutator subgroup of $G$. Show that .

(iii) Prove that is abelian.

(iv) If $G/N$ is abelian, prove that $G \subset N$.

(v) Prove that if $H$ is a subgroup of $G$ and , then .

First we give the following definition.

**Definition**:

Let $G$ be a group and let $I$, the indexing set. The smallest subgroup of $G$ containing is the subgroup generated by , If this subgroup is all of $G$, then generates $G$ and the are generators of $G$. If there is a finite set $m \in H$ that generates $G$, then $G$ is finitely generated.
Remark:
If $G$ is abelian, then could be simplified to $(a_1)^3(a_2)^3$, but this may not be true in the non abelian group.

Solution:

(i) Given $gug^{-1} \in U \forall g \in G, \forall u \in U$. To show $\bar{U}G$

$\Theta$ is the subgroup generated by $U$.

$= \{ \text{all finite products of integral powers of } a \text{ in } U \}$

Let $x \in \bar{U}$, $u_i \in U$, $n_i \in Z$.

$g^{-1} = g_{u_1}^{-1}g_{u_2}^{-1}g_{u_3}^{-1}g \ldots \ldots g_{u_i}^{-1}g$

$= (gu_1g^{-1})^{n_1}(gu_2g^{-1})^{n_2} \ldots \ldots (gu_kg^{-1})^{n_k} \in \bar{U}$

because

Hence $gxg^{-1} \in \bar{U} \forall g \in G$

$\Rightarrow \bar{U}A G$ (i.e. $G \triangleleft G$)

(ii) $U = \{ xy^{-1}x^{-1} \mid x, y \in G \}$

The Commutator subgroup of $G$

From (1) $\bar{U} = G' \triangleleft G$.

(iii) $G/G' = \{ xG | x \in G \}$. To show abelian,

We must show $xG'yG' =$

i.e. $=$

L.H.S.

$= (\Theta$ is a commutator and so $y^{-1}x^{-1}xyG' = G'\}$

$= (xyx^{-1}y^{-1})yG' = xyG'$

$= yG'xG' = R.H.S.$

(iv) To show abelian $\Leftrightarrow G' \subseteq N$

$\Rightarrow ? x^{-1}Ny^{-1}N = y^{-1}Nx^{-1}N \Rightarrow x^{-1}y^{-1}N = y^{-1}x^{-1}N \Rightarrow xyx^{-1}y^{-1}N = N \Rightarrow xyx^{-1}y^{-1} \in N$

i.e. every commutator to a group $N$, hence all finite products of integral powers of commutators are in $N$.

$\therefore G' \subseteq N$. 
Conversely, if $xNyN = xyN = (\Theta)$, then

$$xNyN = xN yN = (xyy^{-1}x^{-1})yN = eyxN$$

$$= yN = yNxN$$

(d) Given $H \triangleleft G$, to show $H \Delta G$ i.e. To show $\forall g \in G, \forall h \in H$

$$= ghg^{-1}h^{-1} = (ghg^{-1}h^{-1})h \in H (\Theta)$$

\[\therefore\]

**Example 13**

Final order of

1. $(15 \ 27) (284)$ in $S_8$
2. $(153) (284697)$ in $S_9$

**Solution**

Both are product of disjoint cycles. Hence order of each would be l.c.m. of the lengths if its cycles.

(i) $12$ in $S_8$
(ii) $6$ in $S_9$

**Example 14**

Write $(12345)$ as a product of transpositions. It can be written in more than one way.

$$(12345) = (54) (53) (52) (51)$$

$$= (15) (14) (13) (12)$$

$$= (54) (52) (51) (14) (32) (41)$$

**Q. 26.** Let $\alpha = a_1a_2a_3\ldots a_s$ be a cycle and let $\pi$ be a permutation in $S_n$. Then $\pi$ is the cycle $(\pi \pi \ldots \pi)$.

**Example 15**

Compute $aba^{-1}$, Where

(i) $a = (135) (12), b = (1579)$
(ii) $a = (579), b = (123)$

**Solution**

(i) $a = (135) (12) = (1235)$

$$a (1579) a^{-1} = a(1) a(5) a(7) a(9) \zeta$$

$$= (2179)$$

(ii) $= a(1) a(2) a(3) \zeta$ Where $(579)$

$$= (123)$$
Ideals and Quotient Rings

**Definition.** Let $S$ be a subring of a ring $R$. If $x \in S, a \in R \Rightarrow ax \in S,$
then $S$ is called **left ideal** of $R$.
If $x \in S, a \in R \Rightarrow xa \in S,$
then $S$ is called **right ideal** of $R$.
If $x \in S, a \in R \Rightarrow xa \in S$ and $ax \in S$ then $S$ is called **two sided ideal** or simply ideal of $R$.
* If $R$ is a commutative ring then all the three notions are same since in that case $ax = xa \in S$.
** Every ring has two trivial ideals:
(i) $R$ itself and is called **unit ideal**
(ii) Zero ideal $[0]$ consisting of zero element only.
Any other ideal except these two trivial ideals is called proper ideal.

**Theorem.** The intersection of any two left ideals of a ring is again a left ideal of the ring.

**Proof.** Let $S_1$ and $S_2$ be two ideals of $R$. $S_1$ and $S_2$ being subring of $R$, $S_1 \cap S_2$ is also a subring of $R$.
Again let $x \in S_1 \cap S_2,$
$$\Rightarrow x \in S_1, x \in S_2.$$ 
Let $a \in R$. Then since $S_1$ and $S_2$ are left ideals,
$$a \in R, x \in S_1 \Rightarrow ax \in S_1$$
$$a \in R, x \in S_2 \Rightarrow ax \in S_2$$
$$\Rightarrow ax \in S_1 \cap S_2$$
$$\Rightarrow S_1 \cap S_2$$ is a left ideal.

**Theorem :-** Let $K(T)$ be the kernel of a ring homomorphism $T : R \rightarrow S$. Then $K(T)$ is a two sided ideal of $R$.

**Proof.** Let $a, b \in K(T)$. Then $T(a) = T(b) = 0$.
Therefore,
$$T(a+b) = T(a) + T(b) = 0 + 0 = 0$$ (by ring homomorphism)
$$T(ab) = T(a).T(b) = 0.0 = 0$$
which implies that $a+b, ab \in K(T)$. Hence $K(T)$ is a subring of $R$.
Now let $a \in K(T)$ and $r \in R$. It suffices to prove that $ar, ra \in K(T)$
$$T(ar) = T(a).T(r)$$
$$= 0 \cdot T(r) \quad (\Theta a \in K(T) \Rightarrow T(a) = 0)$$
$$= 0$$
This implies that $ar \in K(T)$. Similarly,
$$T(ra) = T(r)T(a) = T(r).0 = 0$$
$$\Rightarrow ra \in K(T).$$
Hence $K(T)$ is an ideal of $R$.

**Theorem.** A field has no proper ideal.
**Proof.** Let us suppose that $S$ is a proper ideal of a field $F$. Then

$$S \subseteq F$$  \hspace{1cm} (i)

If $x \in S$, then $xx^{-1} \in S$. But $xx^{-1} = 1$. Therefore, $1 \in S$. As $S$ is an ideal, $y \in F \Rightarrow y.1 \in S$. Thus $y \in F \Rightarrow y \in S$. That is $F \subseteq S$. Therefore, $F = S$. This contradicts our supposition. Hence $F$ has no proper ideal.

**Theorem.** If a commutative ring $R$ with unity has no proper ideal, then $R$ is a field.

**Proof.** It suffices to prove that every non-zero element of $R$ is invertible. Let $a$ be a non-zero element of $R$. Consider the set

$$S = \{ xa \mid x \in R \}.$$

We claim that $S$ is an ideal of $R$. To show it, let $p, q \in S$. Then

$$p = x_1 a, \quad q = x_2 a \mid x_1, x_2 \in R$$

$$p + q = x_1 a + x_2 a = (x_1 + x_2) a \in S. \quad (\Theta x_1 + x_2 \in R)$$

Similarly

$$-p = -x_1 a = (-x_1) a \in S.$$  

Therefore, $S$ is an additive subgroup of $R$.

Moreover, if $r \in R$, then

$$rp = r(x_1 a) = (rx_1) a \in S.$$

Since $R$ is commutative, $rp \in S \Rightarrow pr \in S$.

Hence $S$ is an ideal of $R$. But by supposition

$$S \neq \{0\} \text{ or } S = R.$$  

Since $1 \in R \Rightarrow a \in S \quad (\Theta 1.a \in S),$  

$S$ is not equal to $\{0\}$. Hence $S = R$. By definition of $S$, $1 = xa, x \in R$. Therefore, every non-zero element of $R$ is invertible and hence $R$ is a field.

Let $A$ be an ideal of a ring $R$. Then $R$ is an abelian group and $A$ is an additive subgroup of $R$. But every subgroup of an abelian group is normal, therefore $A$ is a normal subgroup of $R$. So we can define the set

$$R/A = \{ r + A \mid r \in R \}.$$

We shall prove that $R/A$ is a ring. This ring will be called quotient ring.

**Theorem.** Let $A$ be an ideal of $R$. Then the set

$$R/A = \{ r + A \mid r \in R \}$$

is a ring.

**Proof.** We define addition and multiplication compositions as follows:

$$\begin{align*}
(r+A) + (s+A) &= (r+s) + A \\
(r+A)(s+A) &= rs+A
\end{align*}$$

for all $r, s \in R$.

We show first that above defined binary operations are well defined. Let

$$r+A = r_1+A \quad r_1, s_1 \in R$$

$$s+A = s_1+A$$

which implies $r-r_1 \in A, s-s_1 \in A$. Then
\[(r+s) - (r_1+s_1) = (r-r_1) + (s-s_1) \in A\]
\[\Rightarrow (r+s) + A = (r_1+s_1) + A\]
which proves that addition is well defined.

Moreover,
\[rs - r_1s_1 = rs - r_1s + r_1s - r_1s_1\]
\[= (r-r_1)s + r_1(s-s_1) \in A\]
Therefore, \(rs + A = r_1s_1 + A\) and hence multiplication composition is also well defined. We now prove that these compositions satisfy all the properties of a ring.

(i) **Associativity of addition** :- If \(r+A, s+A, t+A \in R/A\), then
\[\[(r+A) + (s+A)] + (t+A) = [(r+s)+A] + (t+A)\]
\[= [(r+s)+t]+A\]
\[= [r+(s+t)]+A\]
\[= (r+A) + [(s+t)+A]\]
\[= (r+A) + [(s+A) + (t+A)].\]

(ii) **Existence of the identity of addition** :- If \(r+A \in R/A\), then
\[0+A + (r+A) = r+A\]
and
\[(r+A) + (0+A) = r+A\]
Therefore \(0+A = A\) is identity element of addition.

(iii) **Existence of additive inverse** :- If \(r+A \in R/A\), then
\[(r+A) + (-r+A) = [r+(-r)] + A\]
\[= 0+A = A\]
and
\[(-r+A) + (r+A) = [(-r) + r] + A\]
\[= 0+A = A\]
which shows that \(-r+A\) is the inverse of \(r+A\).

(iv) **Commutativity of addition** :- If \(r+A, s+A \in R/A\), then
\[(r+A) + (s+A) = (r+s) + A\]
\[= (s+r) + A\]
\[= (s+A) + (r+A)\]

(v) **Associativity of multiplication** :- If \(r+A, s+A, t+A \in R/A\), then
\[\[((r+A) (s+A))] (t+A) = (rs+A) (t+A)\]
\[= (rs)t + A\]
\[= r(st) + A\]
\[= (r+A) (st+A)\]
\[= (r+A) [(s+A) (t+A)].\]

(vi) **Distributivity of multiplication over addition** :- If \(r+A, s+A, t+A \in R/A\), then
\[(r+A) [(s+A) + (t+A)] = (r+A) [(s+t)+A]\]
= r(s+t) + A = (rs + rt) + A
= (rs+A) + (rt+A)
= (r+A) (s+A) + (r+A)(t+A) .

Similarly,

[(r+A) + (s+A)] (t+A) = (r+A)(t+A) + (s+A) (t+A) .

Hence R/A is a ring.

* If R is commutative, then R/A will be abelian since if

r+A, s+A ∈ R/A , then by the commutativity of R, we have

(r+A) (s+A) = rs+A
= sr+A
= (s+A) (r+A)

In addition if R has unit element then R/A has also identity 1+A.

**Theorem.** Every ideal A of a ring R is a kernel of some ring homomorphism.

**Proof.** Let φ : R → R/A be a mapping defined by φ(r) = r+A. This mapping is known as natural mapping. If r, s ∈ R, then

φ(r+s) = (r+s) +A
= (r+A) + (s+A)
= φ(r) + φ(s)

and

φ(rs) = rs+A
= (r+A) (s+A)
= φ(r) φ(s)

Therefore φ is a homomorphism. Kernel of this homomorphism, is given by

K(φ) = {r | r ∈ R, φ(r) = A}
= {r | r ∈ R, r+A = A}
= {r | r ∈ R}
= A

which proves the required result.

**Theorem.** Let φ : R → S be a ring homomorphism of R onto S. Then

R/K(φ) ~ S.

**Proof.** We know that K(φ) is an ideal of R. Therefore, R/K(φ) is defined. Elements of this set are cosets of K(φ) in R. Let r+K ∈ R/K(φ). Then

φ(r+x) = φ(r) + φ(x) for all x ∈ K(φ)
= φ(r) + 0 (Θ x ∈ K(φ) ⇒ φ(x) = 0 )
= φ(r)

Thus we can define a mapping ψ(r+K) = φ(r) for all r ∈ R. We shall prove that ψ is an isomorphism. Let r+K, s+K ∈ R/K(φ). Then

ψ [(r+K) + (s+K)] = ψ [(r+s) + K]
= ψ(r+s)
= φ(r) + φ(s)
and

\[ \psi [(r+K) (s+K)] = \psi(rs+K) = \phi(rs) = \phi(r)\phi(s) = \psi(r+K) \psi(s+K) \]

Therefore \( \psi \) is a ring homomorphism.

If \( x \in S \), then

\[ x = \phi(r), \ r \in R \ (\Theta \ \phi \ is \ onto \ mapping) \]

\[ = \psi (r+K) \]

Therefore to each element \( x \in S \) there corresponds an element \( r + K \) of \( R/K(\phi) \) such that \( \psi(r+K) = x \). Hence \( \psi \) is surjective.

Moreover,

\[ \psi(r+K) = \psi (s+K) \Rightarrow \phi(r) = \phi(s) \]
\[ \Rightarrow \phi(r-s) = 0 \]
\[ \Rightarrow r-s \in K(\phi) \]
\[ \Rightarrow r+K = s+K \]

Therefore \( \psi \) is one-to-one mapping also. Hence \( \psi \) is an isomorphism, as a consequence of which \( R/K(\phi) \cong S \).

**Theorem.** A homomorphic image of a ring \( R \) is also a ring.

**Proof.** Let \( T : R \rightarrow S \) be a ring homomorphism. Then homomorphic image of \( R \) is

\[ \text{Im}(T) = \{ x \mid x \in S, \ x = T(r), \ r \in R \} \]

We know that \( T(0) = 0 \). Therefore, \( \text{Im}(T) \) is non-empty. If \( x, y \in \text{Im}(T) \), then \( \exists \ r, s \in R \) such that \( x = T(r), y = T(s) \).

Therefore,

\[ x+y = T(r) + T(s) = T(r+s) \in \text{Im}(T) \quad (\Theta \ T \ is \ a \ homomorphism) \]

and

\[ xy = T(r)T(s) = T(rs) \in \text{Im}(T). \]

Hence \( \text{Im}(T) \) is a subring of \( S \).

---

**Types of Ideal**
**Definition.** Let $R$ be a commutative ring. An ideal $P$ of $R$ is said to be a **prime ideal** of $R$ if for $a, b \in R$

$$ab \in P \Rightarrow a \in P \text{ or } b \in P.$$  

**Theorem.** An ideal $P$ of a commutative ring $R$ is a prime ideal if and only if $R/P$ is without zero divisor.

**Proof.** Let us suppose that $R/P$ is without zero divisor and let $r, s \in R$ such that $rs \in P$. Then

$$rs \in P \Rightarrow rs + P = P$$

$$\Rightarrow (r+P) (s+P) = P$$

$$\Rightarrow r+P = P \text{ or } s+P = P \quad (\Theta \text{ R/P is without zero divisor})$$

$$\Rightarrow r \in P \text{ or } S \in P.$$  

Hence $P$ is a prime ideal.

Conversely, let $P$ be a prime ideal and let

$$(r+P) (s+P) = P, \ r, s \in P$$

Then

$$rs + P = P$$

$$\Rightarrow rs \in P$$

$$\Rightarrow r \in P \text{ or } s \in P \quad (\Theta P \text{ is a prime ideal})$$

$$\Rightarrow r + P = P \text{ or } s + P = P.$$  

Hence $R/P$ is without zero divisor.

**Examples.** 1. Let $p$ be a prime. Then ring of integer mod $p$, is without zero divisor. Therefore, ideal of $\mathbb{Z}/p\mathbb{Z}$ is a prime ideal.

2. Zero ideal of the ring of integers is a prime ideal.

**Definition.** An ideal generated by a single element is called a **principal ideal**.

For example every ideal of the ring of integers is a principal ideal.

Let us suppose that $I$ is an ideal of $\mathbb{Z}$. If $I = \{0\}$ then it is clearly a principal ideal. If $I$ is a non-zero ideal then $x \in I \Rightarrow -x \in I$. Therefore, I certainly contains positive elements. Let $m$ be the smallest positive integer belonging to $I$. If $y \in I$ be an arbitrary element of $I$ then by Euclidean algorithm there exist $q, r \in \mathbb{Z}$ such that

$$y = mq + r, \ 0 \leq r < m.$$  

Since $m \in I, \ q \in \mathbb{Z}$, therefore $mq \in I$.

Therefore,

$$y - mq = r$$

$$\Rightarrow r \in I.$$  

Hence by the minimality of $m$ in (i) we have $r = 0$. It follows therefore that

$$y = mq.$$  

This implies that $I = \langle m \rangle$. Hence $I$ is a principal ideal.

**Definition.** A maximal ideal $M$ of a ring $R$ is a proper ideal which is not strictly contained in any ideal other than $R$.

Thus $M$ is a maximal ideal if and only if
Example. An ideal generated by a prime number is a maximal ideal of the ring of integers. But the zero ideal of the ring of integers is not maximal.

Proof. Let \( p \) be any prime integer and let \( S \) be any ideal containing the principal ideal generated by \( p \). Now the ring of integers being principal ideal ring the ideal \( S \) is a principal ideal and it is generated by the integer \( q \). We have therefore

\[
(p) \subset (q) \subset R
\]

\[
\Rightarrow p \in (q)
\]

\[
\Rightarrow p = kq, \ k \in R .
\]

Since \( p \) is prime, \( p = kq \Rightarrow \) either \( k = 1 \) or \( q = 1 \).

Now \( k = 1 \)

\[
\Rightarrow p = q
\]

\[
\Rightarrow (p) = (q)
\]

and \( q = 1 \)

\[
\Rightarrow (q) = (1) = R \quad \text{(Since } R \text{ is generated by } 1).\]

Hence \((p)\) is maximal ideal.

Theorem. Every maximal ideal \( M \) of a commutative ring \( R \) with unity is a prime ideal.

Proof. It suffices to prove that if \( a, b \in R \) then

\[
ab \in M \Rightarrow a \in M \text{ or } b \in M .
\]

Let us suppose that \( a \notin M \). If we prove that \( b \in M \) then we are done. It can be seen that the set

\[
N = \{ra + m \mid r \in R, \ m \in M\}
\]

is an ideal of \( R \).

Since \( 1 \in R \), therefore \( a + m \in N \). But \( a + m \notin M \) since \( a \notin M \). Therefore

\[
M \subset N \subset R , \quad M \neq N .
\]

\( M \) being a maximal ideal asserts that \( N = R \). Therefore \( 1 \in R \Rightarrow 1 \in N \). So we can find two elements \( r \in R, m \in M \) such that

\[
l = ra + m
\]

\[
\Rightarrow b = r(ab) + mb, \ b \in R
\]

Since \( M \) is an ideal of \( R \), therefore

\[
ab \in M, \ r \in R \Rightarrow r(ab) \in M
\]

and

\[
m \in M, \ b \in R \Rightarrow mb \in M .
\]

Therefore

\[
b \in M .
\]

Hence \( M \) is a prime ideal.

Theorem. An ideal \( M \) of a commutative ring \( R \) with unity is maximal if and only if \( R/M \) is a field.

Proof. Let \( M \) be a maximal ideal of \( R \). Since \( R \) is a commutative ring with unity, \( R/M \) is also a commutative ring with unity element. Let \( A^* \) be an ideal of \( R/M \) and

\[
A = \{r \mid r+M \in A^*\}
\]

If \( r, s \in A \), then \( r+M, s+M \in A^* \). Therefore

\[
(r-s) + M = (r+M) - (s+M) \in A^*
\]

\[
\Rightarrow r-s \in A
\]

If \( r \in A, t \in R \), then \( r+M \in A^* \) and

\[
r+M \]


rt + M = (r+M) (t+M) ∈ A* (because A* is an ideal of R/M).
⇒ rt ∈ A.
R being commutative tr also belongs to A.

Hence A is an ideal of R.

If a ∈ M, then
a+M = M ∈ R/M (since M is the zero element of R/M)
⇒ a+M ∈ A* (since (1+M) (a+m) ∈ A*, A* being ideal of R/M)

Therefore
M ⊂ A ⊂ R.
Let us suppose that A* ≠ {0} then there exists an element r+M of A* such that
r +M ≠ M
But r+M ∈ A* ⇒ r ∈ A,
r+M ≠ M ⇒ r ∈ M ⇒ A ≠ M.

Thus we have proved that if A* ≠ {0}, then
M ⊂ A ⊂ R.

Since M is maximal therefore, A = R. If r ∈ R then r ∈ A which implies that r +M ∈ A*.
It follows therefore, that A* = R/M.

We have proved therefore, that R/M has only two ideals {0} and R/M and hence R/M is a field.
Conversely, let R/M is a field. Then R/M has only two ideals {0} and R/M itself. Hence
A* = {0}
or A* = R/M.

If A* = {0} then A* = M (Θ M is zero element of R/M)

Therefore,
A = {r | r +M ∈ A*}
    = {r | r+M = M}
    = {r | r ∈ M}
    = M

If A* = R/M then
A = {r | r +M ∈ R/M}
    = {r | r ∈ M}
    = R.

Therefore, R has only two ideals M and R. Hence M is a maximal ideal.

**Imbedding of a ring and an integral domain.**

**Definition.** If a ring R is isomorphic to a subring T of a ring S then R is called imbedded in S. The ring S is called extension or over ring of R.

**Theorem.** Every ring R can be imbedded in a ring S with unit element.

**Proof.** Let S be a set defined by
S = Z × R = {(m,a) | m ∈ Z, a ∈ R}.
We define addition and multiplication in $S$ as follow:

$$(m, a) + (n, b) = (m+n, a+b)$$

$$(m, a) (n, b) = (mn, na+mb+ab)$$

We now prove that $S$ is a ring with unity under these binary operations. Let $(m, a), (n, b), (p, c) \in S$. Then

(i) 

$$[(m, a) + (n, b)] + (p, c) = (m+n, a+b) + (p, c)$$

$$= (m+n+p, a+b+c)$$

(by Associativity of $R$ and $Z$)

$$= (m, a) + (n+p, b+c)$$

$$= (m, a) + [(n, b) + (p, c)]$$

(ii) 

$$(0, 0) + (m, a) = (m, a)$$

$$(m, a) + (0, 0) = (m, a)$$

Therefore $(0, 0)$ is additive, identity.

(iii) 

$$(m, a) + (-m, -a) = (0, 0)$$

$$(-m, -a) + (m, a) = (0, 0)$$

Therefore $(-m, -a)$ is the inverse of $(m, a)$.

(iv) 

$$(m, a) + (n, b) = (m+n, a+b)$$

(by commutativity of $R$ and $Z$)

$$= (n+m, b+a)$$

$$= (n, b) + (m, a)$$

(v) 

$$[(m, a) (n, b)] (p, c) = [mn, na + mb + ab] (p, c)$$

$$= [mn, p(np+mb+ab) + mnc + c(na+mb+ab)]$$

$$= [(mn)p, p(na) + p(mb) + p(ab) + (mn)c + (na)c + (mb)c + (ab)c]$$

and

$$(m, a) [(n, b) (p, c)] = (m, a) [np, pb + nc + bc]$$

$$= [m(np), anp + m(pb) + m(nc) + m(bc) + a(pb+nc+bc)]$$

$$= [(mn)p, p(na) + p(mb) + p(ab) + (mn)c + (na)c + (mb)c + (ab)c]$$

(by Associativity and commutativity of $R$ and $Z$).

Hence

$$(m, a) [(n, b) (p, c)] = [(m, a) (n, b)] (p, c)$$

(vi) 

$$[(m, a) + (n, b)] (p, c) = (m+n, a+b)(p, c)$$

$$= [(m+n)p, p(a+b) + (m+n)c + (a+b)c]$$

$$= (mp+np, pa + pb + mc+ nc + ac + bc)$$

and
\[(m, a) (p, c) + (n, b) (p, c) = (mp, pa + mc + ac) + (np, pb + nc + bc)\]

Therefore

\[[(m, a) + (n, b)](p, c) = (m, a) (p, c) + (n, b) (p, c)\]

Similarly we can check it for right distributive law.

(vii)

\[(1, 0) (m, a) = (m, a) = (m, a) (1, 0)\]

Hence \((1, 0) = 1\) is unity of \(S\).

Hence \(S\) is a ring with unit element.

Consider the set

\[T = \{(0, a) \mid A \in R\}\]

Since

\[(0, a) + (0, b) = (0, a + b) \in T\]

\[0 = (0, 0) \in T\]

\[-(0, a) = (0, -a) \in T\]

and

\[(0, a)(0, b) = (0, ab) \in T,\]

therefore \(T\) is a subring of \(S\).

We define a mapping

\[f : R \rightarrow T\]

by

\[f(a) = (0, a), \ a \in R\]

Then

\[f(a+b) = (0, a+b)\]

\[= (0, a) + (0, b)\]

\[= f(a) + f(b)\]

and

\[f(ab) = (0, ab)\]

\[= (0, a)(0, b)\]

\[= f(a) + f(b)\]

Thus \(f\) is a ring homomorphism. Also,

\[f(a) = f(b) \Rightarrow (0, a) = (0, b)\]

\[\Rightarrow a = b.\]

Therefore \(f\) is an isomorphism and hence \(R\) can be imbedded in \(S\).

**Theorem.** Every integral domain can be imbedded in a field.

**Proof.** Let \(D\) be an integral domain and

\[S = \{(a,b) \mid a, b \in D, b \neq 0\}\]
be the set of the ordered pairs of \( D \). Then we claim that the relation
\[
R = \{ ((a,b), (c,d)) | (a,b), (c,d) \in S \text{ and } ad = bc \}
\]
is an equivalence relation.

(i) Since \( D \) is commutative, therefore \( ab = ba \) for all \( a, b \in D \).
Hence for all \( (a,b) \in S \)
\[
((a,b), (a,b)) \in R.
\]

(ii) **Symmetry.** If \( ((a,b), (c,d)) \in R \), then
\[
ad = bc
\]
\[
\Rightarrow \quad cb = da \quad \text{(by commutativity of } D)\]
\[
\Rightarrow \quad ((c,d), (a,b)) \in R.
\]

(ii) **Transitivity.** If \( ((a,b), (c,d)) \in R, ((c, d), (e,f)) \in R \) then \( ad = bc \) and \( cf = de \)
Therefore
\[
adf = bcf = bde
\]
\[
\Rightarrow \quad (af - be)d = 0
\]
\[
\Rightarrow \quad (af - be) = 0 \quad \text{(if } d \neq 0)\]
\[
\Rightarrow \quad af = be
\]
\[
\Rightarrow \quad ((a,b), (e,f)) \in R.
\]

We represent the equivalence class of \( (a,b) \) by the fraction \( \frac{a}{b} \). Thus
\[
\frac{a}{b} = \{ (c,d) | (c,d) \in S, \quad ((a,b), (c,d)) \in R \}
\]
Consider the set
\[
F = \{ \frac{a}{b} \mid a, b \in D, b \neq 0 \}
\]
Of these equivalence classes.

Let \( \frac{a}{b}, \frac{c}{d} \in F \). Then we define addition and multiplication in \( F \) as follows:
\[
\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}
\]
and
\[
\left( \frac{a}{b} \right) \left( \frac{c}{d} \right) = \frac{ac}{bd} .
\]
Since \( D \) is an integral domain and \( b \neq 0, d \neq 0 \). Therefore, \( bd \neq 0 \). Therefore \( \frac{ad + bc}{bd} \in F \).

Now we shall prove that this addition is well defined. To show it, it suffices to show that if
\[
\frac{a}{b} = \frac{a_1}{b_1}, \quad \frac{c}{d} = \frac{c_1}{d_1}
\]
then
\[
\frac{ad + bc}{bd} = \frac{a_1 d_1 + b_1 c_1}{b_1 d_1}
\]
that is
\[
a(d + bc) (b_1 d_1) = bd(a_1 d_1 + b_1 c_1)
\]
Now \((ad + bc)(b_1d_1) = adb_1d_1 + bcb_1d_1\)
\[= a(db_1)d_1 + b(cb_1)d_1\]
\[= ab_1d_1d_1 + bb_1c_1d_1\]  \hspace{1cm} (by commutativity of D)
\[= ba_1d_1d_1 + bb_1c_1d_1\]  \hspace{1cm} (using (i))
\[= bd(a_1d_1 + b_1c_1)\]

Therefore addition is well defined.

If \(\frac{a}{b} = \frac{a_1}{b_1}, \frac{c}{d} = \frac{c_1}{d_1}\) then
\[\frac{ac}{bd} = \frac{a_1c_1}{b_1d_1}\]

that is
\[acb_1d_1 = bda_1c_1\]

Now
\[acb_1d_1 = ab_1cd_1\]
\[= ba_1dc_1\]
\[= bda_1c_1\]

\(\therefore\) multiplication is also well defined.

We now prove that F is a field under these operations of addition and multiplications.

Let \(\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in F\). Then

(i) \(\left(\frac{a}{b} + \frac{c}{d}\right) + \frac{e}{f} = \frac{ad + bc}{bd} + \frac{e}{f} = \frac{(ad + bc)f + bde}{bdf}\)
\[= \frac{adf + bcf + bde}{bdf}\]

and
\[\frac{a}{b} + \left(\frac{c}{d} + \frac{e}{f}\right) = \frac{cf + de}{df}\]
\[= \frac{adf + bcf + bde}{bdf}\]

Therefore
\[\left(\frac{a}{b} + \frac{c}{d}\right) + \frac{e}{f} = \frac{a}{b} + \left(\frac{c}{d} + \frac{e}{f}\right)\]

(ii) \(\frac{0}{b} + \frac{a}{b} = \frac{0b + ab}{b^2} = \frac{ab}{b^2} = \frac{a}{b}\).

Similarly \(\frac{a}{b} + \frac{0}{b} = \frac{a}{b}\)

Therefore \(\frac{0}{b}\) is additive identity.
Thus every element of $F$ is invertible.

(iv) \[
\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}
\]

and \[
\frac{c}{d} + \frac{a}{b} = \frac{cb + da}{db} = \frac{bc + ad}{bd} \quad \text{(by commutativity of D)}
\]

(v) If \(\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in F\), then
\[
\left(\frac{a}{b} + \frac{c}{d}\right) \frac{e}{f} = \frac{ace}{bdf} = \frac{a \left(\frac{c}{d} + \frac{e}{f}\right)}{b}
\]

(vi) \[
\frac{a}{b} \left(\frac{c}{d} + \frac{e}{f}\right) = \frac{a}{b} \left(\frac{bf + df}{bd}\right)
\]
\[
= \frac{acf}{bdf} + \frac{ade}{bdf}
\]
\[
= \frac{ac}{bd} + \frac{ae}{bf}.
\]

Similarly it can be shown that
\[
\left(\frac{a}{b} + \frac{c}{d}\right) \frac{e}{f} = \frac{ae + ce}{bf + df}
\]

(vii) \[
\left(\frac{a}{b}\right) \left(\frac{a}{b}\right) = \left(\frac{aa}{ba}\right) = \frac{a}{b}
\]

and \[
\frac{a}{a} \cdot \frac{a}{b} = \frac{a}{b}.
\]

Hence \(\frac{a}{a} = 1\) is multiplicative identity.

(viii) \[
\left(\frac{a}{b}\right) \left(\frac{b}{a}\right) = \frac{ab}{ba} = 1
\]
\[
\left(\frac{b}{a}\right) \left(\frac{a}{b}\right) = \frac{ba}{ab} = \frac{ba}{ab} = 1
\]

Thus every element of $F$ is invertible.

(ix) \[
\left(\frac{a}{b}\right) \left(\frac{c}{d}\right) = \frac{ac}{bd}
\]
\[
= \left(\frac{c}{d}\right) \left(\frac{a}{b}\right).
\]

Hence $F$ is a field. This field $F$ is called Quotient field or field of fractions.

We define a function
\[f : D \to F\]
by
\[ f(a) = \frac{a}{1}, \ a \in D. \]

Then
\[ f(a+b) = \frac{a+b}{1} = \frac{a}{1} + \frac{b}{1} = f(a) + f(b) \]
and
\[ f(ab) = \frac{ab}{1} = \left( \frac{a}{1} \right) \left( \frac{b}{1} \right) = f(a) f(b). \]

Therefore \( f \) is a ring homomorphism. Also,
\[ f(a) = f(b) \Rightarrow \frac{a}{1} = \frac{b}{1} \Rightarrow a = b. \]

It follows therefore that \( f \) is an isomorphism. Hence \( D \) can be imbedded in \( F \).

**Definition.** The Quotient field of an integral domain: By the quotient field \( K \) of an integral domain \( D \) is meant the smallest field containing \( D \). Thus a field \( K \) is a quotient field of an integral domain \( D \) if \( K \) contains \( D \) and is itself contained in every field containing \( D \).

For example, field \( Q \) of rational numbers is the quotient field of the integral domain \( Z \) of integers.

*The quotient field of a finite integral domain coincides with itself.

**Definition.** Let \( F \) be a field. If a subring \( F_1 \) of \( F \) form a field under the induced compositions of addition and multiplication, then \( F_1 \) is called a subfield of \( F \).

For example, field \( Q \) of rational numbers is a subfield of the field \( R \) of real numbers. The field \( R \) is a subfield of the field \( C \) of complex numbers. Every field is a subfield of itself.

It is clear from the definition that a nonempty set \( K \) is a subfield of a field \( F \) if

(i) \( x, y \in K \Rightarrow x-y \in K \)
(ii) \( x \in K, y \in K, y \neq 0 \Rightarrow xy^{-1} \in K \).

**Characteristic of a field:** Let \( K \) be a field and \( e \) be the multiplicative identity of \( K \). Then, the mapping \( f: Z \rightarrow K \) defined by \( f(n) = ne, n \in Z \) is a ring homomorphism. For,
\[ f(m+n) = (m+n)e \]
\[ = (me) + (ne) \]
\[ = f(m) + f(n) \]
and
\[ f(mn) = (mn)e \]
\[ = (me)(ne) \]
\[ = f(m)f(n). \]

Let \( A \) be the kernel of this homomorphism. Then
\[ A = \{ n \mid f(n) = 0 \} \]
\[ = \{ n \mid ne = 0 \} \]
and
\[ \mathbb{Z}/A \simeq \text{Im}(f) = f(z). \]

But \( \text{Im } f \) is a subring of \( K \). Therefore, \( \text{Im}(f) \) is without zero divisor. It follows therefore that \( \mathbb{Z}/A \) is without zero divisor. Therefore either \( A = \{0\} \) or \( A \) is a prime ideal.

If \( A = \{0\} \), then
\[ ne = 0 \iff n = 0. \]

If \( A \) is a prime ideal then we can find a prime number \( p \) such that
\[ A = \ker f = < p > \quad (\text{ii}) \]
Hence from (i) and (ii)
\[ ne = 0 \iff p \mid n. \]

Thus we have seen that if \( K \) is a field, then one of the following two cases, holds

(i) \[ ne = 0 \iff n = 0 \]

(ii) \[ ne = 0 \iff p \mid n \quad \text{where } p \text{ is a prime.} \]

In the first case we say that the field \( K \) is of characteristic zero while in the second case, \( K \) is called a field of characteristic \( p \). Thus characteristic of a filed is zero or a prime number.

It is clear that a field of characteristic zero is infinite since in that case \( \mathbb{Z}/A = \mathbb{Z} \) and therefore \( \mathbb{Z} \simeq \text{Im}(f) \). Hence \( \text{Im}(f) \) and \( K \) are infinite.

**Example 1.** The characteristic of the field \( \mathbb{Q} \) of rational numbers is zero, since \( ne = 0 \Rightarrow n = 0 \). (\( \Theta e \neq 0 \)).

2. The characteristic of the field \( \mathbb{Z}/<p> \) is a prime number \( p \).

**Definition.** Fields with non-zero characteristic are known as Modular Fields.

**Definition.** A field is said to be prime if it has no subfield other than itself.

**Examples 1.** If \( p \) is a prime, then \( \mathbb{Z}/p\mathbb{Z} \) is a prime field. Additive group \( \mathbb{Z}/p\mathbb{Z} \). Hence \( \mathbb{Z}/p\mathbb{Z} \) is a prime field.

2. Field \( \mathbb{Q} \) of rational numbers is a prime field. To prove it let \( K \) be a subfield of \( Q \). Then \( 1 \in K \). Since \( K \) is an additive subgroup of \( Q \), therefore \( 1+1 = 2 \in K \). Similarly \( 3 \in K \). Now \( K \) being a field, every non-zero element of a \( K \) is invertible under multiplication. Therefore, \( ne \in K, n \neq 0 \Rightarrow \frac{1}{n} \in K \). Then \( m \in K, \frac{1}{n} \in K \Rightarrow \frac{m}{n} \in K \). Hence \( K \) contains all rational numbers. Hence \( K = \mathbb{Q} \) as a consequence of which \( Q \) is a prime field.

We have seen that the field \( \mathbb{Q} \) of rational numbers and \( \mathbb{Z}/p\mathbb{Z} \) are prime fields. Now we shall prove that up to isomorphism there are only two prime fields \( \mathbb{Q} \) and \( \mathbb{Z}/p\mathbb{Z} \).

**Proof.** Let \( K \) be any prime field and let \( e \) denote the unit element of the same. Since \( K \) is prime, the subfield generated by \( e \) must coincide with \( K \).

Consider the mapping \( f : \mathbb{Z} \to K \) defined by
\[ f(n) = ne, \quad n \in \mathbb{Z}. \]

This mapping is a ring homomorphism. For,
\[ f(n+m) = (n+m)e = ne + me = f(n) + f(m) \]
\[ f(nm) = (nm)e = (ne)(me) = f(n)f(m) \]
Let \( \ker f = A \). Since \( A \) is an ideal of \( \mathbb{Z} \) and every ideal in \( \mathbb{Z} \) is a principal ideal, therefore
\[
A = \{0\} \quad \text{or} \quad A = \langle p \rangle, \quad p \neq 0.
\]
If \( \ker f = A = \{0\} \), then \( f \) is one-to-one. Hence \( f(\mathbb{Z}) \) is a subring of \( K \) isomorphic to the integral domain \( \mathbb{Z} \). The prime field \( K \), being now the quotient field of the integral domain \( f(\mathbb{Z}) \) is isomorphic to the quotient field of \( \mathbb{Z} \). But the quotient field of \( \mathbb{Z} \) is the field \( \mathbb{Q} \) of rational numbers. Hence \( K \) is isomorphic to \( \mathbb{Q} \).

If \( \ker f = A = \langle p \rangle, \quad p \neq 0 \), then \( p \) is a prime number. In fact, if \( p = mn, \quad m \neq 1, n \neq 1 \) then
\[
0 = mne = (me)(ne).
\]
Hence \( me = 0 \) or \( ne = 0 \) which is impossible for each integer \( x \) such that \( ne = 0 \) is a multiple of \( p \). Hence \( p \) is a prime. Hence
\[
F(\mathbb{Z}) \simeq \mathbb{Z}/p\mathbb{Z}
\]
Since \( \mathbb{Z}/p\mathbb{Z} \) is a field, \( f(\mathbb{Z}) \) is itself a field necessarily identical with \( K \). Hence
\[
K \simeq \mathbb{Z}/p\mathbb{Z}
\]
Hence apart from isomorphism there are only two prime fields.

**Polynomial Rings**

**Definition.** Let \( A \) be an arbitrary ring. By a polynomial over a ring \( A \), is meant an ordered system \((a_0, a_1, a_2, \ldots, a_n, \ldots)\) of elements of \( A \) such that all except, at the most, a finite number of elements are zero.

Two polynomials \((a_0, a_1, a_2, \ldots, a_n, \ldots)\) and \((b_0, b_1, b_2, \ldots, b_n, \ldots)\) are said to be equal if and only if
\[
a_n = b_n, \quad n \in \mathbb{N}
\]
Let \( R \) be a ring and \( P \) be the set of all polynomials.

Let \((a_0, a_1, \ldots, a_n, \ldots)\) and \((b_0, b_1, b_2, \ldots, b_n, \ldots)\) be any two elements of \( P \). If
\[
a_n = 0 \quad \text{for all } n \geq j \quad \text{and} \quad b_n = 0 \quad \text{for all } n \geq k
\]
then
\[
a_n + b_n = 0 \quad \text{for all } n \geq \max(j, k)
\]
Thus all except at the most, a finite number of elements in the ordered system \((a_0+b_0, a_1+b_1, \ldots)\) are zero. Therefore \((a_0 + b_0, a_1+b_1, a_2+b_2, \ldots, a_n+b_n, \ldots) \in P \). Hence we can define addition composition in \( P \) by
\[
(a_0, a_1, a_2, \ldots, a_n) + (b_0, b_1, b_2, \ldots, b_n, \ldots) = (a_0 + b_0, a_1+b_1, a_2+b_2, \ldots, a_n+b_n, \ldots).
\]

Multiplication \( P \) is defined by
\[
(a_0, a_1, a_2, \ldots, a_n) (b_0, b_1, \ldots, b_n, \ldots) = (c_0, c_1, c_2, \ldots, c_n, \ldots)
\]
where
\[
c_0 = a_0b_0
c_1 = a_0b_1 + a_1b_0
c_2 = a_0b_2 + a_1b_1 + a_2b_0
\]
\[\vdots \]
\[
c_n = a_0b_n + a_1b_{n-1} + \ldots + a_nb_0 = \sum_{m=0}^{n} a_m b_{n-m}
\]
If $a_n = 0$ for all $n \geq j$ and $b_n = 0$ for all $n \geq k$, then $c_n = 0$ for all $n \geq (j+k)$.

Thus product of two polynomials is again a polynomial.

The set $P$ of all polynomials over a ring $R$ form a ring under these operations of addition and multiplication.

Let $(a_0, a_1, a_2, \ldots, a_n, \ldots), (b_0, b_1, b_2, \ldots), (c_0, c_1, c_2, \ldots) \in P$.

Then

(i) $(a_0, a_1, a_2, \ldots) + [(b_0, b_1, b_2, \ldots) + (c_0, c_1, c_2, \ldots)]$

$= (a_0, a_1, a_2, \ldots) + [(b_0 + c_0, b_1 + c_1, b_2 + c_2, \ldots)]$

$= (a_0 + b_0 + c_0, a_1 + b_1 + c_1, a_2 + b_2 + c_2, \ldots)$

$= [(a_0, a_1, a_2, \ldots) + (b_0, b_1, b_2, \ldots)] + (c_0, c_1, c_2, \ldots)$

(ii) $(a_0, a_1, a_2, \ldots) + (0, 0, 0, \ldots) = (a_0 + 0, a_1 + 0, a_2 + 0, \ldots)$

$= (a_0, a_1, a_2, \ldots)$

and

$(0, 0, 0, \ldots) + (a_0, a_1, a_2, \ldots) = (0 + a_0, 0 + a_1, 0 + a_2, \ldots)$

$= (a_0, a_1, a_2, \ldots)$

(iii) $(a_0, a_1, a_2, \ldots) + (-a_0, -a_1, -a_2, \ldots)$

$= (a_0 - a_0, a_1 - a_1, a_2 - a_2, \ldots)$

$= (0, 0, 0, \ldots)$

and

$(-a_0, -a_1, -a_2, \ldots) + (a_0, a_1, a_2, \ldots)$

$= (0, 0, 0, \ldots)$

(iv) $(a_0, a_1, a_2, \ldots) + (b_0, b_1, b_2, \ldots) = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \ldots)$

$= (b_0 + a_0, b_1 + a_1, b_2 + a_2, \ldots)$

$= (b_0, b_1, b_2, \ldots) + (a_0, a_1, a_2, \ldots)$

(v) $[(a_0, a_1, a_2, \ldots) (b_0, b_1, b_2, \ldots)] (c_0, c_1, c_2, \ldots)$

$= (d_0, d_1, d_2, \ldots) (c_0, c_1, c_2, \ldots)$

where

$$d_n = \sum_{j+k=m} a_j b_k$$

$$= (e_0, e_1, e_2, \ldots)$$

where

$$e_m = \sum_{p+q=m} d_p c_q$$

$$= \sum_{p+q=m} \left( \sum_{j+k=p} a_j b_k \right) c_q$$

$$= \sum_{j+k+q=m} a_j b_k c_q.$$
(a₀, a₁, a₂,...) [(b₀, b₁, b₂,...) (c₀, c₁, c₂,...)] = (f₀, f₁, f₂,...)

where

\[ f_m = \sum_{j+k+q=m} a_j b_k c_q \]

Hence

\[ [(a₀, a₁, a₂,...) (b₀, b₁,...)] (c₀, c₁, c₂,...) = (a₀, a₁, a₂,...) [(b₀, b₁, b₂,...) (c₀, c₁, c₂,...)] \]

(vi) \[(a₀, a₁, a₂,...) [(b₀, b₁, b₂,...) + (c₀, c₁, c₂,...)] = (a₀, a₁, a₂,...) (b₀ + c₀, b₁ + c₁, b₂ + c₂,...) = (d₀, d₁, d₂,...) \]

where

\[ d_m = \sum_{j+k=m} a_j (b_k + c_k) \]

\[ = \sum_{j+k=m} a_j b_k + \sum_{j+k=m} a_j c_k \]

\[ = f_m + g_m \text{, say} \]

Also

\[(a₀, a₁, a₂,...) (b₀, b₁, b_n) = (f₀, f₁, f₂,...) , \]

\[(a₀, a₁, a₂,...) (c₀, c₁, c₂,...) = (g₀, g₁, g₂,...) \]

Hence

\[(a₀, a₁, a₂,...) [(b₀, b₁, b₂,...) + (c₀, c₁, c₂,...)] = (a₀, a₁, a₂,...) (b₀, b₁, b₂,...) + (a₀, a₁, a₂,...) (c₀, c₁,...) \]

Hence P is a ring. We call this ring of polynomials as polynomial ring over R and it is denoted by R[x]. Let

\[ Q = \{(a, 0, 0,...) | a \in R \} \]

Then a mapping \( f : R \rightarrow Q \) defined by \( f(a) = (a, 0, 0,...) \) is an isomorphism. In fact,

\[
f(a+b) = (a + b, 0, 0,...) \\
= (a, 0, 0,...) + (b, 0, 0,...) \\
= f(a) + f(b) ,
\]

\[
f(ab) = (ab, 0, 0,...) \\
= (a, 0, 0,...) (b, 0, 0,...) \\
= f(a) f(b) 
\]

and

\[
f(a) = f(b) \Rightarrow (a, 0, 0,...) = (b, 0, 0,...) \\
\Rightarrow a = b .
\]

Hence

\[ R \cong Q \] (i)

So we can identify the polynomial \((a, 0, 0,...)\) with a.

If we represent \((0, 1, 0,...)\) by \(x\) then we can see that

\[ x^2 = (0, 0, 1, 0,...) \]
\[ x^3 = (0, 0, 0, 1, \ldots) \]
\[ \ldots \ldots \ldots \]
\[ x^n = \left( \begin{array}{cccc}
0 & 0 & \cdots & 0 \\
1 & 0 & \cdots & 0
\end{array} \right) \quad \text{n terms} \]

Therefore for \((a, 0, 0, \ldots) \in \mathbb{Q}\) we have
\[
\begin{align*}
(a, 0, 0, \ldots) x & = (0, a, 0, \ldots) \\
(a, 0, 0, \ldots) x^2 & = (0, 0, a, \ldots) \\
\ldots \ldots \ldots \ldots
(a, 0, 0, \ldots) x^n & = \left( \begin{array}{cccc}
0 & 0 & \cdots & 0 \\
a & 0 & \cdots & 0
\end{array} \right) \quad \text{n terms}
\end{align*}
\]

(ii)

If \((a_0, a_1, a_2, \ldots, a_n, 0, \ldots)\) be any arbitrary element of the polynomial ring \(P\), then by (ii) we have
\[
\begin{align*}
(a_0, a_1, a_2, \ldots, a_n, 0, \ldots) & = (a_0, 0, \ldots) + (0, a_1, \ldots) + \ldots + \left( \begin{array}{cccc}
0 & 0 & \cdots & 0 \\
1 & 0 & \cdots & 0
\end{array} \right) \quad \text{n terms}
\end{align*}
\]

Hence every element \((a_0, a_1, a_2, \ldots)\) of \(P\) can be denoted by
\[ a_0 + a_1 x + a_2 x^2 + \ldots a_n x^n. \]

* The numbers \(a_0, a_1, \ldots, a_n\) are called coefficients of the polynomial. If the coefficient \(a_n\) of \(x^n\) is non-zero, then it is called leading coefficient of \(a_0 + a_1 x + \ldots a_n x^n\).

* A polynomial consisting of only one term \(a_0\) is called constant polynomial.

**Example.** If \(R\) is a commutative ring with unity, prove that \(R[x]\) is also a commutative ring with unity.

**Degree of Polynomial.** Let \(f(x) = a_0 + a_1 x + \ldots a_n x^n\) be a polynomial. If \(a_n \neq 0\), then \(n\) is called the degree of \(f(x)\). We denote it by \(\deg f(x) = n\).

It is clear that degree of a constant polynomial is zero.

If
\[ f(x) = a_0 + a_1 x + a_2 x^2 + \ldots a_m x^m, \quad a_m \neq 0 \]
and
\[ g(x) = b_0 + b_1 x + \ldots b_n x^n, \quad b_n \neq 0 \]
are two elements of \(R[x]\), then
\[ \deg f(x) = m \quad \text{and} \quad \deg g(x) = n \]
and
\[ f(x) + g(x) = (a_0 + a_1 x + a_2 x^2 + \ldots + a_m x^m) + (b_0 + b_1 x + b_2 x^2 + \ldots + b_n x^n) \]

If \(m = n\) and \(a_m + b_m \neq 0\), then
\[ f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + \ldots + (a_m + b_m)x^m \]

Therefore in this case
\[ \deg [f(x) + g(x)] = m. \]

It is also clear that if \(m = n\) and \(a_m + b_m = 0\), then
\[ \deg [f(x) + g(x)] < m. \]
If \( m > n \), then
\[
 f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + \ldots + (a_n + b_n)x^n + a_{n+1}x^{n+1} + \ldots + a_mx^m
\]

Therefore in this situation
\[
 \deg [f(x) + g(x)] = m
\]
Similarly it can be seen that if \( m < n \), then
\[
 \deg [f(x) + g(x)] = n
\]
It follows therefore that if \( m \neq n \), then
\[
 \deg [f(x) + g(x)] = \max (m, n)
\]
Also,
\[
 f(x) g(x) = a_0b_0 + (a_0b_1 + a_1b_0)x + \ldots + a_mb_nx^{m+n}
\]
Therefore
\[
 \deg[f(x) g(x)] = \begin{cases} 
 m+n & \text{if } a_mb_n \neq 0 \\
 < m+n, & \text{where } a_mb_n = 0 .
\end{cases}
\]
If \( R \) is without zero divisor, then
\[
 a_mb_n \neq 0 \quad \text{since } a_m \neq 0, \ b_n \neq 0 .
\]
Hence for such a ring \( R \) we have
\[
 \deg [f(x) g(x)] = m+n = \deg f(x) + \deg g(x)
\]
If \( R \) is without zero divisor and \( f(x) \) and \( g(x) \) are non-zero polynomial of \( R[x] \), then
\[
 \deg f(x) \leq \deg [f(x) g(x)] \quad (\Theta \deg g(x) \geq 0).
\]

**Theorem.** If \( R \) is an integral domain, then so is also polynomial ring \( R[x] \).

**Proof.** \( R \) is a commutative ring with unity. Therefore \( R[x] \) is commutative with unit element. It suffices to prove that \( R[x] \) is without zero divisor. Let
\[
 f(x) = \sum_{i=0}^{m} a_ix^i, \quad a_m \neq 0
\]
and
\[
 g(x) = \sum_{i=0}^{n} b_ix^i, \quad b_n \neq 0 ,
\]
be two non-zero polynomials of \( R[x] \) and let \( m \) and \( n \) be their degrees respectively.

Since \( R \) is an integral domain and \( a_m \neq 0 , \ b_n \neq 0 \), therefore \( a_mb_n \neq 0 \). Hence \( f(x) g(x) \neq 0 \). Hence \( R[x] \) is without zero divisor and therefore an integral domain.

**Division Algorithm for polynomials over a field.**

**Theorem.** Corresponding to any two polynomials \( f(x) \) and \( g(x) \neq 0 \) belonging to \( F[x] \) there exist uniquely two polynomials \( q(x) \) and \( r(x) \) also belonging to \( F[x] \) such that
\[
 f(x) = g(x) q(x) + r(x)
\]
where
\[
 r(x) = 0 \quad \text{or } \deg r (x) < \deg g(x) .
\]

**Proof.** Let
\[
 f(x) = \sum_{i=0}^{m} a_ix^i, \quad a_m \neq 0
\]
\[ g(x) = \sum_{i=0}^{n} b_i x^i, \ b_n \neq 0. \]

Then either

(i) \( \deg f(x) < \deg g(x) \)

or

(ii) \( \deg f(x) \geq \deg g(x) \)

In the first case we write

\[ f(x) = g(x) q(x) + r(x) \]

so that \( q(x) = 0 \) and \( r(x) = f(x) \).

In respect of the second case we shall prove the existence of \( q(x) \) and \( r(x) \) by mathematical induction on the degree of \( f(x) \). If \( \deg f(x) = 1 \), then the existence of \( q(x) \) and \( r(x) \) is obvious. Let us suppose that the result is true when \( \deg f(x) \leq m-1 \). If

\[ h(x) = f(x) - \left( \frac{a_m}{b_n} \right) x^{m-n} g(x) \quad (iii) \]

\[ f(x) = a_0 + a_1 x + \ldots + a_m x^m \]

\[ = a_m b_n^{-1} x^{m-n} (b_0 + b_1 x + \ldots + b_n x^n) \]

\[ + (a_{m-1} - a_m b_n^{-1} b_{n-1}) x^{m-1} + (a_{m-2} - a_m b_n^{-1} b_{n-2}) x^{m-2} \]

\[ = a_m b_n^{-1} x^{m-n} g(x) + h(x) \]

then \( \deg h(x) \leq m-1 \).

Hence by supposition

\[ h(x) = g(x) q_1(x) + r(x), \quad (iv) \]

where \( r(x) = 0 \) or \( \deg r(x) < \deg g(x) \).

From (iii) and (iv) we have

\[ f(x) - \left( \frac{a_m}{b_n} \right) x^{m-n} g(x) = g(x) q_1(x) + r(x) \]

That is,

\[ f(x) = g(x) [q_1(x) + \left( \frac{a_m}{b_n} \right) x^{m-n}] + r(x) \]

\[ = g(x) q(x) + r(x) \]

where

\[ q(x) = q_1(x) + \left( \frac{a_m}{b_n} \right) x^{m-n} \]

Thus existence of \( q(x) \) and \( r(x) \) is proved.

Now we shall prove the uniqueness of \( q(x) \) and \( r(x) \).

Let us suppose that \( q_1(x) \) and \( r_1(x) \) are two polynomials belonging to \( F[x] \) such that

\[ f(x) = g(x) q_1(x) + r_1(x) \]

where \( r_1(x) = 0 \) or \( \deg r_1(x) < \deg g(x) \).

But by the statement of the theorem, \( q(x) \) and \( r(x) \) are two elements of \( F(x) \) such that

\[ f(x) = g(x) q(x) + r(x) \]

where \( r(x) = 0 \) or \( \deg r(x) < \deg g(x) \).

Hence
that is,
\[
g(x) [q(x) - q_1(x)] = r_1(x) - r(x) \tag{v}
\]
But
\[
\deg g(x) [q(x) - q_1(x)] \geq n
\]
and
\[
\deg [r_1(x) - r(x)] < n.
\]
Hence (v) is possible only when
\[
g(x) [q(x) - q_1(x)] = 0
\]
and
\[
r_1(x) - r(x) = 0
\]
That is, when
\[
q(x) = q_1(x) \text{ and } r(x) = r_1(x)
\]
Hence \( q(x) \) and \( r(x) \) are unique.

With the help of this theorem we shall prove that a polynomial domain \( F[x] \) over a field \( F \) is a principal ideal domain.

**Theorem.** A polynomial domain \( F[x] \) over a field \( F \) is a principal ideal domain.

**Proof.** Let \( S \) be any ideal of \( F[x] \) other than the zero ideal and let \( g(x) \) be a polynomial of lowest degree belonging to \( S \). If \( f(x) \) is an arbitrary polynomial of \( S \), then by division algorithm there exist uniquely two polynomials \( q(x) \) and \( r(x) \) belonging to \( F[x] \) such that
\[
f(x) = g(x) q(x) + r(x)
\]
where \( r(x) = 0 \) or \( \deg r(x) < \deg g(x) \).
Thus
\[
r(x) = f(x) - g(x) q(x) \in S.
\]
Also, since \( g(x) \) is a polynomial of lowest degree belonging to \( S \), we see that \( \deg r(x) \) cannot be less than of \( g(x) \). Thus \( r(x) = 0 \) and we have
\[
f(x) = g(x) q(x)
\]
Since \( f(x) \) is arbitrary polynomial belonging to \( S \), therefore
\[
S = (g(x))
\]
Hence \( F[x] \) is principal ideal domain.

**Example.** Show that the polynomial ring \( I[x] \) over the ring \( I \) of integers is not a principal ideal ring.

To establish this we have to produce an ideal of \( I[x] \) which is not a principal ideal. In fact we shall show that the ideal \( (x, q) \) of the ring \( I[x] \) generated by two elements \( x \) and \( q \) of \( I[x] \) is not a principal ideal.

Let if possible \( (x, q) \) be a principal ideal generated by a member \( f(x) \) of \( I[x] \) so that we have
\[
(x, q) = (f(x))
\]
Thus we have relations of the form
\[
q = f(x) g(x)
x = f(x) h(x)
\]
where \( g(x) \) and \( h(x) \) are members of \( I[x] \). These imply
\[
\deg f(x) + \deg g(x) = \deg q = 0 \tag{i}
\]
\[
\deg f(x) + \deg h(x) = \deg x = 1 \tag{ii}
\]
From (ii) we get
\[
\text{deg } f(x) = 0 \text{ and deg } g(x) = 0
\]
So \(f(x)\) and \(g(x)\) are non-zero constant polynomials i.e. are non-zero integers.
Again since
\[
f(x)g(x) = 2
\]
where \(f(x)\) and \(g(x)\) are non-zero integers, we have the following four alternatives
\[
\begin{align*}
f(x) &= 1, \quad g(x) = 2 \\
f(x) &= -1, \quad g(x) = -2 \\
f(x) &= 2, \quad g(x) = 1 \\
f(x) &= -2, \quad g(x) = -1.
\end{align*}
\]
If
\[
f(x) = 1 \text{ or } -1,
\]
we have
\[
(f(x)) = I[x].
\]
Thus we arrive at a contradiction in that
\[
(f(x)) = I[x]
\]
and
\[
I[x] \neq (x, 2).
\]
Now suppose that \(f(x) = \pm 2\), then \(x = f(x)h(x)\) and we have a relation of the form \(x = \pm 2 (c_0 + c_1x + \ldots)\). This gives \(1 = \pm 2 c_1\) which is again a contradiction in as much as there is no integer \(c_1\) such that \(1 = \pm 2c_1\). Thus it has been shown that \((x, 2)\) is not a principal ideal.

**Unique Factorisation Domain**

**Definition.** An element \(a\) is called a unit if there exists \(b\) such that \(ab = 1\).
Let \(D\) be an integral domain. Then multiplicative identity of \(D\) is a divisor of each element of the same. In fact we have
\[
a = 1.a \quad \text{for all } a \in D \\
\Rightarrow 1|a \quad \text{for all } a \in D.
\]
Besides 1, there may also exist other elements which are divisors of each element of the domain. In fact if \(e\) is any invertible element and \(a\) be any arbitrary element, then
\[
a = e(e^{-1}a) \Rightarrow e|a.
\]
Thus all invertible element are divisors of every element of the domain \(D\).

**Definition.** The invertible elements of an integral domain are known as its units.
Thus each unit is a divisor of every element of the domain.

* An element \(a\) is a unit of an integral domain iff it has a multiplicative inverse.

**Proof.** Let \(a\) be a unit. The \(a | 1\), where 1 is the unit of the integral domain \(D\). Hence \(1 = ab\). Hence \(a\) has a multiplicative inverse \(b\).
Again, if the multiplicative inverse of \(a\) is \(b\) then \(ab = 1\). Hence \(a | 1\) and \(1 | a\) for every \(a \in D\) showing that \(a\) is a unit.
For example each non-zero element of a field is a unit thereof.
\(\pm 1\) are the only two units in domain \(I\) of integers.
Definition. A non-zero element of integral domain \( D \), which is not a unit and which has no proper divisors is called a prime or irreducible (indecomposable) element.

Definition. An element \( a \) is said to be an associate of \( b \) if \( a \) is a divisor of \( b \) and \( b \) is a divisor of \( a \).

For example each of 3 and \(-3\) is a divisor of the other in the domain \( I \) of integrals.

Definition. A ring \( R \) is called a factorisation domain if every non-zero non-unit element of the same can be expressed as a product of irreducible elements. Thus if \( a \) is non-zero unit element of a F.D. then 
\[
    a = p_1 p_2 p_3 \ldots p_n,
\]
where \( p_i \)'s are irreducible elements.

Definition. A F.D. is called a unique factorisation domain if whenever 
\[
    a = p_1 p_2 p_3 \ldots p_n = q_1 q_2 \ldots q_s
\]
then \( r = s \) and after rearrangement, if necessary, 
\[
    p_1 \sim q_1, p_2 \sim q_2, \ldots, p_r \sim q_s.
\]

Definition. An integral domain \( D \) is said to be principal ideal domain if every ideal \( A \) in \( D \) is principal ideal.

Theorem. A principal ideal domain is a unique factorisation domain.

Proof. Firstly we show that principal ideal domain is a factorisation domain.

Let \( a \) be a non-zero non-unit element of a principal ideal domain \( D \). If \( a \) is prime we are done. If \( a \) is not a prime, there exist two non-unit elements \( b \) and \( c \) such that 
\[
    a = bc
\]
\[
    \Rightarrow a \in (b)
\]
\[
    \Rightarrow (a) \subseteq (b), (b) \neq (a).
\]
In case \( b, c \) are both irreducible, then again we have finished. If they are not prime, we continue as above. That is, there exists two non-unit elements \( c \) and \( d \) such that 
\[
    b = cd
\]
\[
    \Rightarrow b \in (c)
\]
\[
    \Rightarrow (b) \subseteq (c), (b) \neq (c)
\]
Thus two cases arise:

(i) After a finite number of steps, we arrive at an expression of \( a \) as a product of irreducible elements.

(ii) Howsoever far we may continue, we always have a composite element occurring as a factor in the expression of \( a \) as product of elements of \( D \).

In case (i) we have finished.

In case (ii), there exists an infinite system of elements \( a_1, a_2, \ldots, a_n, \ldots \) such that 
\[
    (a_1) \subseteq (a_2) \subseteq (a_3) \ldots \subseteq (a_n) \subseteq \ldots \quad (I)
\]
no two of these principal ideals being the same.

Consider the union 
\[
    A = \bigcup(a_n)
\]
We assert that \( A \) is an ideal of \( D \). In fact 
\[
    0 \in (a_1) \Rightarrow 0 \in A
\]
\[
    \Rightarrow A \neq \emptyset.
\]
If \( x, y \in A \), then there exist integers \( i \) and \( j \) such that
\[
x \in (a_i), \ y \in (a_j)
\]
Without loss of generality suppose that \( i \geq j \). Then \( x, y \in (a_i) \). This implies that \( x - y \in (a_i) \) and \( \alpha \in (a_i) \) where \( \alpha \in D \). Hence \( x-y, \alpha x \in A \).

Since \( D \) is a principal ideal domain, therefore \( \exists \) an element \( \beta \) of \( D \) such that
\[
A = (\beta).
\]
There exists, therefore, an ideal member \( (a_m) \) of the system such that
\[
\beta \in (a_m)
\]
and accordingly
\[
\beta \in (a_n) \quad \text{for all } n \geq m \\
\Rightarrow (\beta) \subseteq (a_n) \quad \text{for all } n \geq m \quad \text{(II)}
\]
Also since \( (\beta) \) is the union of the ideals, we have
\[
(\beta) \supset (a_n) \quad \text{for all } n \quad \text{(III)}
\]
Thus from (II) and (III)
\[
(\beta) = (a_n) \quad \text{for all } n \geq m,
\]
\[
\Rightarrow (a_m) = (a_{m+1}) = (a_{m+2}) = \ldots
\]
which is a contradiction to (I). Hence case (ii) cannot arise.

Thus we have proved that every non-zero non-unit element of a principal ideal domain is expressible as a product of prime element. Hence \( D \) is a F.d.

To prove the uniqueness, let
\[
a = p_1 p_2 \ldots p_t = q_1 q_2 \ldots q_s \quad \text{(IV)}
\]
where each \( p \) and \( q \) is prime. We shall prove the result by induction on \( r \). The result is obvious if \( r = 1 \).

Suppose now that the result is true for each natural number \( < r \). Since \( D \) is a principal ideal domain, every prime element generates a prime ideal. Therefore \( p_1 p_2 \ldots p_n \in (p_1) \) which implies \( q_1 q_2 \ldots q_s \in (p_1) \)

Therefore one of the factors \( q_1 q_2 \ldots q_s \) should belong to \( (p_1) \). Without loss of generality say, \( q_1 \in (p_1) \). Then \( p_1 | q_1 \). As \( q_1 \) is prime, this implies \( q_1 / p_1 \) and therefore \( p_1 \) and \( q_1 \) are associates. Let
\[
q_1 = e_1 p_1 \quad \text{(V)}
\]
where \( e_1 \) is a unit.

From (IV) and (V) we have
\[
p_2 p_3 \ldots p_t = (e_1 q_2) q_3 \ldots q_s \quad \text{(VI)}
\]
By the assumed hypothesis
\[
r-1 = s-1
\]
and each factor, on the right of (VI) is an associate of some factor on the left and vice-versa. This proves the theorem.

**Theorem.** In a principal ideal domain a prime element generates a maximal ideal.

**Proof.** Let \( p \) be a prime element in a principal ideal domain \( R \) and let
\[
p = (p)
\]
be an ideal of \( R \) generated by \( p \).
Let $p \nmid q$ where $Q = (a), a \in R$.

Now since $p$ is a prime, greatest common divisor of $a$ and $p$ is $p$ or $1$. If $(a, p) = p$ then $p \mid a$ and so

\[
\begin{align*}
    a & \in (p) = p \\
    \Rightarrow (a) & \subseteq p \\
    \Rightarrow Q & \subseteq p
\end{align*}
\]

But then $Q = p$ which is not the case. Therefore g.c.d. of $a$ and $p$ is one. Thus there exist $x$ and $y$ such that

\[1 = ax + py\]

Let us suppose that $b \in R$.

Now $bpy \in p \subseteq Q$ and $bax \in Q$

\[\therefore b \in Q\]

But $Q$ being an ideal of $R$ we have

\[Q \subseteq R\]

Hence \[Q = R\]

This proves that $p$ is maximal.

**Cor.** If $D$ is a P.I.D and $p$ is a prime, then $(p)$ is a prime ideal, in fact, since for a commutative ring $D$ every maximal ideal is a prime ideal.

**Euclidean Domain.** An integral domain $R$ is said to be a Euclidean domain (Euclidean ring) if there exists a mapping $\phi$ of the set of non-zero members of $R$ into the set of positive integers such that if $a, b$ be any two non-zero members of $R$ then

(i) there exists $q, r \in R$ such that

\[a = bq + r\]

where either $r = 0$ or $\phi(r) < \phi(b)$

(ii) $\phi(ab) \geq \phi(a)$ or $\phi(b)$.

**Example 1.** The domain $I$ of integer is Euclidean, for the mapping $\phi$ defined by

\[\phi(a) = |a|\]

satisfies the properties in question.

2. The domain $K[x]$ of polynomials over a field $K$ is Euclidean with the mapping defined by

\[f(ax) = 2^{\deg ax} \text{ where } a(x) \in K[x]\]

**Theorem.** Euclidean domain is a principal ideal domain.

**Proof.** Let $D$ be any Euclidean domain and $\phi$ a mapping referred to in the definition. Let $I$ be any ideal of $D$. If $I$ is zero ideal, then it is a principal ideal. Now suppose that $I \neq (0)$ so that it contains some non-zero members.

Consider the set of $\phi$ images of the non-zero members of $I$ which are all positive integers. Let $a \neq 0$ be a member of $I$ so that $\phi(a)$ is minimal in all the $\phi$ images.

Let $b$ be any arbitrary member of $I$. Then there exist two members $q$ and $r$ of $D$ such that

\[b = qa + r\]

where either $r = 0$ or $\phi(r) < \phi(a)$
The possibility $\phi(r) < \phi(a)$ is ruled out in respect of the choice of $a$. Therefore, $r = 0$ and we have

$$b = aq$$

$$\Rightarrow \quad I = (a)$$

and $I$ is accordingly a principal ideal.

**Note:** Since P.I.D. is U.F.D., it follows that Euclidean domain is unique factorisation domain.

*We know that a polynomial domain $F[x]$ over a field $F$ is a principal ideal domain, therefore $F[x]$ is also a unique factorisation domain.

**Definition.** Let $D[x]$ be a polynomial ring over a unique factorisation domain $D$ and let $f(x) = a_0 + a_1x + \ldots + a_nx^n$ be a polynomial belonging to $D[x]$. Then $f(x)$ is called primitive if the greatest common divisor of $a_0, a_1, \ldots, a_n$ is 1.

**Definition.** The content of the polynomial $f(x) = a_0 + a_1x + \ldots + a_nx^n$ is the greatest common divisor of $a_0, a_1, \ldots, a_n$.

If a polynomial $f(x) = c g(x)$ where $g(x)$ is primitive polynomial, then $c$ is called content of $f(x)$.

**Definition.** A polynomial $p(x)$ in $F[x]$ is said to be irreducible over $F$ if whenever $p(x) = a(x) b(x) \in F[x]$ then one of $a(x)$ or $b(x)$ has degree zero (i.e. is a constant).

**Definition.** Let $D[x]$ be the polynomial ring over a unique factorisation domain $D$. Then a polynomial $f(x) \in D[x]$ is called primitive if the set $\{a_0, a_1, \ldots, a_n\}$ of coefficients of $f(x)$ has no common factor other than a unit. For example $x^3 - 3x + 1$ is a primitive member of $I[x]$ but the polynomial $3x^3 - 6x + 3$ is not a primitive member of $I[x]$ since in the later case 3 is a common factor.

* $f(x) \in D[x]$ is called primitive if the g.c.d. of $a_0, a_1, \ldots, a_n$ is 1. Every irreducible polynomial is necessarily primitive but the converse need not be true. For example the primitive polynomial $x^2 + 5x + 6$ is reducible since $x^2 + 5x + 6 = (x+2)(x+3)$.

**Lemma 1.** The product of two primitive polynomials is primitive.

**Proof.** Let $f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_mx^m$ and $g(x) = b_0 + b_1x + b_2x^2 + \ldots + b_nx^n$ be two primitive polynomials belonging to $D[x]$. Let

$$(h(x) = f(x) g(x)) = c_0 + c_1x + c_2x^2 + \ldots + c_{m+n}x^{m+n}$$

Let if possible, a prime element $p$ be a common divisor of each of the coefficients of the product $f(x) g(x)$.

Also let $a_i$ and $b_j$ be the first coefficients of $f(x)$ and $g(x)$ which are not divisible by $p$. Then

$$c_{i+j} = a_i b_j + a_i-1 b_{i+1} + a_i-2 b_{i+2} + \ldots + a_0 b_{i+j} + a_{i+1} b_{i-1} + a_{i+2} b_{i-2} + \ldots + a_{i+j} b_0$$

$$\Rightarrow \quad a_i b_j = c_{i+j} - (a_{i-1} b_{j+1} + a_{i-2} b_{j+2} + \ldots) - (a_{i+1} b_{j-1} + a_{i+2} b_{j-2} + \ldots)$$

Since $p$ is a divisor of each of the terms on the right, we have

$$p | a_i b_j$$

$$\Rightarrow \quad p | a_i \quad \text{or} \quad p | b_j$$

so that we arrive at a contradiction. Hence the Lemma.

**Lemma 2.** If $f_1(x)$ and $f_2(x)$ are two primitive members of $D[x]$ and are also associates in $K[x]$, then they are also associates in $D[x]$, $K$ being the quotient field of the domain $D$.

**Proof.** Since $f_1(x)$ and $f_2(x)$ are associates in $K[x]$, we have
\[ f_1(x) = kf_2(x) \] where \( 0 \neq k \in K \)

We have \( k = gh^{-1} \) where \( g \in D, \ h \in D \)

\[ \therefore hf_1(x) = gf_2(x) \]

\[ \therefore f_1(x) \sim f_2(x) \text{ in } D[x] \quad (\text{Application of Lemma III}). \]

**Lemma 3.** Every non-zero member \( f(x) \) of \( D[x] \) is expressible as a product \( cg(x) \) of \( c \in D \) and of a primitive member \( g(x) \) of \( D[x] \) and this expression is unique apart from the differences in associateness.

**Proof.** Let \( c \) be the H.C.F. of the set

\[ \{ a_0, a_1, \ldots, a_i, \ldots, a_n \} \]

of the coefficients of \( f(x) \).

Let

\[ a_i = cb_i, \ 0 \leq i \leq n \]

Consider the set

\[ \{ b_0, \ldots, b_i, \ldots, b_n \} \]

This set has no common factor other than units. Thus

\[ g(x) = \sum_{i=0}^{n} b_i x^i \]

is a primitive polynomial member of \( D[x] \) and we have \( f(x) = cg(x) \) which expresses \( f(x) \) as required.

We now attend to the proof of the uniqueness part of the theorem.

If possible let

\[ f(x) = cg(x) \]

\[ f(x) = dh(x) \]

where \( g(x) \) and \( h(x) \) are primitive members of \( D[x] \).

We have therefore

\[ cg(x) = dh(x) \]

\[ \Rightarrow cb_i = dc_i \]

This implies that each prime factor of \( c \) is a factor of \( dc_i \) for all \( 0 \leq i \leq n \). This prime factor of \( c \) must not, however be a factor of some \( c_i \).

It follows that each prime factor of \( c \) is a factor of \( d \Rightarrow \) that \( c \) is a factor of \( d \).

Similarly, it follows that \( d \) is a factor of \( c \). Thus \( c \) and \( d \) are associates. Let \( c = ed \) where \( e \) is a unit.

Also since

\[ cg(x) = dh(x) \]

it follows that

\[ eg(x) = h(x) \]

implying that \( g(x) \) and \( h(x) \) are associates.

Hence the lemma.

**Definition.** A polynomial \( p(x) \) in \( F[x] \) is said to be irreducible over \( F \) if whenever \( p(x) = a(x) b(x) \), with \( a(x), b(x) \in F[x] \), then one of \( a(x) \) or \( b(x) \) has degree zero (i.e. is constant).
Lemma 4. If \( f(x) \) is an irreducible polynomial of positive degree in \( D[x] \), it is also irreducible in \( K[x] \) where \( K \) is the quotient field of \( D \).

**Proof.** Let if possible, \( f(x) \) be reducible in \( K[x] \) so that we have a relation of the form

\[
f(x) = g(x) h(x)
\]

where \( g(x), h(x) \) are in \( K[x] \) and are of positive degree.

Now

\[
g(x) = \frac{a_1}{b_1} g_1(x)
\]

\[
h(x) = \frac{a_2}{b_2} h_1(x)
\]

where \( a_1, b_1, a_2, b_2 \in D \) and \( g_1(x) \) and \( h_1(x) \) are primitive in \( D[x] \).

Thus we have

\[
f(x) = \frac{a_1 a_2}{b_1 b_2} g_1(x) h_1(x)
\]

\[
\Rightarrow (b_1 b_2) f(x) = (a_1 a_2) g_1(x) h_1(x)
\]

But by Lemma 1, \( g_1(x) h_1(x) \) is primitive. The constant of right hand side in \( a_1 a_2 \). Also \( f(x) \) being irreducible in \( D[x] \) is primitive and the constant of the left hand side is \( b_1 b_2 \). Therefore, \( a_1 a_2 = b_1 b_2 \).

Therefore

\[
f(x) = g_1(x) h_1(x)
\]

This contradicts the fact that \( f(x) \) is irreducible in \( D[x] \).

Therefore \( f(x) \) is irreducible in \( K[x] \).

**Theorem.** The polynomial ring \( D[x] \) over a unique factorisation domain \( D \) is itself a unique factorisation domain.

**Proof.** Let \( a(x) \) be any non-zero non-unit member of \( D[x] \). We have

\[
a(x) = g a_0(x)
\]

where \( g \in D \) and \( a_0(x) \) is a primitive polynomial belonging to \( D[x] \).

Since \( D \) is a U.F.D. we have

\[
g = p_1 p_2 \ldots p_r
\]

where \( p_i \)'s are prime elements of \( D \).

If now \( a_0(x) \) is reducible, we have

\[
a_0(x) = a_{01}(x) a_{02}(x)
\]

where \( a_{01}(x) \) and \( a_{02}(x) \) are both primitive of positive degree.

Proceeding in this manner, we shall after a finite number of steps, arrive at a relation of the form

\[
a(x) = p_1 p_2 \ldots p_r \ a_1(x) \ldots \ a_s(x)
\]

where each factor on the right is irreducible.

This shows that \( D[x] \) is a f.d.

To show uniqueness, let us suppose that

\[
a(x) = p_1 p_2 \ldots p_r \ a_1(x) \ldots \ a_s(x) = p_1' p_2' \ldots p_r' a_1'(x) a_2'(x) \ldots a_m'(x)
\]
where each of the factors is irreducible and degree of each of $a_i(x)$ and $a_i'(x)$ is positive. By Lemma 1, $a_1(x) a_2(x) \ldots \ a_s(x)$ and $a_1'(x) a_2'(x)$ are primitive. The constant of R.H.S. is $p_1' \ p_2' \ldots \ p_s'$ and that of L.H.S. is $p_1 p_2 \ldots p_t$. Therefore

$$p_1 \ p_2 \ldots \ p_t = p_1' \ p_2' \ldots \ p_s'$$

and hence

$$a_1(x) a_2(x) \ldots \ a_s(x) = a_1'(x) a_2'(x) \ldots \ a_m'(x)$$

Since each of $a_1(x) a_2(x) \ldots \ a_s(x)$ and $a_1' \ a_2' \ldots \ a_m'(x)$ are irreducible in $D[x]$, by Lemma 4 there are irreducible in $K[x]$. Now $K[x]$ being a unique f.d. we see that two sets of polynomials.

$$a_1(x), \ldots, a_s(x) \text{ and } a_1'(x), \ldots, a_m'(x)$$

and the same except for order and the difference in associateness. Thus by a possible change of notation we have

$$a_1(x) \sim a_1'(x), \quad a_2(x) \sim a_2'(x) \ldots \text{ in } K[x].$$

By Lemma II this relation of associateness also hold good in $D[x]$.

Thus the two factorisations of $a(x)$ in $D[x]$ are the same except for the difference in order and associateness. Hence $D[x]$ is a u.f.d.

**Theorem.** If the primitive polynomial $f(x)$ can be factored as the product of two polynomials having rational coefficients it can be factored as the product of two polynomials having integer coefficients.

**Proof.** Suppose that

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

where $g(x)$ and $h(x)$ have rational coefficients. By clearing of denominators and taking out common factors we can write

$$f(x) = \left[ \frac{a}{b} \right] \lambda(x) \ \mu(x)$$

where $a$ and $b$ are integers and where both $\lambda(x)$ and $\mu(x)$ have integer coefficients and are primitive. Thus

$$bf(x) = a \ \lambda(x) \ \mu(x)$$

The content of the left hand side is $b$, since $f(x)$ is primitive. Since both $\lambda(x)$ and $\mu(x)$ are primitive, therefore, $\lambda(x) \ \mu(x)$ is also primitive so that the content of the right hand side is $a$. Therefore $a = b$ and

$$f(x) = \lambda(x) \ \mu(x)$$

where $\lambda(x)$ and $\mu(x)$ have integer coefficients. This is the assertion of the theorem.

**Definition.** A polynomial is said to be integer monic if all its coefficients are integer and the coefficient of its highest power is 1.

**Eienstein Criterion of Irreducibility**

**Statement.** Let $a(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$ be a polynomial belonging to $D[x]$ and $p$ is a prime element of $D$ such that

$$p \mid a_0, \ p \mid a_1, \ldots, \ p \mid a_{n-1}$$

whereas $p$ is a not a divisor of $a_n$ and $p^2$ is not a divisor of $a_0$. Then $a(x)$ is irreducible in $D[x]$ and hence also in $K[x]$. 
**Proof.** Let, if possible,
\[ a_0 + a_1 x + \ldots + a_n x^n = (b_0 + b_1 x + \ldots + b_l x^l) (c_0 + c_1 x + \ldots + c_m x^m) \]
where \( l > 0, \ m > 0 \).
We have
\[ a_0 = b_0 c_0 \]
Therefore \( p | a_0 \Rightarrow p | b_0 \) or \( p | c_0 \)
Now, since \( p^2 \) is not a divisor of \( a_0 \), therefore, \( p \) cannot be a divisor of both \( b_0 \) as well as \( c_0 \).
Suppose that \( p | c_0 \).
Also, we have
\[ a_n = b_l c_m \]
implying that \( p \) is not a divisor of \( c_m \).
Let \( r \leq m \) be the smallest index such that each of
\[ c_0, c_1, \ldots, c_{r-1} \]
is divisible by \( p \).
Also
\[ a_r = b_0 c_r + b_1 c_{r-1} + \ldots + b_r c_0 \]
Since neither \( b_0 \) nor \( c_r \) is divisible by \( p \), and each of
\[ c_0, c_1, \ldots, c_{r-1} \]
is divisible by \( p \), we deduce that \( a_r \) is not divisible by \( p \). This shows, that \( r = n \) so that the degree of the second of the two factors is \( n \) and accordingly the polynomial is actually irreducible.

**Theorem.** If \( a, b \) are arbitrary elements of a unique factorisation domain \( D \) and \( p \) is a prime element of \( D \), then
\[ p \mid ab \Rightarrow p \mid a \text{ or } p \mid b. \]

**Proof.** Let
\[ a = p_1 p_2 \ldots p_r \]
\[ b = p'_1 p'_2 \ldots p'_s \]
where each of \( p_1, p_2, \ldots, p_r, p'_1, p'_2, \ldots, p'_s \) is a prime element of \( D \). Then we have
\[ ab = p_1 p_2 \ldots p_r p'_1 p'_2 \ldots p'_s \]
(i)
By virtue of the fact that expression as product of primes occur as a factor on the right side of (i) so that we have

either \( p | a \) or \( p | b \).

* Examples of rings which are not U.F.D.

We know that if \( a, b \) are two arbitrary element of a unique factorisation domain, then \( p | ab \Rightarrow \) either \( p | a \) or \( p | b \).

The ring \( \mathbb{Z}[\sqrt{-5}] \) of numbers \( a+b \sqrt{-5} \) where \( a \) and \( b \) are any integers is not a u.f.d. For,
\[ 9 = (2 + \sqrt{-5}) (2 - \sqrt{-5}) = 3 \cdot 3 \]
The prime 3 is a divisor of the product \( (2 + \sqrt{-5}) (2 - \sqrt{-5}) \) without being a divisor of either \( (2+\sqrt{-5}) \) or of \( (2-\sqrt{-5}) \).
Similarly \( \mathbb{Z}[\sqrt{-3}] \) is not a u.f.d. For,
The prime 3 divides the product but does not divides the individual elements.

**Theorem.** The domain of Gaussian integers is an Euclidean domain.

**Proof.** The set of numbers $a+ib$ where $a$, $b$ are integers and $i = \sqrt{-1}$ is an integral domain relatively to usual addition and multiplication of numbers as the two rings compositions. This domain is called domain of Gaussian integers.

We shall show that the mapping $\phi$ of the set of non-zero Gaussian integers into the set of positive integers satisfies the two conditions of the Euclidean domain.

We write

$$\phi(a+ib) = a^2 + b^2$$

Then

$$\phi((a+ib)(c+id)) = (a^2 + b^2)(c^2 + d^2)$$

$$= [\phi(a+ib)][\phi(c+id)]$$

so that condition (i) is satisfied.

We now write $\alpha = a+ib$, $\beta = c+id$. Then

$$\frac{\alpha}{\beta} = \lambda = p+iq, \text{ say}$$

where $p$ and $q$ are rational numbers.

There exist integers $p'$, $q'$ such that

$$|p' - p| \leq \frac{1}{2}, \ |q' - q| \leq \frac{1}{2}$$

We write

$$\lambda' = p' + iq'$$

so that $\lambda'$ is a Gaussian integer. We have

$$\alpha - \lambda'\beta = (\alpha - \lambda\beta) + (\lambda - \lambda')\beta$$

$$= 0 + (\lambda - \lambda')\beta$$

$$= (\lambda - \lambda')\beta$$

$$\therefore \quad \alpha = \lambda'\beta + (\lambda - \lambda')\beta$$

Now $\alpha$, $\beta$, $\lambda'$ being Gaussian integers it follows that $(\lambda - \lambda')\beta$ is also Gaussian integer.

Here

$$\phi((\lambda - \lambda')\beta) = \{(p' - p)^2 + (q' - q)^2\} \phi(\beta)$$

$$\leq \left( \frac{1}{4} + \frac{1}{4} \right) \phi(\beta) < \phi(\beta)$$

Thus for every pair of Gaussian integers $\alpha$, $\beta$ there exist Gaussian integers $\lambda'$ and $(\lambda - \lambda')\beta$ such that

$$\alpha = \beta\lambda' + (\lambda - \lambda')\beta$$

where

$$\phi((\lambda - \lambda')\beta) < \phi(\beta).$$

Hence the domain of Gaussian integers is Euclidean.
Unit-II

Composition Series

**Definition:**
A series of subgroups $G = G_0 \triangleleft G_1 \triangleleft G_2 \triangleleft \cdots \triangleleft G_r = (1)$ of a group $G$ is called a **Composition series** of $G$ if 

1. $G_{i+1} \triangleleft G_i$ for every $i$

and

2. if each successive quotient $G_i / G_{i+1}$ is simple

The above composition series is said to have length $r$. The successive quotients of a composition series are called the **Composition factors** of the series.

**Examples:**

1. Consider the symmetric group $S_5$. It has a normal subgroup $A_5$ which is simple from unit I. Since $S_5 / A_5 \cong \mathbb{Z}_2$ is also simple, we see that $A_5 \triangleleft S_5 \triangleleft S_5 = (1)$ is a composition series of $S_5$. This is the only composition series of $S_5$, because only non-trivial proper normal subgroup of $S_5$ is $A_5$.

2. Consider $S_4$, From unit I we have $S_4 \triangleleft A_4 \triangleleft V_4 \triangleleft E_4 \triangleleft (1)$, the composition series of $S_4$.

Recall $V_4 = \{(1), (12)(34), (13)(24), (14)(23)\}$ is Klein’s four group and $E_4 = \{(1), (12)(34)\}$, Further

$$\frac{S_4}{A_4} = 2, \frac{A_4}{V_4} = 3, \frac{V_4}{E_4} = 2, \frac{E_4}{(1)} = 2$$ tells

each successive quotients $\frac{S_4}{A_4}, \frac{A_4}{V_4}, \frac{V_4}{E_4}$ and $\frac{E_4}{(1)}$ is of prime order, hence are simple.

**Theorem 1:**
Every finite group has a composition series.

**Proof:**
Let $G$ be a finite group. Use induction on $|G|$. If $G$ is a simple then $G \triangleleft (I)$ is a composition series of $G$. So let $G$ be not simple, Hence $G$ has some maximal normal subgroup $H$, which has a composition series

by induction. Since $G/H_1$ is simple, so

$G = G_0 \triangleleft H_1 \triangleleft H_2 \triangleleft \cdots \triangleleft H_r = (1)$ is a composition series of $G$.

Note that infinite groups need not have composition series. We can consider infinite cyclic group $\mathbb{Z}$.

As every non-trivial subgroup of infinite cyclic group $\mathbb{Z}$ is isomorphic to $\mathbb{Z}$; as $\mathbb{Z}$ is not simple, we see that $\mathbb{Z}$ has no simple subgroups. So we can not construct composition series of $\mathbb{Z}$.
We can not end to $Z = (1)$.

**Definition:**

Let $G = G_0 \triangleleft G_1 \triangleleft G_2 \triangleleft \cdots \triangleleft G_r = (1)$ be a composition series and suppose that $G = H_0 \triangleleft H_1 \triangleleft H_2 \triangleleft \cdots \triangleleft H_r = (1)$ is another composition series of the same length $r$. We say that these series are **equivalent** if there is some $s \in S$ such that

$$G_{i-1}/G_i \cong H_{\sigma(i)-1}/H_{\sigma(i)} \quad \forall i.$$  

**Example 3.**

Let $G = \langle x \rangle$, $0 (G) = 6$

(from unit I).

Let $G_I = \langle x^2 \rangle$, and $H_I = \langle x^3 \rangle$.

We have two composition series:

$G \triangleleft G_I \triangleleft H_I \triangleleft (I)$ and $G \triangleleft H_I \triangleleft H_2 \triangleleft (I)$

These two series are **equivalent**, as

$$G/G_{I} \cong H_{I}/(I) \cong Z_2$$ and

$$G_{I}/(I) \cong G/H_{I} \cong Z_3.$$  

and take $\sigma = (12) \in S_2$

**Theorem 2:**

**Jorden-Holder Theorem:**

This theorem asserts that, upto equivalence, a group has at most one composition series.

**Statement:**

Suppose that $G$ is a group that has a composition series. Then any two composition series of $G$ have the same length and are equivalent.

**Proof:**

Let $G = G_0 > G_1 > \cdots > G_r = (I)$

and $G = H_0 > H_1 > \cdots > H_s = (I)$

be two composition series of $G$. We use induction on $r$, the length of one of the composition series.
If $r = 1$, then $G$ is simple and so is the only composition series of $G$. So let $r > 1$ and assume by induction that the result holds for any group having some composition series of length less than $r$.

If $G_1 = H_1$, then $G_1$ has two composition series of respective length $r - 1$ and $s - 1$. Therefore by induction we see that $r = s$ and two composition series of $G_1$ and equivalent. Hence $G$ has two composition series which are equivalent.

Therefore, we suppose $G_1 \neq H_1$.

But $G_1$ is simple, so $G_1 \not\leq H_1$, hence

and so because $G/H_1$ is simple.

Let $K = G_1 \cap H_1 \triangleq G$. Now

$$\frac{G}{G_1} = \frac{G_1 H_1}{G_1} \cong \frac{H_1}{G_1 \cap H_1} = \frac{H_1}{K} \text{ and}$$

$$\frac{G}{H_1} = \frac{G_1 H_1}{H_1} \cong \frac{G_1}{G_1 \cap H_1} = \frac{G_1}{K}$$

Then $K \triangleleft G$ and $G$ has a composition series,

$K$ has a composition series, say $K = K_1 \supseteq K_2 \supseteq \ldots \supseteq K_m = \{1\}$

$G_1$ now have two composition series

$G_1 \triangle G_2 \triangle G_3 \triangle \ldots \triangle G_r = (I)$ and

$G_1 \triangle K \triangle K_1 \triangle K_2 \triangle \ldots \triangle K_r = (I)$.

These are of lengths $r - 1$ and $t + 1$, respectively. By induction, we get $t = r - 2$ and that the series are equivalent. Similarly, $H_1$ has two composition series:

$H_1 \triangle H_2 \triangle \ldots \triangle H_s = (I)$ and

$H_1 \triangle K \triangle K_1 \triangle K_2 \triangle \ldots \triangle K_{r-2} = (I)$ \hspace{1cm} (I) \hspace{1cm} ($\Theta t = r - 2$)

These have respective length $s - 1$ and $r - 1$, so by induction we see $r = s$ and the series are equivalent.

We now conclude that the composition series

and $G = H_0 \triangle H_1 \triangle K \triangle K_1 \triangle \ldots \triangle K_{s-2} = (I)$

are equivalent, because we have proved above

$$\frac{G}{G_1} \cong \frac{H_1}{K} \text{ and}$$
Hence we finally conclude that our two initial composition series of $B$ are equivalent.

**Definition:**
A series of sub groups

$$G = G_0 \triangleleft G_1 \triangleleft G_2 \triangleleft \cdots \triangleleft G_n = (I)$$

of group $G$ is called a **subnormal** series of $G$ if $G_{i+1} \triangleleft G_i$ for each $i$.

A subnormal series is called a **normal series** of $G$ if

**Solvable groups:**

First we define **Commutators** in a group $G$. Let $a, b \in G$. The element

$$[a, b] = a^{-1} b^{-1} a b$$

is called a **Commutator** and is denoted by $[a, b]$. The Commutator $[a, b] = 1$, only when $ab = ba$.

$[a, b]^{-1} = [b, a]$, i.e., the element, inverse to the Commutator is itself a Commutator. But a product of Commutators need not be a Commutator. Thus, in general, the set of Commutators of a group is not a sub group. The smallest sub group $G_1$ of the group $G$ containing all Commutators is called its **Commutator sub group**. Note that the commutator sub group $G_i$ is the set of all possible products of the form $[a_1, b_1] \cdots [a_r, b_r]$, where $a_i, b_i \in G$, and $r$ is a natural number. From which, as a consequence, implies that $G^i \triangleleft G$.

**Remarks:**

1. The commutator sub group $G'$ of an abelian group is trivial.
2. The Commutator sub group of $S_n$ is $A_n$, $n \geq 1$.
3. The Commutator sub group of $GL(n, F)$ is $SL(n, F)$, $F$ is a field.
4. The Commutator sub group $A_n$ of $A_n$ is $A_n$, is $A_n = A_n$, because the non-commutative group $A_n$, has no non-trivial proper normal subgroups.

**Theorem 4:**

The Commutator sub group $G'$ of a group $G$ is the smallest among the normal sub group $H$ of the group $G$ for which is an abelian group.

**Proof:**

The Commutator $[xH, yH] = [x, y]H$

is trivial is abelian

From $[a, b]^2 = [a^x, b^y], a, b, g \in G$, we get the second Commutator sub group $G''$, i.e. the Commutator sub
group of the Commutator sub group of the group G, is a normal sub group in G. The same result holds for the
k-th Commutator sub group G^{(k)}, i.e. the Commutator subgroup of the (k–1)-th Commutator subgroup
G^{(k–1)}, k ≥ 2. Thus, any group G has a sequence of Commutator sub groups

\[ G^{(0)} = G, \quad G^{(1)} = G', \quad G^{(2)} = G'', \ldots \]

**Definition:**
If for some k, we have G^{(k)} = (1), then G is called **solvable** (Also soluble). Note that in the case of = Aₙ, n ≥ 5, all members of above sequence coincide. i.e. Aₙ, n ≥ 5 not soluable.

From unit I, we see that S₄, S₃ are solvable. An abelian group is solvable, and non-abelian simple group is not solvable.

or

A group is solvable if it has a subnormal series with each factor abelian.

**Theorem 5:**
1. A subgroup of a solvable group is solvable.
2. A homomorphic image of a solvable group is solvable.
3. If N \unlhd G and \unlhd H are solvable groups.
4. A group of pⁿ, where p is a prime number, is solvable.
5. If G and H are solvable, then G\times H is solvable.

**Proof:**
1. for all k, and G^{(k)} = (1) for some k, as G is solvable, \therefore H is solvable.
2. Let \( \phi: G \to H \) be a homomorphism. Then \( \phi(G) = \text{Im} \) is solvable because

3. To show N and \( G/N \) are solvable:
It is trivial from above 1 and 2).

Now N and \( G/N \) are solvable, so we get subnormal series

\[ G/N = G_0/N \triangleleft G_1/N \triangleleft \ldots \triangleleft G_i/N = (I) \] such that \( G_j/N \triangleleft G_{i+1}/N \) for all i. Now get

\[ G = G_0 \triangleleft G_1 \triangleleft \ldots \triangleleft G_2 = N = N_0 \triangleleft N_1 \triangleleft \ldots \triangleleft N_2 = (I) \]

is a subnormal series of G having abelian successive quotients. Hence G is solvable.

or

We can use
4. The centre $Z(G)$ and the quotient group $G/Z(G)$ are finite $p$-groups of strictly smaller order. So by induction and using above parts of this theorem, we get $G$ is solvable.

5. $1 \times H \cong H$ is a solvable normal subgroup of $G \times H$, and is also solvable. Hence from part (3) $G$ is solvable.

Nilpotent Groups

Definition:

Central Series of a group $G$:

A normal series $G = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_r = \{1\}$ of a group $G$ is called a central series of $G$ if, for each $i$, $G_i/G_{i+1}$ is contained in the center of $G_i$, i.e.

$$\frac{G_i}{G_{i+1}} \leq Z\left(\frac{G_i}{G_{i+1}}\right), \forall i.$$

A group $G$ is said to be nilpotent if it has a central series.

Examples: 1.

1. An abelian group $G$ has the central series $G > \{1\}$, and abelian groups are nilpotent.

2. $S_4$, $S_3$, the symmetric groups of degree 4 and 3 are solvable groups but they are not nilpotent.

Recall are subnormal series in which each factor is abelian and hence $S_4$ and $S_3$ are solvable.

But center of $S_i$, $i = 3, 4$, i.e. $Z(S_i) = \{1\}$.

$$\therefore \frac{G_i}{G_{i+1}} \subseteq Z\left(\frac{G_i}{G_{i+1}}\right), \text{ does not hold } \forall i,$$

where $G = S_4$ or $S_3$.

Remarks:

1. The least number of factors in a central series in $G$ is called nilpotency class (or just the class) of $G$.

2. The condition $\frac{G_i}{G_{i+1}} \subseteq Z\left(\frac{G_i}{G_{i+1}}\right)$ is equivalent to the Commutator condition that

$$[G_{i+1}, G_i] = G_{i+1}, \forall x \in G_i \text{ and } \forall g \in G.$$

For any $x \in G_i$, $\frac{G_i}{G_{i+1}} \subseteq Z\left(\frac{G_i}{G_{i+1}}\right)$.
\[ d_{i+1}x \cdot id_{i+1}i = d_{i+1}i \cdot d_{i+1}x \quad \forall \ g \in G \]

\[ [G_{i+1}x, G_{i+1}g] = G_{i+1}, \quad \forall \ x \in G_i, \quad \forall \ x \in G. \]

However,

\[ G_{i+1}x G_{i+1}g^{-1} G_{i+1}g = G_{i+1} [x, g] \]

So the condition can be restated as

\[ [x, g] \in G_{i+1} \quad \forall \ i, \quad \forall \ x \in G_i \quad \text{and} \quad \forall \ g \in G. \]

Hence in words, whenever we take a commutator of an element of \( G_i \) with an arbitrary element of the group, we end up in \( G_{i+1} \).

**Remarks**

1. The trivial group has nilpotency class 0.
2. Non-trivial abelian groups have nilpotency class 1.

**Theorem 6:** Nilpotent group are solvable.

**Proof:** Let \( G \) be a nilpotent group. So it has a central series, which is a normal series with abelian successive quotients and hence \( G \) is solvable.

Converse is not true. There are solvable groups that are not nilpotent. For example \( S_3 \) can not have a central series, as the last but one term of a such a series must have to be a non-trivial subgroup of \( Z(S_3) = (1) \), which is not possible.

**Theorem 7:** Finite p-group are nilpotent

**Proof:** Let \( P \) be a finite p-group, we prove it by induction on \( |P| \) if \( |P|=p \), then \( P \) is abelian and hence nilpotent. Let \( Z=Z(P) \). Since \( Z \neq (1) \) (because finite p-group has non-trival center), by \( P/Z \) has a central series.

We get easily that the series

\[ P = P_0 \Delta P_1 \Delta P_2 \Delta \ldots \Delta P_r = Z \Delta \Delta \Delta \]

a central series of \( P \).

**Theorem 8:** Let \( G \) be a nilpotent group and suppose that \( H<G \) is a proper subgroup of \( G \). Then the normalizer of \( H \) in \( G \) is strictly larger than \( H \) i.e.

A nilpotent group has no proper self-normalizing subgroups.

**Proof:** Let

be a Central Series of the nilpotent group \( G \). Let \( \Delta \) and let \( k \) be such that \( G_{k+1} \) and \( h \) such a \( k \) exists since \( G_i = (1) \) Now
Let \( x \in G_k \) and \( g \in G \)

Since \( G_k / G_{k+1} \leq Z / G_{k+1} \rangle \), we get

Hence \( [G_k, G] \leq G_{k+1} \), and so \( [G_k, H] \leq H \)

We now get that \( G_k \leq N_G (g) \), but \( G_k \triangle H \)

Hence we must have \( H \leq N_G (g) \).

**Corollary:** Every maximal subgroup of a nilpotent \( G \) is normal in \( G \).

**Proof:** Let \( H \) be a maximal subgroup of \( G \). Since \( \triangle \), by hypothesis we must have \( G \) and hence \( H \triangle G \)

**Theorem 9:** If any finite group \( G \) is direct product of its Sylow subgroups, then \( G \) is nilpotent.

**Proof:** From above theorem 7, it suffices to show that the direct product of two nilpotent groups is nilpotent. It can be verified easily.

**Example 1:**
Normal series of \( \mathbb{Z} \) under addition:

1. \( \mathbb{Z} \triangle 8\mathbb{Z} \triangle 4\mathbb{Z} \triangle \mathbb{Z} \)
2. \( \mathbb{Z} \triangle 9\mathbb{Z} \triangle \mathbb{Z} \)

**Examples 2:**

\( \mathbb{Z} \triangle 72\mathbb{Z} \triangle 8\mathbb{Z} \triangle \mathbb{Z} \)

can be refined to a series

\( \mathbb{Z} \triangle 72 \triangle 24\mathbb{Z} \triangle 8\mathbb{Z} \triangle 4\mathbb{Z} \triangle \mathbb{Z} \)

Note that two new terms, \( 24\mathbb{Z} \) and \( 4\mathbb{Z} \) have been inserted.

**Example 3:**
We consider two series of \( \mathbb{Z}_{15} \):

\( \mathbb{Z} \triangle 5 \mathbb{Z}_{15} \triangle \) and \( \mathbb{Z} \triangle 3 \mathbb{Z}_{15} \triangle \)

These series are isomorphic

We see that \( \mathbb{Z}_{15} / \langle 5 \rangle \equiv \mathbb{Z}_5 \equiv \langle 3 \rangle / \mathbb{Z} \) and \( \mathbb{Z}_{15} / \langle 3 \rangle \equiv \mathbb{Z}_3 \equiv \langle 5 \rangle / \mathbb{Z} \)

**Example 4:**
We now find isomorphic refinements of the series given in Example 1

i.e.

(1) \( \mathbb{Z} \triangle 9\mathbb{Z} \triangle \mathbb{Z} \)

(2)
we write the refinement
\[ l \mathfrak{a} 72Z \Delta 8Z \Delta 4Z \Delta Z \] (3)
of (1) and the refinement
\[ l \mathfrak{a} 72Z \Delta 18Z \Delta 9Z \Delta Z \] (4)
of (2)
Both refinements have four factor groups:

3. has \( \frac{Z}{4Z} \equiv Z_4, \frac{4Z}{8Z} \equiv Z_2, \frac{8Z}{72Z} \equiv Z_9 \)
\[ l \mathfrak{a} 72Z \equiv 72Z \text{ or } Z \]

4. has \( \frac{Z}{9Z} \equiv Z_9, \frac{9Z}{18Z} \equiv Z_2, \frac{18Z}{72Z} \equiv Z_4 \),
\[ l \mathfrak{a} 72Z \equiv 72Z \text{ or } Z \]

Hence (3) and (4) have four factor groups isomorphic to \( Z_4, Z_2, Z_9 \) and \( 72Z \text{ or } Z \).

Note carefully the order in which the factor groups occur in (3) and (4) is different.

Example 5:
Consider \( G = V_4 = Z_2 \times Z_2 \)
We write a normal series for \( G = V_4 \):
\[ G = Z_2 \times Z_2 \Delta Z_2 \times \mathfrak{m} \Delta \mathfrak{m} \times \mathfrak{m} \]
This is a composition series, because

But \( Z_2 \) is a simple group. Therefore, above normal series is a composition series. The composition factors for \( G = V_4 = Z_2 \times Z_2 \) are \( Z_2 \) and \( Z_2 \).

Example 6:
Let \( G = S_3 \), a normal series for \( G \) is given by
\[ G = S_3 \Delta A_3 \Delta 1 \mathfrak{a} \]
\[ S_3 / A_3 \equiv Z_2, A_3 / 1 \mathfrak{a} \equiv Z_3 \]
Both \( Z_2 \) and \( Z_3 \) are simple groups. Therefore, normal series for \( S_3 \) is a composition series. The composition factors for \( S_3 \) are \( Z_2 \) and \( Z_3 \).
Example 7:

For $n \geq 5$, the composition factors of the normal series

$$S_n \triangleleft A_n \triangleleft C$$

are

But $A_n$ is simple. Hence above is a composition series for $S_n$. However, for $A_n$ is not abelian. Hence $S_n$ is not solvable.

Example 8:

Let $G_1$ and $G_2$ be two groups and $N_1 \triangleleft G_1, N_2 \triangleleft G_2$ are normal subgroups. Then the product $N_1 \times N_2 \triangleleft G_1 \times G_2$ and

Solution

Let $p_i : G \rightarrow N_i$ be the projection. Then defined by

is an epimorphism.

The Ker $G \rightarrow N_1 \times N_2$ Hence

$$G \rightarrow G_1 \times G_2 \rightarrow N_1 \times N_2 \equiv G_1 / N_1 \times G_2 / N_2$$

Illustration:

$$G \times R \rightarrow Z \rightarrow N \rightarrow Z / N$$

Example 9:

Consider the product $G \times G$. Then by above and $G \times G \rightarrow G \rightarrow N \rightarrow N / G$.

Now subnormal series

give two subnormal series of $G \times G'$:

If factors are suitably permuted, they are isomorphic in these series.

Example 10:

Let $C$ be a cyclic group generated by $a$ and $O(c) \equiv p^e$. We write the composition series of length $e$:
of length \( e \) in which each \( C_i \) is the cyclic subgroup generated by \( a \) this can be easily verified that above is the only composition series for \( C \).

**Example 11:**

Let \( G \) be a cyclic group of order 30 units generator \( a \).

\[ G = \langle a \rangle = \{ a, a^2, a^3, \ldots, a^{28}, a^{29} \} \]

The only subgroups of \( G \) other than \( G \) itself are:

\[ G_5 : n \cdot a^6, a^{12}, a^{18}, a^{24} \]
\[ G_6 : n \cdot a^5, a^{10}, a^{15}, a^{20}, a^{25} \]
\[ G_{10} : n \cdot a^3, a^6, \ldots, a^{24}, a^{27} \]
\[ G_{15} : n \cdot a^2, a^4, \ldots, a^{26}, a^{28} \]

Note that the subscript \( i \) on \( G' \) indicates the order of the group. (e.g., \( o(G_{10}) = 10 \)). Since \( G \) is cyclic, all the subgroups are normal. Now we construct their composition series:

\[ G \triangleleft G_{15} \triangleleft G_5 \triangleleft G_1 = \{ e \} \quad (1) \]

\[ G \triangleleft G_{10} \triangleleft G_5 \triangleleft G_1 \]
\[ G \triangleleft G_6 \triangleleft G_2 \triangleleft G_1 \]
\[ G \triangleleft G_3 \triangleleft G_1 \]
\[ \equiv G_5 \triangleleft G_1 \]

The factor groups of (1) are

\[ G/G_{15} : G_{15}, aG_{15} \]
\[ G_{15}/G_5 : G_5, a^2G_5, a^3G_5 \]
\[ G_5/G_1 : G_1, a^6G_1, a^{12}G_1, a^{18}G_1, a^{24}G_1 \]

The factor groups of (2) are

\[ G/G_6 \equiv G_6/G_5 \]

We are clearly, \( G/G_{15} \equiv G_6/G_5 \) under the mapping.
\( G_{15}/G_1 \cong G_5/G_1 \) under the mapping

\[
G_5 \leftrightarrow G_1 \\
a^2G_5 \leftrightarrow a^{10}G_1 \\
a^4G_5 \leftrightarrow a^{20}G_1
\]

\( G_5/G_1 \cong G_3/G_6 \) under the mapping

\[
G_1 \leftrightarrow G_6 \\
a^6G_1 \leftrightarrow aG_6 \\
a^{12}G_1 \leftrightarrow a^2G_6 \\
a^{18}G_1 \leftrightarrow a^3G_6 \\
a^{24}G_1 \leftrightarrow a^4G_6
\]

Multiplication table for factor groups for \( G_{15}/G_5 \)

\[
\begin{array}{c|ccc}
    & G_5 & a^2G_5 & a^4G_5 \\
\hline
G_5 & G_5 & a^2G_5 & a^4G_5 \\
a^2G_5 & a^2G_5 & a^4G_5 & G_5 \\
a^4G_5 & a^4G_5 & G_5 & a^2G_5
\end{array}
\]

The multiplication table for \( G_3/G_1 \)

\[
\begin{array}{c|ccc}
    & G_1 & a^{10}G_1 & a^{20}G_1 \\
\hline
G_1 & G_1 & a^{10}G_1 & a^{20}G_1 \\
a^{10}G_1 & a^{10}G_1 & a^{20}G_1 & G_1 \\
a^{20}G_1 & a^{20}G_1 & G_1 & a^{10}G_1
\end{array}
\]

The isomorphism of \( G_{15}/G_5 \) and \( G_3/G_1 \) can be easily seen from above tables.

**Remark**: Above is very good example of the **Jordan-Holder Theorem**.

**Example 12**: Any nilpotent group is solvable.

**Solution**: By the definition of the \( k \)-th center, each \( Z_k(G) \) is abelian, so any commutator of two elements of \( Z_k(G) \) must lie in \( Z_{k+1}(G) \) (see (iv) of example 12 of section I). Hence, if \( G \) is nilpotent of class \( c \), (A finite group \( G \) is defined to be nilpotent when there is some index \( c \) with \( Z_c(G)=G \), the first such index \( c \) is called the class \( c \)-th center)
of nilpotency of $G$), so $Z_c(G) = G$. Now $G'$.

Hence $G$ is solvable.

Note that the converse is not true i.e. a solvable group need not be nilpotent. For example:

$G_3 \Delta \Lambda _2 \Delta \lambda$

$S_3$ is solvable but is not nilpotent because center of $S_3$ is (1). (Every nilpotent group has a non-trivial center)

**Example 13:**

Consider $Z_2 \times S_3$. Now $Z_2 \times S_3 \triangleleft Z_2 \times S_3$ and every $Z_2 \times S_3 \triangleleft Z_2 \times S_3$. Therefore, ascending central series (or upper central series) never reach $G$. Hence $Z_2 \times S_3$ is not nilpotent.
Unit-III

Definition
Let \( R \) be a commutative ring with identity \( 1 \). \((M, +, \cdot_R)\) is called an \( R \)-module \( M \) if \((M, +)\) is an abelian group, together with a scalar multiplication \( \cdot \) such that:

1. \( r \cdot (m_1 + m_2) = r \cdot m_1 + r \cdot m_2 \)
2. \( (r_1 \cdot r_2) \cdot m = r_1 \cdot (r_2 \cdot m) \)
3. \( 1 \cdot m = m \)

for all \( r, s \in R \) and \( m \in M \).

Remarks
Above are precisely the axioms for a vector space. In \( F \)-module is just an \( F \)-vector space, where \( F \) is a field. Hence modules are the natural generalizations of vector spaces to rings. But modules are more complicated as elements of rings need not be invertible.

Submodule
A submodule of an \( R \)-module \( M \) is a non-empty subset such that:

1. \( x + y \in M \) for all \( x, y \in M \)
2. \( \alpha x \in M \) for all \( x \in M \) and \( \alpha \in R \)

Cyclic Modules
An \( R \)-module \( M \) is cyclic if in \( M \) there is a generating element \( x_\circ \), such that:

\[ M = R x_\circ = \{r x_\circ \mid r \in R \} \]

Remark
Any ring \( R \) is both a left and a right \( R \)-module over itself and also a \((R, R)\)-module. These modules are denoted by \( _R R, R_R, _R R \).

The submodules of the module \( _R R \) are the left ideals, etc.

Simple (or irreducible) module: The \( R \)-module, \( M \) is called simple if it does not contain proper non-trivial submodules.

Examples
1. When \( R \equiv \mathbb{Z} \), the ring of integers :- Any abelian group \( V \), with law of composition addition, is a module over the ring \( \mathbb{Z} \), if
\[ n \cdot v = \]

i.e. abelian group \( \equiv \mathbb{Z} \)-module

2. A vector space \( V \) over a field \( F \) is an \( F \)-module

3. A linear Vector space \( V \) is an \( M_n(F) \)-module if \( A \cdot V \) is usual product, where

\[
A = (a_{ij})_{n \times n} \in M_n(F), \quad v = \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix}, \text{ the column vector } v \text{ of length } n \text{ from } F^n.
\]

4. Let \( V \) be a vector space over the field \( F \). \( T : V \to V \) is a linear operator. \( V \) can be made a \( F[x] \)-module by defining

\[
f(x) \cdot v = f(T)v,
\]

**Free modules**

Let \( M \) be a \( R \)-module over a ring \( R \), and \( S \) be a subset of \( M \). \( S \) is said to be a **basis** of \( M \) if

1. \( S \) generates \( M \)
2. and \( m \) is \( + \)ve integer
3. \( S \) is linearly independent.

If \( S \) is a basis of \( M \), then in particular, if and every element of \( M \) has a **unique** expression as a linear combination of elements of \( S \).

If \( R \) is a ring, then as a module over itself, \( R \) admits a basis, consisting of unit element 1.

**Free Module**

A module which admits a basis. We include in definition, the zero module also for free module

**Remarks**

1. An ordered set \( (m_1, m_2, \ldots, m_k) \) of element of a module \( M \) is said to **generate** (or **span**) if every \( m \in M \) is a linear combination:

\[
r_i \in R
\]

Here elements \( v_i \) are called **generators**. A module \( M \) is said to be **finitely generated** if there exists a finite set of generators.

A \( \mathbb{Z} \)-module \( M \) is finitely generated \( \iff \) it is finitely generated abelian group.

2. Consider,
(\(R^n + , R\)) is a module over \(R\), where +, are defined:

\[
\begin{align*}
  a_1 + b_1 + a_2 + b_2 + \ldots + a_n + b_n &\in M \\
  a_1 + b_1 + \ldots + a_n + b_n &\in M
\end{align*}
\]

3. A module isomorphic to any of the modules \(R^n\) is called a **free module**.

Thus a finitely generated module \(M\) is free if there is an isomorphism \(\phi : R^n \longrightarrow M\).

4. A set of elements \(\{m_1, m_2, \ldots, m_k\}\) of a module \(M\) independent if

\[
r_1m_1 + r_2m_2 + \ldots + r_km_k = 0, \quad r_i \in R, \text{ the ring, then } \forall U.
\]

5. Suppose a module \(M\) has a basis

\[
\{m_1, m_2, \ldots, m_k\}.
\]

Then \(R^k \cong M\)

Define \(R^k \longrightarrow M\)

\[
(r_1, r_2, \ldots, r_k) \longrightarrow r_1m_1 + \ldots + r_km_k, \quad \forall r_i \in R
\]

\(\phi\) is clearly module-homomorphism. \(\phi\) is surjective: Let \(m\) be any element of \(M\)

then \(m = a_1m_1 + a_2m_2 + \ldots + a_km_k, \ a_i \in \text{ the ring}\)

\[
\therefore \quad \text{such that}
\]

\[
\phi(a_1, a_2, \ldots, a_k) = m
\]

\(\phi\) is injective:

\[
\Rightarrow \quad (a_1 - b_1)m_1 + \ldots + (a_k - b_k)m_k = 0,
\]

\[
\Rightarrow \quad \text{(since \(\{m_1, \ldots, m_k\}\) is a basis for \(M\))}
\]

\[
\Rightarrow \quad a_i = b_i, \ \forall i
\]

\[
\therefore \quad \phi \text{ is a bijective} \iff M \text{ has a bases; in this case} \ M \text{ is a free module} \quad \text{. So a module} \ M \text{ has a basis} \iff \text{it is free.}
\]

The following result shows how homomorphisms are affected when there are no proper submodules.
Theorem 1
Let $M, N$ be $R$-modules and let $f : M \rightarrow N$ be a non-zero $R$-morphism. Then
1. If $M$ is simple, $f$ is a monomorphism.
2. If $N$ is simple, $f$ is an epimorphism.

Proof
1. Ker$f$ is a submodule of $M$, since $f$ is not the zero morphism, we must have ker$f = (0)$, because $M$ is simple, so only submodules of $M$ are $(0)$ and $M$ itself (if Ker$f = M$, then $f(M) = (0) \Rightarrow f = 0$, but ).

Hence Ker is a monomorphism.

2. $\text{Im} f$ is a submodule of $N$, But $N$ is simple, so $\text{Im} f$ or . If then but . Therefore, Here $f$ is an epimorphism.

Corollary: (Shur's Lemma) If $M$ is a simple $R$-module, then the ring $\text{End } R M$ of $R$-morphisms.

Proof
From (1) and (2) above, every non-zero $f \in \text{End } M$ is an isomorphism and so is an invertible element in the ring. Hence $\text{End } R M$ is a division ring.

Fundamental structure theorem for finitely generated modules over a principal ideal domain:
Before proving this we have to build some tools needed to prove above theorem:
Suppose we have a sequence of modules with a homomorphism from each module to the next:

\[
\ldots \rightarrow M_0 \xrightarrow{f_0} M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} \ldots
\]

This sequence is said to exact at $M_i$ if

$\text{Im } f_1 = \text{Ker } f_2$

The sequence is exact if it is exact at every module
An exact sequence of the form

\[
(0) \xrightarrow{\alpha} M_1 \xrightarrow{\alpha} M \xrightarrow{\beta} M_2 \xrightarrow{\beta} (0)
\]

is called a short exact sequence.
Recall that every module over a general ring $R$ is a homomorphic image of a free module. Every $R$-module $M$ forms part of a short exact sequence.

\[
(0) \rightarrow G \rightarrow F \rightarrow M \rightarrow (0)
\]

where $F$ is free, this is called a presentation of $M$; If $M$ is finitely generated, $F$ can be taken to be of finite rank.
We shall use the result (without proving it)
"If $R$ is a principal ideal domain, then for any integer $n$, any submodule of is free of rank at most $n$.”
Using this, we assume that above $G$ is free, at least when $M$ is finitely generated. More precisely, when $M$ is generated by $n$ elements, then it has a presentation
(0) \rightarrow R^m \rightarrow R^n \rightarrow M \rightarrow (0)

where \( m \leq n \).

**Fundamental Structure Theorem for finitely generated modules over a principal ideal domain:**

**Theorem 2**

Let \( R \) be a Principal Ideal Domain and \( M \) a finitely generated \( R \)-module. Then \( M \) is direct sum of cyclic modules:

\[
M \cong R^{d_1} \oplus R^{d_2} \oplus \cdots \oplus R^{d_r},
\]

where \( d_i/d_{i+1} = 1, \ldots, m - 1 \).

(Recall that a module \( M \) over a using \( R \) is **cyclic** if \( M \) has an element \( x \) for which \( M = Rx \). Thus a cyclic group is the same as a cyclic module over \( Z \), the ring of integers. Every cyclic module is representable in the form of a quotient module of the free cyclic module, i.e., in the case of a ring of Principal ideals it has the form \( \mathbb{Z} / \langle d \rangle \).)

**Proof**

Suppose \( M \) is generated by \( n \) elements, then \( M \) has a presentation

\[
(0) \rightarrow R^m \xrightarrow{\phi} R^n \rightarrow M \rightarrow (0).
\]

Where \( m \leq n \), where \( M = \text{CoKernel} \) if a homomorphism \( \phi : R^m \rightarrow R^n \), which is given by \( m \times n \) matrix \( A \).

Now we Claim:

invertible matrices \( P \) and \( Q \) of orders \( m, n \) respectively over \( R \) such that

\[
PAQ = \text{diag}(d_1, d_2, \ldots, d_r).
\]

Where \( d_i/d_{i+1} \) for \( i = 1, \ldots, r - 1 \); more precisely \( PAQ = \text{diag} \).

Two vector \( u, v \) are called **right associated** if \( \exists S \in GL_2(R) \) such that \( u = vS \).

We show here that any vector \( (a, b) \) is right associated to \( (h, o) \), where \( h \) is an HCF of \( a \) and \( b \). Since \( R \) is a PID, \( a \) and \( b \) have an HCF \( h \); \( a = h; a', b = hb' \). Since \( h \) generates the ideal generated by \( a \) and \( b \), we have \( h = ha'd' - hb'c' \), cancelling \( h \) we get or \( h = ha'd' - hb'c' \), Cancelling \( h \) we get \( 1 = a'd' - b'c' \), Hence

\[
(h, o) = (a, b) \mathbf{d}_{a'}^{-b'} \mathbf{i}
\]

Which shows \( (a, b) \) is right associated to \( (h, o) \).

Now we prove the general case, i.e. we find a matrix right associated to \( A \) which all entries of the 1st row
after the first one are zero. We continue in this way, we find a matrix right associated to A, such that $b_{ij} = o$ for $i < j$. We shall now have to operate with invertible matrices on the left. We say two matrices $A$ and $A'$ are associated if, for invertible matrices $S$ and $T$ of suitable size.

By multiplying $B$ on the left by an invertible matrix we can reduce the entries of the first column after the first one to zero. By doing this we may get more non-zero elements in the 1st row, if it so happens, it will reduce the length of the $(1, 1)$ - entry, which allows us to use induction on the length of $A$ and we find that $A$ is associated to

$$
\begin{bmatrix}
0 & \cdots & 0 \\
\end{bmatrix}
$$

where $A_1$ is an $(m-1) \times (n-1)$ matrix. Now by induction on $m+n$, $A_1$ is associated to a matrix in diagonal form, say $\text{diag} \ (a_2, a_3, \ldots, a_r, o, o, \ldots, o)$ . Now we combine this with previous statements we find that $A$ is associated to a diagonal matrix:

$$
SA = \text{diag} \ (a_2, a_3, \ldots, a_r, o, o, \ldots, o)
$$

If $a_i/a_{i+1}$ for $i = 1, 2, \ldots, r - 1$, we get the required form. So we assume $a_i \times a_2$ and consider the $2 \times 2$ matrix formed by first two rows and columns. We get an equation

If we reduce the matrix on the right to diagonal form as before we again reach the form $SA = \text{diag}$, but with $a_i$ if shorter length than before. After a finite number of steps we have $a_i/a_2$. By repeating this process we find that $a_i/a_i, i = 2, \ldots, r$. The same process can be used for $a_2, a_3, \ldots, a_{n-1}$ and so we get the required form. Hence our claim is proved i.e.

$\exists$ invertible matrix $P$ and $Q$ such that $PAQ = \text{diag}$, where $d_i/d_{i+1}$ for $i = 1, 2, \ldots, r - 1$ and $r = m$, because $\phi$ is 1-1. Here $P$ and $Q$ correspond to changes if bases in $R^m$ and $R^n$ respectively; but these changes do not affect the Cokernel, so if $v_1, \ldots, v_n$ is the new basis in $R^m$, then the submodule $R^n$ has the basis $d_1, v_1, \ldots, d_m v_m$ and Cokernel takes the form

$$
\frac{R}{Rd_i} \oplus \cdots \oplus \frac{R}{Rd_m} \oplus R^{n-m}, \frac{d_i}{d_{i+1}}, i = 1, \ldots, m - 1.
$$

Where Cokernel $\phi = M$, and

$$(o) \rightarrow R^m \phi \rightarrow R^n \rightarrow M \rightarrow (o) \cdot \frac{R^n}{\phi(R^n)} = \frac{R^n}{\phi(R^n)}$$
Corollary (application to finitely generated abelian groups)

Since every abelian group is $\mathbb{Z}$-module, so every f.g. abelian group $G$ by above theorem, can be written as direct sum of finitely many cyclic groups of infinite, or prime-power orders.

Primary Decomposition

Theorem 3

Let $R$ be a PID and $M$ a f.g. torsion module over $R$. Then $M$ can be written as a direct sum of sub modules $M_p$, where $p$ are different primes in $R$ and $M_p$ consists of elements that are annihilated by a power of $p$.

(A module of the form $M_p$ is called $p$-primary)

Proof

Let $x \in M$, suppose that $xa = o, a \in R$. Let $a = q_1 q_2 \ldots q_r$ be the factorization of $a$ into powers of different primes, say $q_i = \alpha$ power of $p_i$. Put $s_i = \frac{a}{q_i}$. Now the $s_i, 1 \leq i \leq r$ have no common factor, so $s_1c_1 + s_2c_2 + \ldots + s_rc_r = 1, c_i \in R$

Hence $x = xs_1c_1 + xs_2c_2 + \ldots + xs_rc_r$ and $xs_iq_i = xac_i = 0$. Therefore, $xs_i c_i \in M_p$.

\therefore

It is easy to prove that above sum is direct

$$M = \bigoplus_{i=1}^{r} M_{p_i}$$

Rational Canonical form

See, 'Topics in Algebra' Herstein, Pages 305-308. Nicely given there.

Canonical forms

We can get linear transformation in each similarity class whose matrix, in some basis, is of a particular nice form. These matrices will be called the canonical forms.

Definition

The sub space $W$ of $V$ is invariant under a linear transformation $T$ on $V$ if $T(W) \subseteq W$ i.e.

Reduction to triangular form

Theorem 5

If a linear transformation $T$ on a vector $V$ over a field $F$, has all its eigenvalues in $F$, has all its then there exists a basis of $V$ in which the matrix of $T$ is triangular.

Proof

We shall prove it by induction on the dimension of $V$ over $F$.

If $\dim V = 1$, then every linear transformation is scalar, have proved.

Let $\dim V = n > 1$. Suppose that the theorem is true for all vector spaces over $F$ of dimension $n-1$.

By hypothesis, $T$ has all its eigenvalues in $F$. So let $T$ have eigen value in $F, \exists$ a corresponding eigen vector such that Let $= \{\alpha_i \nu_i : \alpha_i \in F\}$ be a one-dimensional
Vector space over $F$. Let $x \in W, x = \alpha_j v_j, \alpha_j \in F$ and $T(x) = \alpha_j T(v_j) = \alpha_j \lambda_j v_j \in W$. Hence $W$ is $T$-invariant.

Let $V = V/W = \dim, \dim (V) = \dim \mathcal{E}_{W} = \dim V - \dim W = n - 1$.

$T$ induces a linear transformation on $W$ defined by

$$T(v) = \alpha_{ij} v_j$$

Also minimal polynomial over $F$ of $T$, divides the minimal polynomial of $T$ over $F$. Hence all the roots of the minimal polynomial of $T$ are roots of minimal polynomial of $T$. Therefore all eigen values, of $T$ lie in $F$. Now satisfies the hypothesis of the theorem. Since $\dim V = n$ so by induction hypothesis, $\exists$ a basis of $V$ such that $T$ is triangular.

$$T(v_j) = \alpha_{32} v_2 + \alpha_{33} v_3$$

$$T(v_n) = \alpha_{n_2} v_2 + \alpha_{n_3} v_3 + \ldots + \alpha_{n_n} v_n$$

Let $v_2, v_3, \ldots, v_n$ be elements of $V$ mapping to $v_2, v_3, \ldots, v_n$ respectively, then it is easy to prove that $v_1, v_2, \ldots, v_n$ form a basis of $V$. Now $T(v_2)[- \alpha_{22} = 0 = W i.e.,$

$T(v_2) = \alpha_{21} v_1 + \alpha_{22} v_2$

Similarly, $T(v_1) = \lambda_j v_j = \alpha_{11} v_1$ (Taking).

Hence a basis of $V$ over $F$, such that $T(v_i) = \lambda_i v_i$ and its predecessors in the basis. Therefore, matrix of $T$ in this basis:

$$\begin{pmatrix}
\alpha_{22} & \alpha_{32} & \alpha_{33} & 0 \\
\alpha_{42} & \alpha_{43} & \alpha_{44} & 0 \\
\alpha_{n2} & \alpha_{n3} & \ldots & \alpha_{nn}
\end{pmatrix}$$

is triangular.
**Jordan Forms**

*Theorem 4*

If a square matrix $A$ of order $n$ has $s$ linearly independent eigen vectors, then it is similar to a matrix $J$ of the following form, called the **Jordan Canonical form**,

$$J = Q^{-1}AQ = \begin{pmatrix} J_1 & & \\ & \ddots & \\ & & J_s \end{pmatrix}$$

in which each $J_i$ called a **Jordan block**, is a triangular matrix of the form

$$J_i = \begin{pmatrix} \lambda_i & 1 & & \\ & \lambda_i & \ddots & \\ & & \ddots & 1 \\ & & & \lambda_i \end{pmatrix}$$

where $\lambda_i$ is a single eigen value of $A$ and $s$ is the number of linearly independent eigen vectors of $A$.

**Remarks**

1. If $A$ has more than one linearly independent eigen vector, then same eigen value $\lambda_i$ may appear in several blocks.
2. If $A$ has a full set of $n$ linearly independent eigen vectors, then there have to be $n$ Jordan blocks so that each Jordan block is just $1 \times 1$ matrix, and the corresponding Jordan canonical form is just the diagonal matrix with eigen values on the diagonal. Hence, a diagonal matrix is a particular case of the Jordan canonical form.

The Jordan canonical form of a matrix can be completely determined by the multiplicites of the eigen values and the number of linearly independent eigen vectors in each of the eigen spaces.

**Definition**

Let $V$ be an $n$-dimensional vector space over a field $F$. Two linear transformations $S, T$ on $V$ is said to be **similar** if $\exists$ an **invertible** linear transformation $C$ and $V$ such that

In terms of matrix form :

Two $n \times n$ matrices $A$ and $B$ over $F$ is said to be **similar** if $\exists$ an **invertible** $n \times n$ matrix $C$ over $F$ such that

Proof of Theorem 4 is not important but its application is very important. (Interested readers may see proof in Herstein P. 301-303)

**Example 1**

Let $A$ be a $5 \times 5$ matrix with eigen value $\lambda$ of multiplicity 5. Write all possible Jordan Canonical forms:

We can get 7 Jordan canonical forms:
1. Only one linearly independent eigen vector belonging to \( \lambda \) gives the Jordan canonical form:

\[
J = \begin{pmatrix}
2 & 1 & 0 & 0 \\
\lambda & 1 & 0 & 0 \\
0 & \lambda & 1 & 0 \\
0 & 0 & \lambda & 1 \\
0 & 0 & 0 & \lambda
\end{pmatrix}
\]

This Jordan canonical form consists of only one Jordan block with eigen value \( \lambda \) on the diagonal.

2. Two linearly independent eigen vectors belonging to \( \lambda \) gives the Jordan canonical form:

\[
J = \begin{pmatrix}
\lambda & 1 & 0 & 0 \\
0 & \lambda & 1 & 0 \\
0 & 0 & \lambda & 1 \\
0 & 0 & 0 & \lambda
\end{pmatrix}, \text{ or } \begin{pmatrix}
\lambda & 1 & 0 \\
0 & \lambda & 1 \\
0 & 0 & \lambda
\end{pmatrix}
\]

Each of which consists of two Jordan blocks with eigen value \( \lambda \) on the diagonal.

3. Three linearly independent eigen vectors belonging to \( \lambda \) gives the Jordan canonical form:

\[
J = \begin{pmatrix}
\lambda & 1 & 0 \\
0 & \lambda & 1 \\
0 & 0 & \lambda
\end{pmatrix}, \text{ or } \begin{pmatrix}
\lambda & 1 & 0 \\
0 & \lambda & 0 \\
0 & 0 & \lambda
\end{pmatrix}
\]

Each of which consists of three Jordan blocks with eigen value \( \lambda \) on the diagonal.

4. Four linearly independent eigen vectors belonging to \( \lambda \) gives the Jordan canonical form:

\[
J = \begin{pmatrix}
\lambda & 1 \\
0 & \lambda
\end{pmatrix}, \text{ or } \begin{pmatrix}
\lambda & 1 & 0 \\
0 & \lambda & 0 \\
0 & 0 & \lambda
\end{pmatrix}
\]

This consists of four Jordan blocks with eigen value \( \lambda \) on the diagonal.

5. Five linearly independent eigen vectors belonging to \( \lambda \) gives the Jordan canonical form:

Then the Jordan canonical form of \( A \) is of the form.
This is just the diagonal matrix.

**Remark**

We see from (5) that the Jordan form of the matrix $A$ consists entirely of $1 	imes 1$ blocks $\leftrightarrow$ the algebraic and geometric multiplicities coincide for each eigen value of $A$. This is of course precisely the criterion for diagonalizability. (The **algebraic multiplicity** of the eigen value $\lambda$ of the $n \times n$ matrix $A$ is its multiplicity as a root of the characteristic polynomial of $A$).

(The **geometric multiplicity** of the eigen value $\lambda$ of the $n \times n$ matrix $A$ is the dimension of the eigen space corresponding $\lambda$, i.e. maximum number of linearly independent eigen vectors corresponding to eigen value $\lambda$).

**Useful Information to determine $J$:**

1. The sum of the sizes of the blocks involving a particular eigen value of $A = \text{algebraic multiplicity of that eigen value}$.
2. The number of blocks involving a particular eigen value of $A = \text{geometric multiplicity of the eigen value}$.
3. The largest block involving a particular eigen value of $A = \text{multiplicity of the eigen value as a root of the minimal polynomial of } A$.

(The **minimal polynomial** of the $n \times n$ matrix $A$ is the monic polynomial of least degree such that $m_A(\lambda) = 0$. The minimal polynomial of $A$ always divides characteristic polynomial of $A$).

**Example 2**

1. $A$ has only the eigen value $\lambda$ which has algebraic multiplicity 3 and geometric multiplicity 1. $E(\lambda)$:

   Eigen space for $\lambda = 0 =$

2. $A = \begin{bmatrix} -1 & -3 \\ 3 & 3 \\ 1 & -1 \end{bmatrix}$

   Characteristic polynomial of $A = (2 - \lambda)^2 (\lambda - 2) \lambda = 2$ occurs with geometric multiplicity
3. Let $A$ be a $7 \times 7$ matrix whose characteristic polynomial is $(2 - \lambda)^4(3 - \lambda)^3$ and whose minimal polynomial is $(2 - \lambda)^2(3 - \lambda)^2$.

Corresponding to $\lambda = 3$ there must be one $2 \times 2$ Jordan block and $1 \times 1$ Jordan block.

Corresponding to $\lambda = 2$ there must be at least one $2 \times 2$ Jordan block. Hence there must be either two or three Jordan blocks for $\lambda = 2$, according as to whether the geometric multiplicity of $\lambda = 2$ is two or three.

Two possibilities for the Jordan form of $A$ depending on the geometric multiplicity of the eigen value $\lambda = 2$:

\[
J = \begin{pmatrix}
2 & 1 & 0 & 0 & 0 \\
0 & 2 & 0 & 0 & 0 \\
0 & 0 & 2 & 0 & 0 \\
0 & 0 & 0 & 3 & 1 \\
0 & 0 & 0 & 0 & 3
\end{pmatrix}
\]

or

\[
J = \begin{pmatrix}
2 & 1 & 0 & 0 & 0 \\
0 & 2 & 0 & 0 & 0 \\
0 & 0 & 2 & 0 & 0 \\
0 & 0 & 0 & 3 & 1 \\
0 & 0 & 0 & 0 & 3
\end{pmatrix}
\]

Example 1

An irreducible right $R$-module is cyclic.

(Let $R$ be a ring and $M$ be a nontrivial right $R$-module $M$, $M$ is called an irreducible right $R$-module if its only submodules are $(0)$ and $M$. Since $MR \neq (0)$ and $MR$ is a submodule of $M$, $MR = M$ and so an irreducible module is unital. A right $R$-module $M$ is called trivial if $MR = (0)$, i.e.

A right $R$-module $M$ is called cyclic if $\exists o \neq M$ such that $mR = M$. Thus a cyclic module is unital).

Proof

Let $M$ be an irreducible right $R$-module. Let $N = \{x \in M / xR = 0\}$. $N$ is a submodule of $M$ and hence $N = (0)$, i.e. lims $P - 103$ Therefore, any non zero element of $M$ generates $M$. For if and , then $yR$ is a non zero submodule of $M$ and, therefore, $yR = M$. 

\[
J = \begin{pmatrix}
4 & 0 & 0 \\
2 & 1 & 0 \\
0 & 2 & 0
\end{pmatrix}
\]
Example 2

Any homomorphic image of a module $M$ is isomorphic to a quotient module of $M$.

Proof

Let $M \longrightarrow M_1$ be a module epimorphism and let $\ker \psi = N$. Now we define a mapping $f : M \longrightarrow M_1$ defined by $f(x + N) = \psi(x). \forall x + N \in M/N$

From above $f$ is a module homomorphism. Further $f$ is injective since $\ker \psi = 0$, the zero element of $M/N$ is.

Hence $\text{Im } f = M_1 = \psi(M)$ i.e. $\frac{M}{N} \cong \psi(M)$

Q. 1. Let $I$ be an ideal in a commutative ring $R$ with 1. If $M$ is an $R$-module, show that the set $S = \{xm \mid x \in I, m \in M\}$ is not in general an $R$-module. When is $S$ an $R$-module?

Q. 2. If $M$ is an $R$-module and if $r \in R$, prove that the set $rM = \{rm \mid m \in M\}$ is an $R$-module.

Q. 3. Let $M$ be a right $R$-module. Show that the annihilator of $M$ is an ideal of $R$. It is called the annihilator of $M$.

Example 3

If $M$ is a finitely generated $R$-module, it does not follow that each submodule of $N \& M$ is also finitely generated.

Let $M$ be a cyclic right $R$-module, i.e. $M = mR$ for some element of $M$. The right $R$-submodules of $M$ is if the form $mS$, where $S$ is a right ideal in the ring $R$. Suppose $S$ is a finitely generated right ideal, say $mR = \langle ma_1, ma_2, \ldots , ma_k \rangle$. Now the submodule $mS$ is generated by the elements $ma_1, ma_2, \ldots , ma_k$, i.e. $ms = \langle ma_1, ma_2, \ldots , ma_k \rangle$ and so is a finitely generated $R$-module. Actually, $ms$ is a cyclic $S$-module.

If $R$ is a Noetherian ring (i.e. $R$ has the ascending chain condition on right ideals, $I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots$), then every ideal is finitely generated. But if $R$ is not a Noetherian ring, then the ideal $S$ need not be finitely generated and hence the submodule $ms$ of $M$ would not be a finitely generated $R$-module. (See : $F[x_1, x_2, \ldots , x_n]$ is not Noetherian, $F$ is a field).

Example 4

A finitely generated module is not in general a free module, for its generators are not necessarily linearly independent. Consider a cyclic $R$-module $M$ is generated by a single element $m \in M$, i.e. $M = mR$. But is not a free module unless
Example 5
The direct sum of free modules over $R$ is a force module over $R$, its basis being the union of the bases of the direct summands.

Example 6
A submodule of a free module over a ring $R$, is not necessarily a free module. However, every submodule of a free module over a principal ideal domain (P.I.D.) is free.

We mention the following results without proof (can be seen in a standard book of algebra):

Results
1. Let $M$ be a free module over a P.I.D. with a finite basis $x_1, x_2, \ldots, x_n$. Then every submodule $N$ of $M$ is free and has a basis of $\leq n$ elements.
2. From (1) we can deduce that a submodule $N$ of a finitely generated module $M$ over a P.I.D. is finitely generated.

Recall that for each finite abelian group $G \neq \{0\}$ there is exactly one list of integers $m_1 > 1$, each a multiple of the next, for which there is an isomorphism.

$$G \cong \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_k}$$

the first integer $m_1$ is the least positive integer $m = m_1$ with $mG = \{0\}$ and the product

Example 7
The possible abelian group of order 36 are

$$\mathbb{Z}_{36}, \mathbb{Z}_{18}, \mathbb{Z}_{12}, \mathbb{Z}_{6}, \mathbb{Z}_3 \oplus \mathbb{Z}_6$$

No two of these group are isomorphic.
Definition: Ring

Let \( R \) be a non empty set with two binary operations, called addition and multiplication, denoted by + and \( . \), \((R, +, .)\) is called a ring if

1. Closure: \( a+b \in R, a.b \in R \) \( \forall a, b \in R \).
2. Commutative law with respect to +: \( a+b=b+a \) \( \forall a, b \in R \).
3. Associative laws:
   \[
   a+(b+c) = (a+b)+c \\
   a.(b.c) = (a.b).c
   \]
   \( \forall a, b, c \in R \).
4. Distributive Laws:
   \[
   a. (b+c) = a.b+a.c \\
   (b+c).a = b.a+c.a
   \]
   \( \forall a, b, c \in R \).
5. Additive identity: \( R \) contains an additive identity element, denoted by 0, such that \( a+0=a \) and \( 0+a=a \) \( \forall a \in R \).
6. Additive inverses: \( \forall a \in R, \exists x \in R \) such that \( a+x=0 \) and \( x+a=0 \)
   \( x \) is called additive inverse of \( a \), and is denoted by \( -a \).

Remarks: \((R, +, .)\) is abelian additive group and \((R, .)\) is a semigroup, closure and associative law with respect to \( . \), so \((R, +, .)\) is a ring.

7. A ring \((R, +, .)\) is called a commutative ring if \( a.b = b.a \) \( \forall a, b \in R \)
8. A ring \((R, +, .)\) is called a ring with identity if \( a \cdot 1 = a \) and \( 1 \cdot a = a \)
   In this case 1 is called a multiplicative identity element or simply an identity element.

Examples
1. \((\mathbb{Z}, +, \cdot)\) is commutative ring with identity 1 (Ring of integers under ordinary addition and multiplication.
2. \( E \): set of even integers. \((E, +, \cdot)\) is a commutative ring without identity element.

3. \( M_2(\mathbb{R}), +, \cdot \) is a non-commutative ring with identity \( I = \begin{bmatrix} 1 & 0 \cr 0 & 1 \end{bmatrix} \oplus I \in R \)
   whose \( +, \cdot \) are defined as addition of matrices and multiplication of matrices.

\[
A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}, B = \begin{bmatrix} e & f \\ g & h \end{bmatrix} \in M_2(\mathbb{R}) \text{ and}
\]

A. B ≠ B.A.
If IR, the set of real numbers is replaced by E, the set of even integers, then
(M₂ (E), + :) is a non-commutative ring without identity, as


is a commutative ring with identity 1, where +, ; are defined shown in following tables:

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>3</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

Important Remark:
As we saw in a group that Cancellation law holds but in a ring the cancellation law may fail for multiplication:

In Z₄, +, · the 3 = 0 = 4 but 2 ≠ 4.

Definition Subring:
Let (R, +, ·) is a ring and S a non-empty subset of R. Then (S, +, ·) with same binary operations is called a subring if

1. Closure

2. ∀ a ∈ R, −a ∈ R.

Examples:
(1) Z₄, +, · is a commutative ring with identity. (S, +, ·) is a subring with identity (multiplicative) since Note that parent ring Z₄, +, · has identity 4. This shows that a subring may have a different identity from that of a given ring.

Definitions: Units in a ring
Let R be a commutative ring with identity 1. An element a ∈ R is said to be invertible if such that a.b = 1. The element a ∈ R is called a Unit of R.

Divisors of Zero
If and ab = 0 for some non zero . Then ‘a’ cannot be unit in R, since multiplying ab = 0, by the universe of a (if it exists)
An element $a$ such that $ab = 0$ for some $b \neq 0$ in $R$, is called a **divisor of zero**.

In $\mathbb{Z}_4$, $2$ and $3$ are divisors of zero.

2. Let $IR$ be the set of real numbers, and

$$I \times IR$$

is a commutative ring with identity. $+$ defined by

(Addition and multiplication are defined pointwise).

$I \log | \forall x \in IR, I$ is identity of the ring $R$.

Note that $(R, +, \cdot)$ is a commutative ring with identity and also with divisors of zero.

If $f \log $, $x < 0$

and $g \log $, $x \geq 0$

then $f \log $, $x \geq 0$, $\forall x \in IR$. In above example, $(f \log) (x)$

$= f \log$ $\forall x \in IR$

$= f \log$ $\forall x \in IR$

$= f \log$ $\forall x \in IR$

If $f \log$, $f \log = 1$, $f \log = 1$ $\forall x \in IR$

and $f \log \neq 0$, $g \log \neq 0$ $\forall x \in IR$, then $f$ has a multiplicative inverse $\iff$

Hence for example

$f \log = 2 + \sin x$ has a multiplicative inverse, but $g \log \sin x$ does not.

**Definition: Integral Domain:**

If $R$, $+, \cdot$ is a commutative ring with identity such that for all

**Examples:**

1. $\mathbb{Z}_6$, $+, \cdot$ is not an integral domain.

2. $\mathbb{R}$, $+, \cdot$ is not an integral domain.

**Definition:**

A non-commutative ring with identity is a skew field (or Division ring) if every non-zero element has its inverse in it.
Example:

\[(D, +, \cdot)\] is a division ring, where \(+, \cdot\) are defined as

\[
\begin{align*}
D: \quad & a + ij + \alpha j + \alpha j + \beta j + \beta j + \beta j + \delta j = (R, +, \cdot) \\
& a + ij + \alpha j + \alpha j + \beta j + \beta j + \beta j + \delta j = (R, +, \cdot) \\
& a + ij + \alpha j + \alpha j + \beta j + \beta j + \beta j + \delta j = (R, +, \cdot)
\end{align*}
\]

where \(i^2 = j^2 = k^2 = ij = -ji = k,\)

\[
D: a + \alpha j + \alpha j + \alpha j + \beta j + \beta j + \beta j + \delta j = (R, +, \cdot) \\
\Rightarrow a + \alpha j + \alpha j + \alpha j + \beta j + \beta j + \beta j + \delta j = (R, +, \cdot) \\
\Rightarrow a + \alpha j + \alpha j + \alpha j + \beta j + \beta j + \beta j + \delta j = (R, +, \cdot)
\]

\[
\begin{align*}
& a + ij + \alpha j + \alpha j + \beta j + \beta j + \beta j + \delta j = (R, +, \cdot) \\
& a + ij + \alpha j + \alpha j + \beta j + \beta j + \beta j + \delta j = (R, +, \cdot) \\
& a + ij + \alpha j + \alpha j + \beta j + \beta j + \beta j + \delta j = (R, +, \cdot)
\end{align*}
\]

Definition:

A commutative ring with identity is a field if its every non-zero element has inverse in it.

Example:

The ring of real numbers \([\mathbb{R}, +, \cdot]\) is a field.

Theorem. Every field is without zero divisor.

Proof. Let \(F\) be a field and \(x, y \in F, x \neq 0\). Then

\[
xy = x^{-1} (xy) = x^{-1} = 0
\]

\[
\Rightarrow (x^{-1} x)y = 0
\]

\[
\Rightarrow y = 0
\]

Similarly, if \(y \neq 0\), then
\[ xy = 0 \implies xyy^{-1} = 0 \cdot y^{-1} \]
\[ \implies x \cdot e = 0 \]
\[ \implies x = 0 \]

Hence \( xy = 0 \implies x = 0 \) or \( y = 0 \) and so \( F \) is without zero divisor.

**Remark.** It follows from this theorem that **every field is an integral domain.** But the converse is not true. For example, ring of integers is an integral domain but it is not a field.

**Theorem:**

Any finite integral domain is a field.

**Proof:**

Let \( D \) be a finite integral domain

let \( D^* = D - \{0\} \).

Since cancellation law holds in integral domain \( D \). Since \( D \) is finite set, so one-to-one function from finite set to itself must be onto, so \( f \) is onto. Hence

\[ \exists a \in D^* \text{ such that } f(a) = 1. \]
\[ i.e. \ da = 1, \ a \in D^*CD \]

and so \( d \) is invertible. Hence every non-zero element in \( D \) is invertible, i.e. \( D \) is a field.

**Remark:**

Does there exist an integral domain of 6 elements? No, we shall explain in Unit V that every finite integral domain must be \( p^n \), for some prime \( p \), every + ve integer \( n \).

**Ring homomorphism:**

Let \( R \) and \( S \) be rings. A function

\[ \psi: R \rightarrow S \]

is called **ring homomorphism** if

\[ \psi(a + b) = \psi(a) + \psi(b) \]

for all

\[ a, b \in R. \]

**Kernel of ring homomorphism:**

is called the zero elements of \( S \).

\[ \text{, the kernel of } \psi, \text{ denoted by } \ker \psi \]
Examples

1. The polynomial \( f(x) = x^p - 1 \) is irreducible over \( \mathbb{Q} \), where \( p \) is a prime.

Proof

\((x - 1)f(x) = x^p - 1 \). Put \( x = y + 1 \), then

\[
= y^p + \sum_{i=0}^{p-1} y^i + \frac{y^p}{y-1}
\]

(1)

Where \( \sum_{i=0}^{p-1} y^i = 1, \ i < p \)

Note that \( p \) and \( p^i \) divides the product \( y^p \) and \( y-1 \). Hence \( p \) divides

Dividing (1) by \( y \), we see that

satisfies the hypothesis of Eisentein criterion and so it is irreducible over \( \mathbb{Q} \). Hence \( f(x) \) is irreducible.

2. \( f(x) = x^4 + x^3 + x^2 + x + 1 \) is irreducible over \( \mathbb{Q} \), since \( p = 5 \), \( 5 \) divide, \( 10 \) divide, \( 10 \) divide, \( 5 \) divide.

3. \( f(x) = x^n + 1 \) is irreducible over \( \mathbb{Q} \), \( p \) is a prime number.

4. \( f(x) = x^4 + x^3 + x^2 + x + 1 \) is irreducible over \( \mathbb{Q} \). Put \( x = (y + 1) \)

\[
= y^4 + 5y^3 + 10y^2 + 10y + 5
\]

Take \( p = 5 \), so \( y \) is irreducible over \( \mathbb{Q} \), hence \( y^4 \) is irreducible over \( \mathbb{Q} \).

Field Extensions

Definition

Let \( k \) be a field. A field \( K \) is called an extension of \( k \) if \( k \) is subfield of \( K \).

Let \( S \) be a subset of \( K \). \( k(S) \) is defined by smallest subfield of \( k \), which contains both \( k \) and \( S \). \( k(S) \) is an extension of \( k \). We say \( k(S) \) is obtained by adjoining \( S \) to \( k \). If \( S \) is a finite set, then

\[
k(S) := k(a_1, a_2, \ldots, a_n)
\]

If \( K \) is an extension of \( k \), then \( K \) is a vector space over \( k \), so \( K \) has a dimension over \( k \), it may be infinite. The dimension of \( K \), as a vector space over \( k \) is called degree of \( K \) over \( k \). Denote it by

\[
\dim K = \text{degree of } K \text{ over } k = [K : k]
\]
Unit-V

Normal Extension:
An extension K of k is said to be a normal extension of k if
1. K is an algebraic extension of k and
2. every irreducible polynomial \( f(x) \) which has one root in K splits in K[x] (i.e. has all its roots in K).

Theorem 1.
If K is a splitting field over k of some polynomial \( f(x) \), then K is a normal extension of k.

Proof:
Let \( a_1, a_2, \ldots, a_n \) be roots of \( f(x) \) in K. So \( K = k(a_1, a_2, \ldots, a_n) \). Let \( p \) be any irreducible polynomial in \( k[x] \) which has one root in K. Let L be a splitting field of \( p \) over K and let \( b_1 \) be any root of \( p \) in L. Now from unit IV, we get a k-isomorphism \( \sigma \) of \( k(b) \) onto \( k(b_1) \) such that \( \sigma(b) = b_1 \). Also \( \sigma(f(x)) = f(x) \), since \( f(x) \) and \( \sigma \) is k-isomorphism. Since K is a splitting field of \( f(x) \) over \( k(b) \), so \( \sigma(K) \) is a splitting field of \( f(x) \) over \( k(b_1) \). Hence from Unit IV, there exists an isomorphism \( \sigma \) of K onto \( K(b_1) \) such that for all \( a \in K \) and \( \sigma \) is k-isomorphism. Since K is a splitting field of \( f(x) \) over k, so \( \sigma(K) = K \), i.e. \( b_1 \in K \). As \( b_1 \) is arbitrary root of an irreducible polynomial \( P(x) \) in \( k[x] \) such that \( b_1 \in K, P(x) \) splits in \( K[x] \). Therefore K is normal extension of k.

A partial converse is also true.

Theorem 2.
If K is a finite normal extension of k, then K is the splitting field over k of some polynomial in \( k[x] \).

Proof:
Let \( K = k(a_1, a_2, \ldots, a_n) \) and let \( p \) be irreducible polynomial over k such that \( \forall i \).
Since K is a normal extension of k, each \( p \) splits in \( K[x] \). So \( p_1(x) \) \( \ldots \) \( p_n(x) = f(x) \) say, splits in \( K[x] \). K is got by adjoining roots of \( f(x) \) to k. Hence K is a splitting field of \( f(x) \) over k.

Perfect fields
Definition:
A field k is called perfect if k has characteristic 0 or if k has characteristic p, some prime p, and
(Characteristic of a ring with identity:– Let R be a ring with identity 1. If 1 has infinite order under addition, then the characteristic of R is 0. If 1 has order n under addition, then the characteristic of R is n). Note that the characteristic of a field is 0 or a prime.

**Theorem 3.**
Every finite field is perfect.

**Proof:**
Let k be a finite field of characteristic p. Define

\[ a \mapsto a^p \]

Then

\[ a^p + b^p = \psi(a + b) \]

\[ a^p = \psi(a) \]

\[ a^p \neq 0 \text{ when } a \neq 0 \text{ in } k, \text{ so } \ker \psi = \{0\} \]

Now \( \psi \) is one-to-one and since k is finite, so it is onto.

**Theorem 4.**
If \( p(x) \) is irreducible polynomial over a perfect field \( k \), then \( p(x) \) has no multiple roots.

**Proof:**

**Case I:** Characteristic \( k = 0 \) (i.e. \( \text{char } k = 0 \)). Let \( K \) be an algebraic extension of \( k \). Let \( a \in K \) and \( p(x) \) be an irreducible polynomial over \( k \) s.t \( p(a) = 0 \) (i.e. \( p(x) = \text{Irr}(k, a) \)). Then \( p'(a) \neq 0 \) and \( p'(x) \) is of smaller degree than \( p(x) \). Therefore \( a^k \) is separable over \( k \) and so \( p(x) \) has no multiple roots.

**Case II:** Let \( \text{char } k = p \).

Let \( p(x) \) have multiple roots

Since \( p'(a) = 0 \) and since \( \deg p'(x) < \deg p(x) \) so

where

\[ p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_k x^k + \cdots + a_1 x + a_0, \quad a_i \in k \quad \forall i. \]

\[ a_k = 0 \text{ when } p \times k. \text{ Hence only powers of } x \text{ that appear in} \]

are those of the form \( x^{pi} = \prod \). Hence \( p(x) = g(x)^p \) for some \( g(x) \in k[x] \) (for example: if \( p(x) = x^6 + 3x^4 + 5x^2 + x^p + 1 \), then \( g(x) = x^6 + 3x^4 + 5x^2 + x + 1 \).
Now $p(x) = g(x) + k[x]$ and $k^n = k$, so each coefficient $a_i$ of $g(x)$ in $k$ can be written as $b_i^p$ for some $b_i \in k$.

Therefore we get

$$p(x) = g(x) + k[x] = x^{p^n} + b_{n-j}^p x^{p(n-1)} + \cdots + b_j^p x^p + b_0^p$$

$$= d_i + b_{n-j} x^{p(n-1)} + \cdots + b_j x + b_0^p$$

( Char $k = p$ and so $p_i = 0 \forall i$)

But then $p(x)$ is not irreducible over $k$.

**Finite Fields:**

We know $\mathbb{Z}_p + \cdot \cdot \cdot$ is a finite field containing $p$ elements with addition and multiplication module a prime $p$.

**Theorem 5.**

Let $k$ be a finite field such that $\text{char} \ k = p$. Then $k$ has $p^n$ elements, for some positive integer $n$.

**Proof:**

Define

$$\psi: n \in \mathbb{Z}$$

Where

$m$ times

Clearly $\psi$ is a ring homomorphism.

$\ker \psi = p\mathbb{Z}$, $p = \text{char} \ k$

But $\frac{\mathbb{Z}}{p\mathbb{Z}} \cong \mathbb{Z}_p$, a field of $p$ elements, so $\text{Im} \ \psi$ is a subfield of $k$, isomorphic to $\mathbb{Z}_p$. Since $k$ is finite, so $k$ is vector space of finite dimension over a field which is isomorphic to $\mathbb{Z}_p$. Let $[k:F] = n$. Let $u_1, u_2, \cdots, u_n$ be a basis of $k$ over $F$. Now each element $x$ of $k$ can be written as:

$$x = \alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_n u_n, \ \alpha_i \in F \ \forall i.$$
As \(|F| = p^d F \cong \mathbb{Z}_p|\), each \(\alpha \in F\) can be chosen \(p\) ways. Hence that total number of ways in which an element in \(k\) can be defined in \(p^n\) ways. So

**Theorem 6.**

1. Let \(k\) be a finite field with \(p^n\) elements. Then \(k\) is the splitting of the polynomial \(x^{p^n} - x\) over the prime subfield of \(k\).
2. Two finite fields are isomorphic they have the same number of elements.
3. Let \(k\) be a finite field with \(p^n\) elements. Then each subfield of \(k\) has \(p^m\) elements for some divisor \(m\) of \(n\). Conversely, for each \(+ve\) divisor \(m\) of \(n\) a unique subfield of \(k\) with \(p^m\) elements.
4. \(\forall\) prime \(p\) and \(\forall\) positive integer \(n\), \(\exists\) a field with \(p^n\) elements.

**Proof:**

1. \(\Theta \) k has \(p^n\) elements, then \(k^*\), the multiplicative group of \(k\) has \(p^n - 1\) elements. Hence for any \(x \in k \subset k\), \(x^{p^n - 1} = 1\), so \(x^{p^n} = x\). The polynomial \(x^{p^n} - x\) has at most \(p^n\) roots and so its roots must be precisely the elements of \(k\). Hence \(k\) is the splitting field of \(f(x) = x^{p^n} - x\) over the prime subfield of \(k\).
2. Let \(k_1\) and \(k_2\) be two finite fields with \(p^n\) elements, containing prime subfields \(F_1\) and \(F_2\) respectively. But \(F_1 \cong \mathbb{Z}_p \cong F_2\). By (1), \(k_1\) and \(k_2\) are splitting fields \(x^{p^n} - x\) over isomorphic fields \(F_1\) and \(F_2\). Hence from unit (IV), \(k_1 \cong k_2\).
3. Let \(F_1\) be the prime subfield of \(k\). Let \(k_1\) be a subfield of \(k\). Then \(n = [k:F_1] = [k:k_1][k_1:F_1] \Rightarrow [k_1:F_1]/n\).

Let \([k_1:F_1] = m\), so any subfield \(k_1\) of \(k\) must have \(p^m\) elements such that \(m/n\).
Conversely, suppose for some positive integer \(m\). Then \(-1\) is a divisor of \(p^n - 1\) and so \(q(x) = x^{p^n - 1} - 1\) is a divisor of \(x^{p^n} - x\). As \(k\) is the splitting field of \(x^{p^n} - x = xf(x)\) over \(F_1\). We know that \(\{a \in k : a^p = a\}\) is a subfield of \(k\) and has distinct roots. So \(k\) must contain all \(p^m\) distinct roots of \(xg(x)\). Hence these roots form a subfield of \(k\). Moreover, any other subfield with \(p^m\) elements must be a splitting field of \(xg(x) = x^{p^n} - x\). Hence there exists unique subfield of \(k\) with \(p^m\) elements.
4. Let \(k\) be the splitting field of \(f(x) = x^{p^n} - x\) over its prime subfield isomorphic to \(\mathbb{Z}_p\). Now \(x^{p^n} - x = x \sum_{i=0}^{p^n-1} - 1\) and \(p \times \mathbb{Z}_p - 1\). So it is easy to see that \(f(x) = x^{p^n} - x\) has distinct roots. \(\{a \in k : a^{p^n} = a\}\) is a subfield of \(k\) and so set of all roots of \(f(x)\) is a subfield of \(k\). Hence \(k\) consists of
precisely the roots of $f(x)$, and it has exactly $p^n$ elements.

Now we prove the beautiful result given below:

**Theorem 7.**
The multiplicative group of non-zero elements of a finite field is cyclic.

**Proof:**

Let $k$ be a finite field of $p^n$ elements. $k^* = k - (0)$. So $|k^*| = p^n - 1 = m$ say. Let $a \in k^*$ be of maximal order, say $m_i$ i.e. $o(a) = m_i$. Now we use the following result: (Let $G$ be a finite abelian group. Let $a \in G$ be an element of maximal order. Then order of every element of $G$ is a divisor of this order of $a$).

By above result, each element of $k^*$ satisfies $f(x) = x^{m_i} - 1$. Since $k$ is a field, so there are at most $m_i$ roots of $f(x)$, hence $m \leq m_i$. But $m_i \leq m$, so $m = m_i$, and $<a> = m$. Therefore $k^* = <a>$ implies the result.

**Algebraically Closed field:**

A field $k$ is said to be algebraically closed, if every polynomial of +ve degree has a root in $K$.

**Example (Fundamental Theorem of Algebra):**

Every nonconstant polynomial with complex coefficients has a complex root i.e. splits into linear factors.

**Automorphism of extension:**

Let $K$ be an extension of the field $k$.

Define $\psi : K \to K$

such that

$$\psi \circ g \circ \psi \circ g \circ \psi$$

$\psi$ is 1–1 and onto

and $(C) = C \psi$

Then $\psi$ is $k$–automorphism of an extension field $K$.

The group of all $k$–automorphisms of $K$ is called the **Galois group** of the field extension $K$. This group is denoted by $G K k$.

**Galois extension:**

An extension $K$ of the field $k$ is called **Galois extension** if

1. $K$ is algebraic extension of $k$.

2. The fixed field of $K$ is $k$ i.e. $= k$
In this case is called the **Galois group** of

**Fundamental Theorem of Galois Theory:**

**Theorem 8.**

Let $K$ be a finite Galois extension of $k$. Then

1. There is a one-to-one order-reversing correspondence between the fields $L$ such that $k \subseteq L \subseteq K$ and the subgroups of $G_{K/k}$. This correspondence is given by

2. If $k \subseteq L \subseteq K$, then $L$ is Galois

In this case $G_{K/k} \equiv G_{E/L} \equiv G_{E/K}$

**Proof:**

1. Define $\Psi : L : k \subseteq L \subseteq K \rightarrow \{G_{E/L} : G_{E/L} \leq G_{E/K}\}$

i.e. $\Psi$ is a mapping from the set of all fields between $k$ and $K$ into the set of all subgroups of $G_{K/k}$ as follows:

Since $K/k$ is Galois, $K$ is separable. Let $M$ be another field such that $K/k$ is separable and $K/L$ is normal.

So we assume that $K/k$ is separable and $K/L$ is normal.

Such that $L$ is the fixed field of $G_{K/L}$.

This shows that $G_{E/L} \neq G_{E/M}$.

Now $\Psi(G_{E/L} \neq G_{E/M})$ and $L \neq M \Rightarrow G_{E/L} \neq G_{E/M}$

So $L \neq M \Rightarrow \Psi(G_{E/L} \neq G_{E/M})$. Hence there is a one-one mapping $L \rightarrow G_{E/L}$ from the set of all fields between $k$ and $K$ into the set of all subgroups of $G_{K/k}$.

To show $\Psi$ is onto:

Let $H$ be a subgroup of $G_{K/k}$ and let $L$ be the fixed field of $N$. Since $K/k$ is a finite Galois extension, so $L$ is normal and separable, $K/L$ is normal and separable. Hence $L$ is Galois and $L$ is the fixed field of $G_{K/L}$.

Each element of $H$ leaves each element of $L$ fixed and so $H \leq G_{E/L}$.

(Now we use the result: If $G$ be a finite group of automorphisms of a field of $K$ and $F$ be the fixed
field of $G$, then

Hence $[K:L]=O(H)$. Also $O(G(V/L))=[K:L]$, as $K/L$ is separate

Therefore and Hence $\varphi$ is onto.

If are subgroups of , then the subfield left fixed by $H_2$, will be left fixed by all elements of $H_1$, so this subfield is contained in the subfield left fixed by $H_1$. On the other hand if , then it is obvious that .

Consider the field $L$ such that . Suppose is normal and , .

Claim: $\nexists \psi$

Let $a \in L$, then each conjugate of $a$ is in $L$.

( Let $K$ be an extension of $k$, $a$, $b$ $K$ be algebraic over $k$, then $a$ and $b$ are said to be conjugate over $k$ if they are the roots of the same minimal polynomial over $k$.)

Since is a conjugate of $a$.

( minimal polynomial $p(x)$ over $k$ s.t $p(a) = 0$, , $a$ are roots of same minimal polynomial over $k$).

\[ \therefore \quad \sigma^{-1} \rho \sigma^{-1} \in \text{Galois} \Rightarrow a = \sigma^{-1} \rho \sigma^{-1} a \]

Now to show $\mathbb{F}_k / \mathbb{L}$ is Galois:

If suffices to show is normal, because we know that is separable. Let $p(x)$ be nonconstant irreducible polynomial in $k[x]$ which has one root, say $a$, in $L$. Since is normal, $p(x)$ splits in $k[x]$ and all of roots of $p(x)$ can be expressed in the form (a) for some .

Let $\rho \in G_{\mathbb{K}/\mathbb{L}}$, then an element such that , for some $\sigma \in G_{\mathbb{L}/\mathbb{K}}$.

Now $\rho \sigma = \sigma \rho \Rightarrow \rho \sigma \in \text{Galois} \Rightarrow \rho \sigma \rho^{-1} = \sigma$. 


\[ \Rightarrow \rho \circ \sigma \circ \tau = \sigma \circ \rho \circ \tau \quad \sigma, \tau \in G_k \]

\[ \Rightarrow \sigma \zeta \text{ is left fixed by each element of } G_k \]

for all \( \sigma \in G_k \). Hence \( p(x) \) splits in \( L[x] \).

which implies \( L \) is normal, \( L \) is already separably, so \( L \) is Galois extension.

Finally, to show:

Define \( \Psi: G_{e_j}^L \rightarrow G_{e_j}^L \)

\[ \sigma \mapsto \Psi \sigma \zeta \]

such that \( \Psi \) is the restriction of \( \Psi \sigma \in G_{e_j}^L = \sigma^* \)

(\( L \) normal, \( \Psi \sigma \in G_{e_j}^L \), so \( \Psi \sigma \) induces an automorphism \( \sigma^* \) of \( L \) defined by \( \Psi(l) = \sigma^*(l) \) for all \( \sigma \in G_{e_j}^L \).

Further \( \Psi \sigma \) is a homomorphism on \( L \).

Now \( \Psi \sigma_1, \sigma_2 \in G_{e_j}^L \)

but \( \Psi l \in L \)

\[ = \quad \Psi l \in L \]

\[ = \quad \Psi l \in L \]

\[ = \quad \Psi l \in L \]

\[ = \quad \Psi l \in L \]

is a homomorphism.
\[ \Leftrightarrow \sigma \in G_{E/L} \]

Hence \( \ker \).

Therefore

\[ \Rightarrow G_{E/k} \cong \text{Im} \Psi \subseteq G_{E/k} \]

Claim: \( \Psi \) is onto:

Now we use the result: Let \( k \) be a finite normal extension \( k \) and let \( F \) and \( L \) be \( k \)-isomorphic fields between \( k \) and \( K \). Then every \( k \)-isomorphism of \( F \) onto \( L \) can be extended to a \( k \)-automorphism of \( K \):

is extended to \( k \)-automorphism .

Hence \( \Psi \)

such that \( \Psi \circ \sigma \), Hence \( \Psi \) onto, so \( \text{Im} = \).

Finally, we get

S\( \text{olution of Polynomial equations by radicals:} \)

Definition:

An extension field \( K \) of \( k \) is called a radical extension of \( k \) if \( \exists \) elements such that

1. \( K = k \langle \sigma \rangle, \alpha_2, \ldots, \alpha_m \rangle \) and

2.

For \( f \in k[x] \), the polynomial equation \( f(x) = 0 \) is said to be solvable by radicals if \( \exists \) a radical extension \( K \) of \( k \) that contains all roots of \( f(x) \).

Theorem 9.

\[ \text{is solvable by radicals over } k \Leftrightarrow \text{the Galois group over } k \text{ of } f(x) \text{ is a solvable group.} \]

Definition:

Let \( k \) be a field, let \( \Phi \) and let \( K \) be a splitting field for \( f(x) \) over \( k \). Then \( G_{E/k} \) is called the Galois group of \( f(x) \) over \( k \) or the Galois group of the equation \( f(x) = 0 \) over \( k \). It can be shown that any
element of $\sigma \in G$ defines a permutation of the roots of $f(x)$ that lie in $K$.

as $\sigma \alpha \neq \alpha \in k$ so $\sigma f = \sigma$. Hence are roots of $f(x)$. Sinc there are only finitely many roots of $f(x)$ is one-to-one so defines a permutation of those roots of $f(x)$ that lie in $K$).

See Proof of the theorem : Topics in Algebra, by Herstein.

**Theorem 10.**
The general polynomial of degree is not solvable by radicals.

**Note:** is called general polynomial of degree over $k$.

**Proof:**
If $F(a_1, a_2, \ldots, a_n)$ is the field of rational functions in the $n$ variables $a_1, a_2, \ldots, a_n$, then the Galois group of the polynomial $f(x) = x^n + a_1 x^{n-1} + \ldots + a_n$ over $F(a_1, a_2, \ldots, a_n)$ is $S_n$, the symmetric group of degree $n$ (see thm 5.6.3, Hersteins Topics in Algebra). But $S_n$ is not solvable group when $n \geq 5$. Hence by thm 9, $f(x)$ is not solvable by radicals over $F(a_1, a_2, \ldots, a_n)$ when $n \geq 5$.

**Summary of basic results, questions and examples:**

1. Let $F$ be a subfield of a field $K$. $K$ may be regarded as a vector space over $F$. If is a finite dimensional vector space, we call $K$ a **finite extension** of $F$. If the dimension of the vector space $K$ is $n$, we say that $K$ is an extension of degree $n$ over $F$. We write $[K : F] = n$.

   This is read, "the degree of $K$ over $F$ is equal to $n."$

2. Let $e$ be algebraic over $F$ and let $p(x)$ be the minimal polynomial of $e$ over $F$. Let degree of $p(x)$ be $n$. Then $n$ elements are linearly independent over $F$ and generate the smallest field $F(c)$ which contains $F$ and $e$. Now $F(e)$ is a vector space of dimension $n$ over the field $F$. Hence the degree of $F(e)$ over $F$ is equal to the degree of the minimal polynomial of $e$ over $F$.

   $$[F(e) : F] = \deg p(x)$$

**Example 1.**

$$[Q(\sqrt{2}) : Q] = \deg \text{irreducible polynomial } p(x) = x^2 - 2$$

3. If $K$ is a finite extension of $F$ and $K = F(a_1, a_2, \ldots, a_n)$, then $a_1, a_2, \ldots, a_n$ have to be algebraic over $F$.

This is a consequence of important theorem:
4. If \( K \) is a finite extension of \( F \), every element of \( K \) is algebraic over \( F \).

**Example 2.**

\[
[Q \sqrt{2}, \sqrt{3} : Q] = [Q \sqrt{2}, \sqrt{3} : Q \sqrt{2}] [Q \sqrt{2} : Q] = 4
\]

Put \( Q \sqrt{2} = L \), \( Q \sqrt{3} = Q \sqrt{3} j \).

Then \( [Q \sqrt{2}, \sqrt{3} : Q \sqrt{2}] = [L \sqrt{3} : L] = 2 \),

the degree of independent polynomial \( p(x) = x^2 - 3 \) over \( L = Q \sqrt{2} \).

i.e. \( [L \sqrt{3} : L] = \deg L, \sqrt{3} = 2 \).

\[
[Q \sqrt{2} : Q] = \deg L, \sqrt{2} = 2 \text{ (from example 1)}
\]

Hence the result.

5. If \( p(x) \) is an irreducible polynomial of degree \( n \) in \( F[x] \), then \( F[x] / \langle p \rangle \cong F \langle \alpha \rangle \) where \( \alpha \) is a root of \( p(x) \). By (2), \( F(c) \) is of degree \( n \) over \( F \).

If \( a, b \) are roots of the same reducible polynomial \( p(x) \) over \( F \), then \( F(a) \cong F(b) \).

**Example 3.**

We construct a field of four elements. \( p(x) = x^2 + x + 1 \) is irreducible in \( Z_2[x] \), as \( p(1) \neq 0 \). \( p(0) \neq 0 \).

Hence \( Z_2[x] / \langle p \rangle \cong Z_2(\alpha) \) where \( \alpha \) is a root of \( p(x) \).

i.e.

Now elements of \( Z_2(e) \) are \( \{0, 1, c, c+1\} \) which is illustrated from the following tables:

<table>
<thead>
<tr>
<th>+</th>
<th>0</th>
<th>1</th>
<th>c</th>
<th>c+1</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>c</td>
<td>c+1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1+c</td>
<td>c</td>
</tr>
<tr>
<td>c</td>
<td>c</td>
<td>1+c</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>c+1</td>
<td>c+1</td>
<td>c</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>\times</th>
<th>1</th>
<th>c</th>
<th>c+1</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>c</td>
<td>c+1</td>
</tr>
<tr>
<td>c</td>
<td>c</td>
<td>c+1</td>
<td>1</td>
</tr>
<tr>
<td>c+1</td>
<td>c+1</td>
<td>1</td>
<td>c</td>
</tr>
</tbody>
</table>