Advanced Abstract Algebra

M.A./M.Sc. Mathematics (Previous)

Paper-I

Directorate of Distance Education
Maharshi Dayanand University
ROHTAK – 124 001

Maharshi Dayanand University
ROHTAK – 124 001

Developed & Produced by EXCEL BOOKS PVT. LTD., A-45 Naraina, Phase 1, New Delhi-110028

Contents

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

Normal and Subnormal series. Composition Series, Jordan-Holder theorem, Solvable groups. Nilpotent groups.

Unit III

Modules, submodules, cyclic modules, simple modules, Schure's Lemma. Free modules, Fundamental structure theorem for finitely generated modules over a principal ideal domain and its application to finitely generated abelian groups. Similarity of linear transformations. Invariant subspaces, reduction to triangular forms. Primary decomposition theorem and Jordan forms. Rational canonical form.

Unit IV

Rings, subrings ideals, skew fields, integral domains and their fields of quotients, Euclidean rings, polynomial rings, Eisenstein's irreducibility criterian. Prime field, field extensions, Algebraic and transcendental extensions, Splitting field of a polynomial and its uniqueness. Separable and inseparable extensions.

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

Group

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., such that:

1. $a.b \in G \quad \forall a,b \in G$ (closed)

2. (associative law)

3. $\exists$ an element such that $a.e = e.a = a$ (the existence of an identity element in G)

4. such that

   $a.b = b.a = e$ (The existence of an identity element in G)

Example 1:

Let

i.e. G is the set of nonsingular 2×2 matrix over rational numbers Q.

$G = \left\{ \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} : a_{ij} \in \text{Rational numbers } Q, \det(A) \neq 0 \right\}$ $\forall a,b,c \in G$

G forms a group under matrix multiplication. Infact, we note that

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

   Now $a.b$ under matrix multiplication is again 2×2 matrix over Q and det $(a.b)$ = (det a) (det b) $\neq 0$, as det a , det b .

2. We know that matrix multiplication is always associative. Therefore,

   $(a.b).c = a.(b.c) \; \forall a,b,c \in G$

3. $\exists e = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I \in G$ such that $a.I = I.a = a \;\; \forall a \in G$

4. If $a \in G$, say then

   we get $a^{-1} = \dfrac{1}{(a_{11}a_{22} - a_{21}a_{12})} \begin{bmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{bmatrix}$

$$a.a^{-1} = a.\left(\frac{1}{\det(a)}\,adj(a)\right) = I = e$$

similarly $a^{-1}.a = I = e$

$\therefore a^{-1} \in G$

Thus G is a group.

Note that $a.b \neq b.a \;\; \forall a,b \in G$. Infact, let

but a.b = $\begin{bmatrix} 11 & 7 \\ 3 & 2 \end{bmatrix} \neq \begin{bmatrix} 8 & 13 \\ 3 & 5 \end{bmatrix} = b.\,a$

Definition

A group G is said to be abelian (or commutative) if a.b = b.a. $\forall a,b \in G.$

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 a called a **finite group**.

Example 2:

$$G = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix} \right\}$$

G is again a set of 2 x 2 matrices with entries in $\mathbb{Z}$, integers, but containing only four elements.

Let $e = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, a = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, b = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, c = \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}$

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

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 $\mathbb{Z}$).

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, $a = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, b = \begin{pmatrix} 8 & 5 \\ 3 & 2 \end{pmatrix}$

Note that $a^{-1}\, b^{-1} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 2 & -5 \\ -3 & 8 \end{pmatrix} = \begin{pmatrix} 5 & -13 \\ -3 & 8 \end{pmatrix}$

$$\neq \begin{pmatrix} 2 & -7 \\ -3 & 11 \end{pmatrix} = (ab)^{-1}$$

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

$$(ab)\left(b^{-1}\, a^{-1}\right) = a\left(b b^{-1}\right)a^{-1} = a\, e a^{-1} = a^{-1} = e$$

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

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

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

$$(a_1\ a_2\ a_3 - - - a_n)^{-1} = a_n^{-1}\ a_{n-1}^{-1} - - - - a_2^{-1}\ a_1^{-1}$$
$$(a_i \in G, 1 \le i \le n)$$

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

$a^2 = e \Rightarrow a = a^{-1}\ \forall a \in G$ / $x, y \in G = \langle a \rangle$, then $x = a^n, y = a^m$, $n, m \in Z$, *Now*

and $\forall a, b \in G$,

$$\begin{aligned} ab &= (ab)^{-1}\ (\because ab \in G) \\ &= b^{-1}\ a^{-1} \\ &= b\ a. \end{aligned}$$

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 $x = a^n, n \in Z,\ \ \forall\ x \in G.$ It is denoted by $G = \langle a \rangle = \{a^n : n \in Z\}$

Remarks 1:

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

Let

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

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 indentity e and left inverse for all elements of g. show that G is a group.

Proof:

Let a $\in G$ and let b such that b a = e. Now

b a b = (b a) b = e b = b ....(i)

such that c b = e

Hence c (b a b) = cb = e from (i)

$\Rightarrow (cb)(ab) = e$

$\Rightarrow ab = e$

$\therefore$ b is also right inverse of a.

Further,

a e = a (b a) = (a b) a = e 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.

2. $a^{-1} \in H \quad \forall a \in H$

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 a^{-1} , i.e. e = a 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 (e). A nontrivial group has at teast two subgroups namely G and (e). Any other subgroup is called a **proper** subgroup.

Definition:

Let b, a G, b is said to be **Conjugate** of a G, if such that b = x^{-1} ax.

Problems:

1. Let a $\in$ G, let C_G(a) = {x G: x^{-1} ax = a}

   Prove that C_G(a) is a sbgroup of G.

2. is a sub group of G.

3. Find the centre of the group GL (2, **R**) of nonsingular 2 x 2 matrics over real numbers,

Solutions:

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

Let x,y $C_G(a)$. Then

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

$= x(x^{-1}ax)x^{-1} \quad \because x \in C_G(a)$

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

$= e \; a \; e$

$= a$

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

(a), hence $C_G(a)$ is subgroup of G

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

$= y^{-1} a y \quad \because x \in C_G(a)$

$= a \quad \because y \in C_G(a)$

$\Rightarrow xy \in C_G(a)$

Remarks:

so $C_G(a)$ is the set of all elements of G **commuting** with a.

we call $C_G(a)$, the centralizer of a

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

hence

Thus Z (G) is a subgroup.

Note that

Definition

Z (G) is called the **center** of the group G.

3. $let \;\; x = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in$ centre of GL (2, IR)

$\therefore$ x commutes with all non-singular 2 x 2 matrices, So in particular x commutes with

$$\begin{pmatrix}1&1\\0&1\end{pmatrix}, \begin{pmatrix}1&0\\1&1\end{pmatrix} \in GL\left(2, IR\right)$$

$$x\begin{pmatrix}1&1\\0&1\end{pmatrix} = \begin{pmatrix}a&b\\c&d\end{pmatrix}\begin{pmatrix}1&1\\0&1\end{pmatrix} = \begin{pmatrix}a&a+b\\c&c+d\end{pmatrix} \quad .... (1)$$

$$\begin{pmatrix}1&1\\0&1\end{pmatrix} x = \begin{pmatrix}1&1\\0&1\end{pmatrix}\begin{pmatrix}a&b\\c&d\end{pmatrix} = \begin{pmatrix}a+c&b+d\\c&d\end{pmatrix} \quad .... (2)$$

(1) and (2) gives

$$\begin{pmatrix}a&a+b\\c&c+d\end{pmatrix} = \begin{pmatrix}a+c&b+d\\c&d\end{pmatrix}$$

Hence c = 0, a = d

Similarly, gives

b = 0.

Therefore $x = \begin{pmatrix}a&0\\0&a\end{pmatrix}$ *where* $a \neq o,\ a \in \mathbf{R}$

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 H}. This set is called **right coset** of H in G. As e H, so a = e a Ha. Similarly aH = {ah / a 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 G.

Then

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

Proof:

1. $a = ea \in Ha \quad \left(e \in H\right)$
2. Let , Now h due to closure in H.

$\therefore$ $Ha \subseteq H$. To show let h be any element of H.Since

We get a^{-1} and h a^{-1} . Hence h = he = h (a^{-1} a)

= (h a^{-1})a a. So . Thus H = Ha.

Ha = H e a a .

3. Suppose

Then x = h_1a and x = h_2 b, for some h_1, h_2 $\in H$,

Thus

4. $Ha = Hb \Leftrightarrow H = Hba^{-1} \Leftrightarrow ba^{-1} \in H$, from (2)

5. Define $f : Ha \rightarrow Hb$ by $ha \rightarrow hb$ $\forall h \in H$.

$\therefore$ 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, H_1 = {e, a}, H_2 = {e, b}, H_3 = {e, c} order of each H_i, i = 1, 2, 3, is 2. Hence O (H_i) | 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 distinict right cosets of H in G, say Ha_1, Ha_2,............., Ha_r. Now for each a in G, We have Ha = Ha_i for some i. By property (i) of Lemma 1, $a \in Ha$. Hence, each element of G belongs to one of Cosets Ha_i, i.e.

By property (3) of lemma 1,

$$Ha_i \cap Ha_j = \phi,$$
$$for \;\; i \neq j.$$

$\therefore$ $|G| = |Ha_1| + |Ha_2| + ... |H_{ar}|$ for each i.

(Because $f : H \rightarrow Ha_i$ $defined$ by $h \rightarrow ha_i$ is one-one & onto).

Therefore we get

$$|G| = |H| + |H| + ---------- + |H|$$
$$\rightarrow \quad r\ times \quad \leftarrow$$
$$i.e. \quad |G| = r\,|H|$$

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 Lagranges 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 $|G{:}H| = {|G|}/{|H|}$.

We can say:

$$|G| = |H| \times index\ of\ \ H\ in\ G.$$

Corollary 1:

$$|a|\, dvides\ |G|$$

In a finite group, the order of each element of the group divides the order of the group.

Proof:

$|a| = o(< a >)$ = order of the subgroup generated by , Hence the corollary.

Corollary 2:

Groups of Prime order are cyclic.

Proof:

divides .

but $o(\langle a\rangle) \neq 1 and\ |G|\ is\ prime. Hence\ o(\langle a\rangle) = |G|.$

Therefore $\langle a\rangle \leq G \Rightarrow G = \langle a\rangle\ \ ie..G\ \ is\ cyclic.$

Corallary3:

$a^{|G|} = e.$

let G be a finite group, and let $a \in G$. Then

Proof:

$|G| = |a|n$, n is a positive integer, by Corollary 1.

$$Hence \quad a^{|G|} = a^{|a|n}$$
$$= (a^{|a|})^n = e^n$$
$$= e$$

Corollary 4: (Feremat's Little Theorem):

For every integer a and every Prime p, $a^p \equiv a \pmod p$.

Proof:

By division algorithm, $a = pm + r$, $0 \le r < p$. Hence

$a \equiv r \pmod p$. The result will be proved if we prove r^p r (mod 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 r (mod 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 a H = Ha for every a in G. This is denoted by $H \varDelta G$.

Warning:

H G does not indicate ah = ha

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

A subgroup H of G is normal in G if and only if $xHx^{-1} \le H \; \forall x \in G$.

$xHx^{-1} \subseteq H \; \forall x \in G \Rightarrow xH \subseteq Hx \; \forall x \in G$ and

$x^{-1}Hx = x^{-1}H(x^{-1})^{-1} \subseteq H$, hence $Hx \subseteq xH \; \forall x \in G$,

$= Ha\,bc = Ha\,(Hbc) = Ha\,(Hb\,Hc) \; \forall a,b,c \in G$.

Factor groups (or quotient groups):

Let $H \varDelta g$. 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 $G/H = \{Ha / a \in G\}$ 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 $a_1 = h_1 a$ and $b_1 = h_2 b$, $h_1, h_2 \in H$.

Therefore, $Ha_1b_1 = Hh_1\, ah_2b = Ha\, h_2b = aHh_2b = aHb = Hab$

(In proving this we used Ha = H a H and H G).

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

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

Theorem3: ***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 $g^{-1} Z(G) g \subseteq Z(G) \ \forall g \in G.$

let $x \in Z(G)$ *then*

$$g^{-1}xg = g^{-1}(xg) = g^{-1}(gx) \quad (\because x \in Z(G))$$
$$= (g^{-1}g)x = ex = x \in Z(G)$$

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

Therefore, $g^{-1}Z(G)g \subseteq Z(G) \ \forall g \in G.$

We can now form a factor group

Let $G/Z(G) = \langle x\,Z(G) \rangle$ ($\because G/Z(G)$ is cyclic)

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

hence

$$aZ(G) = (xZ(G))^n = x^n Z(G)$$

and $bZ(G) = (xZ(G))^m = x^m Z(G)$ where n, m are integers.

Thus $a \in aZ(G) \Rightarrow a = x^n y$ for some $y \in Z(G)$

and $b = x^m t$ for some $t \in (G)$

Now

$$= b\,a$$

We often use it as: If G is not abelian, then is not cyclic.

Definition: Group Homomorphism

Let be a mapping from a group G to a group defined by

$: G$

a

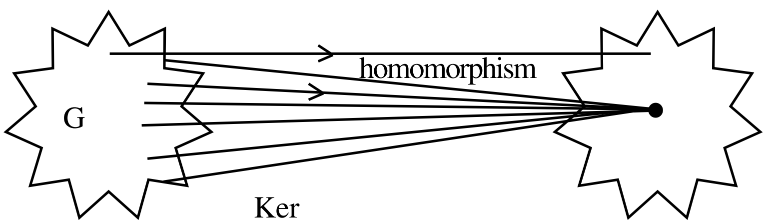
$$f(ab) = f(a)f(b)\ \forall a,b \in G.$$

f is called homomorphism of groups.

Definition: Kernel of a Homomorphism

Let $: G$ be a group homomorphism and be the identify of . Then Kernel of denoted by Ker is defined by

Ker =



We note that ker G. (It is easy to show that ker f is a subgroup of G)

We show that

Let x be any element of ker .

Then

$$f(g^{-1})f(g) = f(g^{-1}g) \quad (\because f \text{ is homomorphism})$$

$$= f(e)$$

$$= \bar{e}$$

(Any homomorphism of groups carries identity of G to identity of)

Explanation:

$$= f(xe)$$

$$= f(x)f(e) \text{ in } \overline{G}$$

So by cancellation property in , we have = (e).)

Hence

$$\Rightarrow g^{-1}xg \in \ker f\ \forall g \in G, \forall x \in \ker f \ \Rightarrow \ker f \Delta G$$

Lemma 2:

Let be a homomorphism of G into , then

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

2.

3. $f\left(x^n\right) = \left(f(x)\right)^n \; \forall x \in G$

Proof :

(1) is proved above

(2) $\bar{e} = f(e) = f\left(x\,x^{-1}\right) = f(x)\, f\left(x^{-1}\right)$

$\Rightarrow (f(x))^{-1}\,\bar{e} = (f(x))^{-1} f(x) f\left(x^{-1}\right)$ in $\overline{G}$

$\Rightarrow (f(x))^{-1} = \bar{e} f\left(x^{-1}\right) = f\left(x^{-1}\right), \; \forall x \in G$

Example 4:

G = GL (2, R): group of nonsingular 2×2 matrices over reals and R* be the group of nonzero real number under multiplication. Then

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

$A \qquad (A) = \det A$

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

Hence is a homomorphism

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

Theorem 4: (Fundamental Theorem of Group Homomorphism)

Lef $: G$ be a group homomorphism with K = ker . Then

$$G/k \cong f(G)$$

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

($\cong$: Isomorphic, when is homomorphism, 1–1 and onto).

Proof:

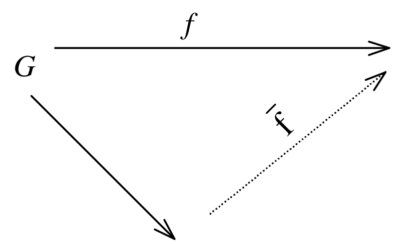
Consider the diagram

f

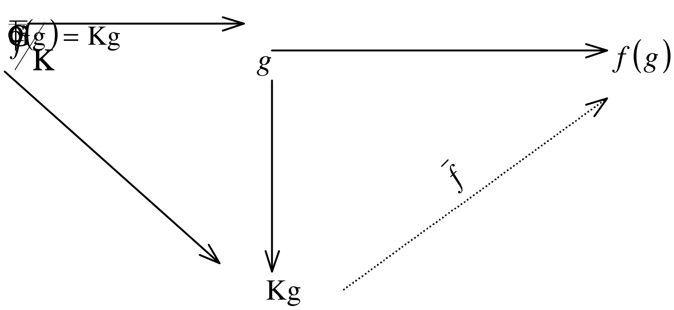
G

where

The above diagram should be completed to



We shall use



to complete the previous diagram.

Define $\bar{f}(kg) = f(g)_s \ \forall$ coset $Kg \in G/K$

$\overline{f}$ is well defined: Let $Kg_1 = Kg_2, g_1, g_2 \in G$

Then $g_1 = kg_2, k \in \ker(f) = K$, and

$$f(g_1) = f(kg_2) = f(k)f(g_2) = \bar{e}f(g_2) = f(g_2)$$

is a homomorphism since

$$\bar{f}(Kg_1\ Kg_2) = \bar{f}(Kg_1g_2) = f(g_1g_2) = f(g_1)f(g_2)$$

(Θ f is a homomorphism).

$\overline{f}$ is 1–1 since $\overline{f}\,(kg_1) = \overline{f}\,(kg_2) \Rightarrow$

$f(g_1) = f(g_2)$, hence $f(g_1)f(g_2)^{-1} = \overline{e}$ and $f(g_1^{-1}g_2) = \overline{e}$ ($\Theta\ \overline{f}$ is a homo).

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

Consider Again Example 4:

$f : GL_n(R) = GL(n, R)$ R^*

A

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

So is a homomorphism.

the identity of R*.

$\Leftrightarrow A \in SL_n(R) = SL(n, R)$, the subgroup of of all n×n matrices with determinant 1.

By above fundmental homomorphism theorem, we get

$$\frac{GL(n,R)}{ker\ f} \cong Im(f)$$

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

But f is onto, since for

$$A = \begin{pmatrix} a_{1_{1_1}} & & 0 \\ & \ddots_1 & \\ 0 & & \end{pmatrix}_{n\times n} \in GL(n,R) \text{ such that } f(A) = \det A = a$$

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

Theorem 5 (First Isomorphism Theorem)

Let *G* be a group with normal subgroup *N* and *H* such that $N \subseteq H$

Then and

$$\left(G/N\right)\Big/\left(H/N\right) \cong G/H$$

Define $f : G/N \longrightarrow$ by

$Na \rightsquigarrow Ha$

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

$\Leftrightarrow Ha = H$

$\Leftrightarrow a \in H$

Hence ker . As ker $f \trianglelefteq G/N$, so $H/N \trianglelefteq G/N$

The fundamental homomorphism theorem for groups implies that

$$G/N \Big/ \ker f \cong \operatorname{Im} f = G/N$$

$f(Nab) = Hab = HaHb = f(Na)f(Nb)$

$(H \cap N)$

$\Leftrightarrow a \in N$ *and* $a \in H$

$\Leftrightarrow a \in H \cap N$

$$\therefore \; G/N \Big/ H/N \cong G/H$$

Theorem 6 (Second Isomorphism Theorem)

Let G be a group, and let $N \trianglelefteq G$, let H be any subgroup of g. Then HN is a subgroup of G, and

Proof:

Define $f{:}H \longrightarrow$ by $a \rightsquigarrow$

is a homomorphism since

a $\in \ker f \Leftrightarrow f(a) = N$, 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 , so $aN = Na$, hence $NaN = NNa = Na$.

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

i.e. $H \big/ H \cap N \cong \frac{HN}{N}$

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 then $G \cong \mathbb{Z} \big/ < n >$

Proof:

1. Let g = <*a*> be infinite cyclic group.

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

   f is a homomorphism, since

   f is onto: since G = <a>, so for any we get $x = a^m$ for some integer m,

   Hence $f(m) = a^m = x \Rightarrow f$ is onto f is 1–1: Let for $m,\ n \in \mathbb{Z}$, with

   Then multiplying by , we get $a^{m-n} = e$ 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 $f : \frac{\mathbb{Z}}{< n >} \longrightarrow G$ by $[m]$

   f is well-defined. We should show that if then where a has finite order n.

   $a^k = a^m \Leftrightarrow a^{k-m} = e \Leftrightarrow n|(k-m) \Leftrightarrow k \equiv m (\text{mod } n)$

   f is onto, since G = <a>.

   is 1–1: let then as above

Also

$\therefore f$ is an isomorphism. Hence every finite cyclic group of order n is isomorphic to additive group of integers mudule 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

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

Therefore,

$$A^r = a^{n-qm} = a^n(a^{-qm})$$
$$= a^n (a^{qm})^{-1} \in H$$

Hence r = 0 , otherwise it will contradicts the fact that m is the least positive integer such 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 $a^m \in G$, $m \in \mathbf{Z}$, then

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

The question arises which of the elements of G other than a and a^{-1} can be 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

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

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

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

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

$$a^{t+1} = a^{rt} \quad \text{for some integer r.}$$

Since G is infinite, this implies

$$t+1 = rt$$
$$\Rightarrow \quad (r-1)t = 1$$

which holds only if t = 1± 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 $a^m \in G$, $m \le n$ is a generator of G if and only if g c d (m, n) = 1.

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

$$um + vn = 1$$
$$\Rightarrow \quad a^{um+vn} = a$$
$$\Rightarrow \quad a^{um} . a^{vn} = a$$
$$\Rightarrow \quad (a^m).(a^n)^v = a$$
$$\Rightarrow \quad (a^m)^u = a \ \ (\Theta \ (a^n)^v = e)$$
$$\Rightarrow \quad a \in H \ (\Theta \ (a^m)^u \in H)$$
$$\Rightarrow \quad G \subseteq H .$$

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

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

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

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

Therefore, we can find an integer u such that

$$a^{mu} = a$$
$$\Rightarrow \quad a^{mu-1} = e$$
$$\Rightarrow \quad O(a) \mid (mu - 1)$$
$$\Rightarrow \quad n \mid (mu-1)$$

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 ≠ {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

$$< a^m > \subseteq H \qquad \text{(i)}$$

Moreover,

$$a^{\lambda} \in H \Rightarrow \lambda = qm, \; q \in \mathbf{Z}$$

Therefore

$$a^{\lambda} = a^{qm}$$
$$= (q^m)^q \in < a^m >$$
$$\Rightarrow < a^{\lambda} > \subseteq < a^m >$$
$$\Rightarrow \quad H \subseteq < a^m > \qquad \text{(ii)}$$

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 ≤ 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

$$a^m \in < a^d >$$
$$\Rightarrow H = < a^m > \subseteq < a^d > \ldots. \qquad \text{(i)}$$

Since gcd (m, n) = d, we can find u, v ∈ Z such that

$$d = un + vm$$
$$\Rightarrow \quad a^d = a^{un+vm}$$
$$= a^{un} . a^{vm}$$
$$= a^{vm} \; (\Theta \; a^{un} = e)$$

But $a^{vm} \in < a^m > = H$. Therefore

$$a^d \in H$$
$$\Rightarrow < a^d > \subseteq H \quad \ldots.. \qquad \text{(ii)}$$

From (i) and (ii), we have

$$H = \langle a^d \rangle$$

$$\Rightarrow\ O(H) = O(\langle a^d \rangle)$$

But

$$O(\langle a^d \rangle) = \frac{n}{d} \qquad\qquad (\Theta\ (a^d)\ \frac{n}{d} = e)$$

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

$$f : G \to H$$

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

$$B^r = b^s \Rightarrow\ b^{r-s} = e$$

$$\Rightarrow\quad n \mid (r-s)$$

$$\Rightarrow\quad nu = r-s, \qquad u \in \mathbf{Z}$$

$$\Rightarrow\quad a^{r-s} = a^{nu}$$

$$= (a^n)^u = e$$

$$\Rightarrow\quad a^r = a^s.$$

Hence f is 1−1 mapping also. Therefore, $G \simeq H$.

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

$$b = \underbrace{f(a).f(b)\ldots f(c)}_{r\,\text{factors}}$$

$$= (f(a)^r$$

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 **permulation 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 σ 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

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

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

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

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

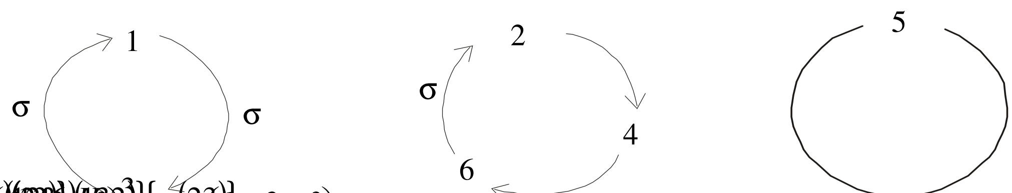
Note that $\alpha\beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \beta\alpha$

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 upto isomophism, 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:



$[S_3 : A_3] = \frac{|S_3|}{|A_3|}$, $\alpha\beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$, $\alpha^2\beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$, $\{e, (23)\}$

In cycle notation σ 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 $A_3 \trianglelefteq S_3$. Infact, it can be generalised, that every subgroup of index 2 is a normal subgroup in its parent group. is called **alternating** group.

Example. Let

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \text{ and } \beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

be two permutations belonging to S_3. Then

$$\alpha o \beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} o \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

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

and

$$\beta o \alpha = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

Thus $\alpha o \beta = \beta o \alpha$. Hence α and β commute with each other.

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

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \ \beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

then

$$\beta o \alpha = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

and

$$\alpha o \beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

Hence

$$\alpha o \beta \neq \beta o \alpha .$$

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

$$\sigma(x_j) = x_j, \ j \neq 1, 2, \ldots, k;$$

then σ is called a **cycle of length k.** We denote this cycle by

$$\sigma = (x_1 x_2, \ldots, x_k)$$

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

$$f(a) = b, \ f(b) = c, \ f(c) = a.$$

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, α and β are disjoint if every $x \in S$ moved by one permutation is fixed by the other.
Further, if α and β are disjoint permutations, then $\alpha\beta = \beta\alpha$. For example, if we consider

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \ \beta = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

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

$$f(y_1) = y_2$$
$$f(y_2) = y_3$$
$$\ldots\ldots\ldots..$$
$$\ldots\ldots\ldots..$$
$$f(y_{k-1}) = y_k$$
$$f(y_k) = y_1$$

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

$$f = (y_1\ y_2\ \dots\ y_k) \circ g$$
$$= (y_1\ \ y_2\ \dots.\ y_k)\ \ \alpha_1\ \alpha_2\ \dots\ \alpha_m$$

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

For example, let

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 4 & 7 & 2 & 5 & 1 & 8 & 9 & 3 \end{pmatrix}$$

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 $(x_1, x_2, \dots, x_m)$. A simple computation shows that

$$(x_1\ x_2 \dots.\ x_m) = (x_1\ x_m)\ \dots.\ (x_1\ x_3)\ \ (x_1\ \ x_2),$$

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 σ be expressed as the product of transpositions as given below:

$$\sigma = \alpha_1\alpha_2 \dots.\ \alpha_r = \ \beta_1\beta_2 \dots \beta_s$$

This yields

$$e = \alpha_1\alpha_2 \dots \alpha_r\ \ \beta_s^{-1}\ \beta_{r-1}^{-1}\beta_1^{-1}$$
$$= \ \alpha_1\alpha_2 \dots \alpha_r\ \beta_s\beta_{s-1}\ \dots.\ \beta_2\beta_1\ ,$$

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 $O(A_n) = \frac{\underline{|n}}{2}$.

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

$$f: S_n \to W$$

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

$$\begin{aligned} K &= \{\alpha \in S_n : f(\alpha) = eW = 1\} \\ &= \{\alpha \in S_n : f(\alpha) = 1\} \\ &= \{\alpha : \alpha \text{ is even}\} \\ &= A_n . \end{aligned}$$

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,

$$\begin{aligned} O(W) &= O\left(\frac{S_n}{A_n}\right) \\ &= \frac{O(S_n)}{O(A_n)} \end{aligned}$$

But $O(W) = 2$, therefore,

$$2 = \frac{O(S_n)}{O(A_n)}$$

or

$$O(A_n) = \frac{O(S_n)}{2} = \frac{\underline{|n}}{2}$$

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 $\frac{\underline{|n}}{2}$.

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

Claim: ϕ_g is a permutation on G.

ϕ_g onto: Let x be any element of G. So $\exists\ g^{-1}x \in G$ such that

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

ϕ_g is one-one:

Let $\phi_g(x) = \phi_g(y)$

so gx = gy; hence

$\Rightarrow x = y.$

Now,

Let

Claim:

is a group of permutations under composition of mappings.

$= g\ (hx)$

Hence $\phi_g\ \phi_h = \phi_{gh}\ \forall\ g, h \in g.$

$((\phi_g\ \phi_h)\ \phi_t)(x) = (\phi_{gh}\ \phi_t)\ (x)$

$= \phi_{(gh)\,t}\ (x)$

$= \phi_g \phi_{ht}\ (x) = (\phi_g\ \phi_{ht})\ (x)$

$= \phi_g\ (\phi_{ht}\ (x))$

$$= \phi_g \, (\phi_h \, \phi_t)\,(x)$$

(associative)

ϕ_e is the identiy and $\phi_{g^{-1}} = (\phi_g)^{-1}$

$\phi_g \, \phi_e = \phi_{ge} = \phi_g \;\forall\; g \in G,$ and

$\phi_g \, \phi_{g^{-1}} = \phi_{gg^{-1}} = \phi_e,$ hence $(\phi_g)^{-1} = \phi_{g^{-1}})$

Thus $\bar{g} = \{\phi_g : g \in G\}$ is a group of permutations.

Define ψ :

$g \to \phi_g \qquad \forall\, g \in G$

i.e. ψ

If g = h, then is trivial, so ψ is a function.

ψ is one-to-one:

If then $\phi_g\,(e) = \phi_h\,(e)$ *or* $ge = he$ i.e.

[illegible] = ψ(h) g = h, i.e. ψ is one-one.

by definition of ψ,

ψ is onto.

ψ is a homomorphism:

ψ ψ ψ

Hence is an isomorphism and so

Remark:

$\bar{g}$ 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 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

Proof.

Every even permutation is the product of an even number if 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 If (a', b', c') is another 3 – cycle and such that

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

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

$\because \pi \in S_n$, so π 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 can not 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

$$\pi^1 = (a_1, a_2, a_3)\,\pi\,(a_1, a_2, a_3$$

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

$$= \begin{pmatrix} a_2 & a_3 & a_4 & a_5 & ---- \\ a_1 & a_2 & a_3 & a_4 & ---- \end{pmatrix} ----- \begin{pmatrix} a_2 & a_3 & a_1 & --- \\ a_3 & a_1 & a_4 & --- \end{pmatrix} ----$$

$= (a_2, a_4, a_1)$: 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

$(a', c, b')\ (a, b, c)\ (a', b', c')\ ----\ (a', b', c) = (a', a, b)\ (c, c', b')$

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 π.

Hence N contains

It follows that if then

$(a, a', c, b, c')\ ---------$

But then N will also contain

$\pi = (a_3, b_2)\ (a_2, b_4)\ \pi\ (a_2, b_1)\ (a_3, b_2)$

$= (a_1, a_2)\ (a_3, b_1)\ (b_2, b_3)\ (a_4, b_4)\ ----$ and hence $\pi\ \pi' = (a_1, a_3, b_2)\ (a_2, b_3, b_1)$ which is final contradiction.

Hence A_n is simple for $n \geq 5$.

As promissed earliar, to give an example that converse of Lagranges 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.

A_4 has 4 cyclic subgroups of order 3.

The Klein's four – group V_4:

is a normal subgroup of A_4.

Each

But N_i is not normal subgroup of A_4 i.e.

Hence Normality is not a transitive relation i.e.

$A \trianglelefteq B,\ B \trianglelefteq C \not\Rightarrow A \trianglelefteq C$ in genral.

Converse of Lagrange's Theorem:

but A_4 does not contain a subgroup of order 6.

Suppose $\exists\, a$ subgroup H in A_4 of order 6. Then $[A_4 : H] = 2 \Rightarrow H \trianglelefteq A_4$

So we consider a quotient group A_4/H.

(123), (124), (134), (234), (132), (142), (143), (243) are elements of A_4.

$\because \left|\dfrac{A_4}{H}\right| = 2, \therefore ((123)\,H)^2 = H,$ the identity of

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

$\Rightarrow (132) \in H$

Similarly, we can show

(123), (124), (142), (134), (143), (234), (243)

are elements of H. Therefore H contains 8 elements, which is absurd.

has no subgroup of order 6, although $6 \,\|A_4\|$.

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 $\in$ a group g, then g is abelion.

Solution:

To show ab = ba $\forall$a, . As m, n are relatively prime positive integers, therefore, mx + ny = 1for 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

$$ab = a^{mx-ny}\ b^{mx-ny}$$

$$= a^{mx}\left[a^{-ny}\ b^{-ny}\right] b^{mx}$$

$$= a^{mx}\left\{\left(a^{-y}\right)^{n}\left(b^{-y}\right)^{n}\right\} b^{mx}$$

$$a^{mx}\left[\left(a^{-y}\right)^{n}\left(a^{-y}\right)^{n}\right] b^{mx} \quad \left(\because a^{-y},\ b^{-y} \in G\right)$$

Claim: $g_1^m g_2^n = g_2^n\ g_1^m \ \forall\ g_1 g_2 \in G \ \forall$

Consider

Caution:

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

$=$

$g_1^m g_2^n = g_1^m g_2^n g_1^m g_1^{-m} = g_1^m \left(g_2^n g_1^m\right)\left(g_2^n g_1^m\right) \ldots \left(g_2^n g_1^m\right) g_1^{-m}$ *mx times*, $mx \in N$ *the set of natural numbers.*

$$= g_1^m \left(g_3^x\right)^m g_1^{-m},\ where\ g_3 = \left(g_2^n g_1^m\right) \in G$$

$$= \left(g_3^x\right)^m g_1^m g_1^{-m} \quad \because a^m b^m = b^m a^m \ \forall\ a, b \in G$$

(1)

Also $\left(g_1^m g_2^n\right)^{-ny} = \left\{\left(g_1^m g_2^n\right)^{ny}\right\}^{-1}$

$$= \left\{\left(g_2^n g_1^m\right)^{ny}\right\}^{-1} \text{ from above}$$

as $ny \in N$.

$\therefore \left(g_1^m g_2^n\right)^{-ny} = \left(g_2^n g_1^m\right)^{-ny}$ (2)

Hence from (1) and (2) we get

$\Rightarrow$ $\forall\ g_{1,} g_2 \in G,\ \forall$ (3)

Therefore,

ab =

$= (a^x)^m (b^{-y})^n (a^{-y})^n (b^x)^m \quad (\because a^x, b^{-y} \in G)$

$= (b^{-y})^n (a^x)^m (b^x)^m (a^{-y})^n \quad (\because b^x, a^{-y} \in G)$ from (3)

$= (b^{-y})^n (b^x)^m (a^x)^m (a^{-y})^n \quad (\because a^m b^m = b^m a^m \ \forall\ a, b \in G)$

=

= b a

is ab = ba and $a,\ b \in g$.

(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 Z_n^x is finite and $|Z_n^x| = o(Z_n^x) = \phi(n)$, the Eulers phi-function.

Special Case: Z_8^x

Multiplication table in Z_8^x

	[1]	[3]	[5]	[7]
[1]	[1]	[3]	[5]	[7]
[3]	[3]	[1]	[7]	[5]
[5]	[5]	[7]	[1]	[3]
[7]	[7]	[5]	[3]	[1]

Z_n^x = {[1], [3], [5], [7]} : Set of units (invertible elements) modulo 8, [3] [3] = [9] $\equiv$ [1] mod 8

[5] [5] = [25] [1], [7] [7] = [49] [1].

$\phi(8) = 4$.

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

Set of units modulo 15.

x_{15}	[1]	[2]	[4]	[7]	[8]	[11]	[13]	[14]
[1]	[1]	[2]	[4]	[7]	[8]	[11]	[13]	[14]
[2]	[2]	[4]	[8]	[14]	[1]	[7]	[11]	[13]
[4]	[4]	[8]	[1]	[13]	[2]	[14]	[7]	[11]
[7]	[7]	[14]	[13]	[4]	[11]	[2]	[1]	[8]
[8]	[8]	[1]	[2]	[11]	[4]	[13]	[14]	[7]
[11]	[11]	[7]	[14]	[2]	[13]	[1]	[8]	[4]
[13]	[13]	[11]	[7]	[1]	[14]	[8]	[4]	[2]
[14]	[14]	[13]	[11]	[8]	[7]	[4]	[2]	[1]

$O(7) = 4$, as $7^1 = 7, 7^2 = 4, 7^3 = 28 \equiv 13, 7^4 = 91 \quad 1$

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

Note: To get calculation easier:

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

We calculate as follows:

$13 \quad -2 \pmod{15}, 13^2 \quad (-2)^2 = 4,$

$13^3 = 13^2 \times 13 \quad 4(-2) \quad -8$

$13^4 \quad -8 \times -2 \quad 1 \pmod{15}.$

Q.1. Show that the set of all 2×2 matrices over reals of the form with forms a group under matrix multiplication. Find all elements that commute with element $\begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}$.

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

Q.3. Find the inverse of in GL $(2, Z_{11})$.

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

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

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

$f_{a,b}(x) = ax + b \ \forall$

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

   $i.e.\ f_{a,b} \in S_n$

2. Prove that

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

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

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

1. Prove that for each integer n, f_n is a permutation of R.

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

3. Prove that $g = \{f_n, n \in Z\}$ 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 $f_1(x) = x$, $f_2(x) = -x$, $f_3(x)=$, $f_4(x) = -1/x$ $\forall\ x \in R$, 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 (1)

$(ab)^{i+1} = a^{i+1}b^{i+1}$ (2) $i \in Z$

(3)

$(ab)^{i+1} = (ab)^i(ab)$

$= a^i b^i (ab)$

$=$ from (2)

$\therefore a^i b^i ab = a^{i+1}b^{i+1}$

$\Rightarrow b^i a = ab^i$ (4)

Similarly $(ab)^{i+2} = a^{i+2}b^{i+2}$

$\Rightarrow b^{i+1}a = ab^{i+1}$

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

$\Rightarrow b[ab^i] = ab^{i+1}$, from (4)

$\Rightarrow ba = ab$ $\forall\ a,b \in G.$

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:

$x = x^1 = x^{mt+ns}$

$= x^{mt}.x^{ns}$

Put $a = x^{mt}, b = x^{ns}$

Then $x = ab = ba \left(x^{mt+ns} = x^{ns+mt}\right)$

must have order n.

Thus $\left(x^n\right)^t$ has order n, since (m, n) = 1 (if o(a) = n, o(a^r) = m and (n, r) = d, then m = n/d)

Similarly x^{ns} 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 $(ab)^{mt} = (a_1b_1)^{mt}$

(1) $\left(\because a_1b_1 = b_1a_1, ab = ba\right)$

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

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

$\Rightarrow a^{1-ns} = a_1^{1-ns} \left(\because mt + ns = 1\right)$

$\Rightarrow a = a_1 . a_1^{-ns} . a^{ns}$

$\Rightarrow a = a_1 . a_1^{-ns} e \left(\because o(a) = n\right)$

$\Rightarrow aa_a^{ns} = a_1 . a_1^{-ns} . a_1^{ns} = a_1$

$\Rightarrow ae = a_1 \left(\because o(a_1) = n\right)$

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 genertors = $\phi(n) = \phi(13) = 12$ $(\because \phi(p) = p-1)$
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 , then prove that $a^{-m}b^s a^m = b^{snm}$. Hence deduce that if then $o(b) = 31.$

Solution.

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

$= a^{-2}ba^2 = (b^n)^n = b^{n^2} \Rightarrow a^{-3}ba^3 = b^{n^3}$

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

$\Rightarrow b^s = (b^s)^{2^5} \Rightarrow b = b^{32}\ (if\ s = 1)$

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

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

(i) Finite non-abelion group.

(ii) Infinite non-abelian group.

(iii) Abelion 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 defined by $\forall$ Let $G = \{\tau_{ab} | a \neq 0\}$

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

ii. Let . Show that

iii. $N = \{\tau_{1,b} \in G\}$, show that

Solution.

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

$= a(cx+d)+b$

$=$ $\forall\ x \in R$

$=$

$\therefore\ \tau_{a,b} o\ \tau_{c,d} = \tau_{ac,\, ad+b} \in G\ (\because ac \neq o \text{ in } R)$

$= \tau_{a(cf),a(cl+d)+b}$

$= \tau_{a,b} o\, \tau_{cf,cl+d}$

$= \tau_{a,b} o\, (\tau_{c,d} o\, \tau_{f,l})$ $\forall$

$b, d, l \in R$

For identity element:

[illegible]

$=$

$\therefore\ \tau_{1,0} \in G \text{ such that } \tau_{a,b} o\ \tau_{1,0} = \tau_{a1,\, o+b} = \tau_{a,b}\quad \forall\ \tau_{a,b} \in G.$

Hence $_{1,0}$= e, the identity of G.

For inverse element:

$\Rightarrow\ ac = 1,\ ad + b = 0$

$\therefore\ c = \frac{1}{a},\ d = -a^{-1}b\ (\because +a \in R)$

Hence $\tau_{c,d} = \tau_{a^{-1},\, -a^{-1}b}$ is the right inverse of $\tau_{a,b}$

$\therefore\ G = \{\tau_{a,b} | a \neq 0\}$ is a group.

(ii) H =

From above H is a subgroup of G.

To show $\forall\ \tau_{c,d} \in G\ \forall$

L.H.S.=

$$= \tau_{(ca)\, c^{-1},\ -(ca)(c^{-1}d)+cb+d} = \tau_{a,\ -ad+cb+d} \in H$$

(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 $ab^{-1} = x^n (y^n)^{-1} = x^n (y^{-1})^n = (xy^{-1})^n$ d $y^{-1},\ x \in g$ i

is a subgroup of g.

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

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

$z \in G^{(n)} \Rightarrow z = x^n,\ x \in G.$

$aza^{-1} = ax^n a^{-1} = (axa^{-1})^n$ b n *is an integer* > 1 g

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

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

$ab^{-1} = x^{n-1}(y^{n-1})^{-1} = x^{n-1}(y^{-1})^{n-1} = (y^{-1}x)^{n-1} \in G^{(n-1)}$ d $y^{-1}x \in G$ i

is a subgroup of G.

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

abab------ab = a^nb^n

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

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

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

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

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

Now $aza^{-1} = ax^{n-1}a^{-1} = (axa^{-1})^{n-1} \in G^{(n-1)}\ (\because\ axa^{-1} \in G)$

$\Rightarrow\ G^{(n-1)} \trianglelefteq G.$

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

(1)

Also

(2)

$= a^{-1}b^na$ from (1) and (2)

$\Rightarrow\ b^na^{n-1} = a^{n-1}b^n$

(iv) To show

$$(aba^{-1}b^{-1})^{n(n-1)} = e\ \ \forall\ a,\ b \in G$$

L.H.S. =

$= \{(ba^{-1}b^{-1})^{n-1}a^{n-1}\}^n\ \ (\because\ (ba)^{n-1} = a^{n-1}b^{n-1}\ \textit{from above})$

$= (ba^{-(n-1)}b^{-1}a^{n-1})^n$

=

=

=

$= b^n a^{-(n-1)} a^{n-1} (b^{-1})^n$ from (iii) Θ $a^{n-1} b^n = b^n a^{n-1}$ $\forall$

=

Example 9.

Let S be a semi-group. If for all Prove that S is an abelian group.

Solution:

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

=

=

$= y x (yx)^2$ from (3)

=

$= yx^3$

$= yx$ from (2)

$\forall$

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

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 show that xy = yx $\forall \; x \in N, \; \forall \; y \in M.$

Q.19. If H is a normal cyclic subgroup 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 (*i.e.* $H \trianglelefteq K \trianglelefteq G \not\Rightarrow H \trianglelefteq G$)

Q.21. Show that S_n is generated by (12) and (1, 2, 3, ----------, 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)

(3) (12) (13) (15) (25).

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 matric over R of the form

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.

Solution:

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

To show

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

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

Example 11.

Let H be a subgroup of a group G, let

Prove that

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

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

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

(iv)

Solution:

(i) Let $g_1,\ g_2 \in N(H)$

To show

Now $\left(g_1g_2^{-1}\right)H\left(g_1g_2^{-1}\right)^{-1} = \left(g_1g_2^{-1}\right)H\left(g_2g_1^{-1}\right) = g_1\left(g_2^{-1}Hg_2\right)g_1^{-1}$

$= g_1Hg_1^{-1} = H \Rightarrow g_1g_2^{-1} \in N(H)$

Hence N(H) is a subgroup of G.

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

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

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

$\Rightarrow H \trianglelefteq N(H)$

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

(1)

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

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

Example 12

Given any group of G. *Let* $\langle U \rangle$ 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 $U = \{xyx^{-1}y^{-1} | x, y \in G\}$, 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 for , 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 $\{a_i | i \in I\}$ that generates G, then G is finitely generated.

Remark :

If G is abelian, then could be simplified to $(a_1)^4(a_2)^5$, 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 $\bar{U} \trianglelefteq G$

Θ is the *subgroup generated* by U.

= {all finite products of integral powers of in U}

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

$$g^{-1} = g_{u_1}^{n_1} g^{-1} \ g_{u_2}^{n_2} g^{-1} \ g.......g_{u_k}^{n_k} g^{-1}$$

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

because

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

$\Rightarrow$ $\bar{U} \trianglelefteq G$ (i.e. $G' \trianglelefteq G$)

(ii) $U = \left\{ xy_x^{-1} \ {}_y^{-1} \,\middle|\, x, y \in G \right\}$

= {all finite products of integral powers of element in U}

The **Commutator subgroup** of G

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

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

We must show $xG'yG' =$

i.e. =

L.H.S.

= = (Θ is a commutator and so $y^{-1}x^{-1}yxG' = G'$)

= $(xyy^{-1}x^{-1})yxG' = yxG'$

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

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

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

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

Conversely, if , then

$xNyN = xyN =$ (Θ)

$= (xyy^{-1}x^{-1})yxN = eyxN$

$= yxN = yNxN$

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

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

$\therefore$

Example 13

Final order of

1. (15 27) (284) in

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 $\alpha = (a_1 a_2 a_3 .... a_s)$ be a cycle and let π be a permutation in . Then π is the cycle (π π)..........π .

Example 15

Compute aba^{-1}, Where

(i) $a = (135)\ (12),\ b = (1579)$

(ii) $a = (579),\ b = (123)$

Solution

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

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

$= (2179)$

(ii) $= (a(1)a(2)a(3))$, 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 $x \in S, a \in R \quad xa \in S$,

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 $ax = \quad xa \in S$.

****** 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,

$$a \in R, x \in S_1 \Rightarrow ax \in S_1$$
$$a \in R, x \in S_2 \Rightarrow ax \in S_2$$
$$\Rightarrow ax \in S_1 \cap S_2$$
$$\Rightarrow S_1 \cap S_2 \text{ is a left ideal.}$$

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

Proof. Let $a, b \in K(T)$. Then

$$T(a) = T(b) = 0.$$

Therefore,

$$T(a+b) = T(a) + T(b) = 0 + 0 = 0 \quad \text{(by ring}$$
$$T(ab) = T(a).T(b) = 0.0 = 0 \quad \text{homomorphism)}$$

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 $ar, ra \in K(T)$

$$T(ar) = T(a).T(r)$$
$$= 0 . T(r) \qquad (\Theta\ a \in K(T) \Rightarrow T(a) = 0)$$
$$= 0$$

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

$$S \subseteq F \qquad \text{(i)}$$

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

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

$$p+q = x_1a + x_2a = (x_1+x_2)\, a \in S. \qquad (\because x_1+x_2 \in R)$$

Similarly

$$-p = -x_1a = (-x_1)a \in S.$$

Therefore, S is an additive subgroup of R.

Moreover, if $r \in R$, then

$$rp = r(x_1a) = (rx_1)a \in S$$

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

Hence S is an ideal of R. But by supposition

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

$$1 \in R \Rightarrow a \in S \qquad (\because 1.a \in S),$$

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 :

$$\left.\begin{aligned} (r+A) + (s+A) &= (r+s) + A \\ (r+A)(s+A) &= rs+A \end{aligned}\right\} \quad \text{for all } r, s \in R.$$

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

$$\left.\begin{aligned} r+A &= r_1+A \\ s+A &= s_1+A \end{aligned}\right\} \quad r_1, s_1 \in R$$

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

$$\begin{aligned}[(r+A) + (s+A)] + (t+A) &= [(r+s)+A] + (t+A)\\ &= [(r+s)+t]+A\\ &= [r+(s+t)]+A\\ &= (r+A) + [(s+t)+A]\\ &= (r+A) + [(s+A) + (t+A)] .\end{aligned}$$

(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

$$\begin{aligned}(r+A) + (-r+A) &= [r+(-r)] + A\\ &= 0+A = A\end{aligned}$$

and

$$\begin{aligned}(-r+A) + (r+A) &= [(-r) + r] + A\\ &= 0+A = A\end{aligned}$$

which shows that $-r+A$ is the inverse of $r+A$.

(iv) Commutativity of addition :- If $r+A, s+A \in R/A$, then

$$\begin{aligned}(r+A) + (s+A) &= (r+s) + A\\ &= (s+r) + A\\ &= (s+A) + (r+A)\end{aligned}$$

(v) Associativity of multiplication :- If $r+A, s+A, t+A \in R/A$, then

$$\begin{aligned}[(r+A)(s+A)](t+A) &= (rs+A)(t+A)\\ &= (rs)t + A\\ &= r(st) + A\\ &= (r+A)(st+A)\\ &= (r+A)[(s+A)(t+A)] .\end{aligned}$$

(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

$r+A,\ s+A \in R/A$, then by the commutativity of R, we have

$$\begin{aligned}(r+A)\,(s+A) &= rs+A\\ &= sr+A\\ &= (s+A)\,(r+A)\end{aligned}$$

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 $\phi : R \to R/A$ be a mapping defined by $\phi(r) = r+A$. This mapping is known as natural mapping. If $r, s \in R$, then

$$\begin{aligned}\phi(r+s) &= (r+s) +A\\ &= (r+A) + (s+A)\\ &= \phi(r) + \phi(s)\end{aligned}$$

and

$$\begin{aligned}\phi(rs) &= rs+A\\ &= (r+A)\,(s+A)\\ &= \phi(r)\,\phi(s)\end{aligned}$$

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

$$\begin{aligned}K(\phi) &= \{r \mid r \in R,\ \phi(r) = A\}\\ &= \{r \mid r\in R,\ r+A = A\}\\ &= \{r \mid r \in R\}\\ &= A\end{aligned}$$

which proves the required result.

Theorem. Let $\phi : R \to S$ be a ring homomorphism of R onto S. Then

$$R/K(\phi) \simeq S\ .$$

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

$$\begin{aligned}\phi(r+x) &= \phi(r) + \phi(x) && \text{for all } x \in K(\phi)\\ &= \phi(r) + 0 && (\Theta\ x \in K(\phi) \Rightarrow \phi(x) = 0\ )\\ &= \phi(r)\end{aligned}$$

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

$$\begin{aligned}\psi\,[(r+K) + (s+K)] &= \psi\,[(r+s) + K]\\ &= \phi(r+s)\\ &= \phi(r) + \phi(s)\end{aligned}$$

$= \psi(r+K) + \psi(s+K)$

and

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

Therefore ψ is a ring homomorphism.

If $x \in S$, then

$$x = \phi(r),\ r \in R \quad (\Theta\ \phi \text{ is onto mapping})$$

$$= \psi\,(r+K)$$

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

Moreover,

$$\psi(r+K) = \psi\,(s+K) \quad \Rightarrow \phi(r) = \phi(s)$$
$$\Rightarrow \phi(r-s) = 0$$
$$\Rightarrow r-s \in K(\phi)$$
$$\Rightarrow r+K = s+K$$

Therefore ψ is one-to-one mapping also. Hence ψ is an isomorphism, as a consequence of which

$$R/K(\phi) \simeq S\,.$$

Theorem. A homomorphic image of a ring R is also a ring.

Proof. Let $T : R \to S$ be a ring homomorphism. Then homomorphic image of R is

$$Im(T) = \{x \mid x \in S,\ x = T(r), r \in R\}$$

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

$$x = T(r),\ y = T(s).$$

Therefore,

$$x+y = T(r) + T(s)$$
$$= T(r+s) \in Im(T) \qquad (\Theta\ T \text{ is a homomorphims})$$

and

$$xy = T(r)T(s)$$
$$= T(rs) \in Im(T).$$

Hence 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

$$\begin{aligned} rs \in P &\Rightarrow rs+P = P \\ &\Rightarrow (r+P)(s+P) = P \\ &\Rightarrow r+P = P \text{ or } s+P = P \qquad (\Theta\ R/P \text{ is without zero divisor}) \\ &\Rightarrow r \in P \text{ or } S \in P . \end{aligned}$$

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

$$rs+P = P$$

$$\Rightarrow rs \in P$$

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

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

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 Z/p**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 **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 $\in$ Z such that

$$y = mq + r,\ 0 \le r < m . \qquad \text{(i)}$$

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

Therefore,

$$y - mq = r$$

$$\Rightarrow \quad r \in I .$$

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

$$y = mq .$$

This implies that I = < m > . 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

$$M \subset M' \subset R \Rightarrow M' = R \text{ or } M' = M.$$

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 $q = 1 \Rightarrow (q) = (1) = R$ (Since R 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

$$M \subset N \subset R, \qquad M \neq N.$$

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

$$1 = ra + m$$
$$\Rightarrow b = r(ab) + mb, \ b \in R$$

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

$$rt + M = (r+M)(t+M) \in A^* \qquad \text{(because } A^* \text{ is an ideal of } R/M\text{)} .$$
$$\Rightarrow \quad rt \in A.$$

R being commutative tr also belongs to A.

Hence A is an ideal of R.

If $a \in M$, then

$$a+M = M \in R/M \qquad \text{(since M is the zero element of R/M)}$$
$$\Rightarrow \quad a+M \in A^* \qquad \text{(since } (1+M)(a+m) \in A^* ,$$
$$\Rightarrow \quad a \in A \qquad A^* \text{ being ideal of } R/M)$$

Therefore

$$M \subset A \subset R .$$

Let us suppose that $A^* \neq \{0\}$ then there exists an element r+M of A* such that

$$r + M \neq M$$

But $r+M \in A^* \Rightarrow r \in A$,

$$r+M \neq M \Rightarrow r \notin M \Rightarrow A \neq M.$$

Thus we have proved that if $A^* \neq \{0\}$, then

$$M \subset A \subset R$$

Since M is maximal therefore, A = R. If $r \in R$ then $r \in A$ which implies that $r + M \in A^*$. 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 $A^* = M$ $\qquad$ (Θ M is zero element of R/M)

Therefore,

$$\begin{aligned} A &= \{r \mid r + M \in A^*\} \\ &= \{r \mid r+M = M\} \\ &= \{r \mid r \in M\} \\ &= M \end{aligned}$$

If $A^* = R/M$ then

$$\begin{aligned} A &= \{r \mid r + M \in R/M\} \\ &= \{r \mid r \in M\} \\ &= R . \end{aligned}$$

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

$$S = \mathbf{Z} \times R = \{(m,a) \mid m \in Z, \ a \in R\}.$$

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)

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

(by Associativity of R and Z)

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

(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)

$$(m,a) + (n,b) = (m+n, a+b)$$
$$= (n+m, b+a) \qquad \text{(by commutativity of R and Z)}$$
$$= (n,b) + (m,a)$$

(v)

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

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

$$(m,a)(p,c) + (n,b)(p,c) = (mp, pa + mc + ac) + (np, pb + nc + bc)$$
$$= (mp + np, pa + mc + ac + pb + nc + bc)$$

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

$$f : R \to T$$

by

$$f(a) = (0,a), \quad a \in R$$

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

$$R = \{((a,b), (c,d)) \mid (a,b), (c,d) \in S \text{ and } ad = bc\}$$

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

$$ad = bc$$
$$\Rightarrow \quad cb = da \qquad \text{(by commutativity of D)}$$
$$\Rightarrow \quad ((c,d), (a,b)) \in R .$$

(ii) **Transitivity**. If $((a,b), (c,d)) \in R$, $((c, d), (e,f)) \in R$ then $ad = bc$ and $cf = de$

Therefore

$$adf = bcf = bde$$
$$\Rightarrow \quad (af - be)d = 0$$
$$\Rightarrow \quad (af - be) = 0 \qquad (\Theta\ d \neq 0)$$
$$\Rightarrow \quad af = be$$
$$\Rightarrow \quad ((a,b), (e,f)) \in R .$$

We represent the equivalence class of (a,b) by the fraction $\frac{a}{b}$. Thus

$$\frac{a}{b} = \{(c,d) \mid (c,d) \in S, \quad ((a,b), (c,d)) \in R\}$$

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

$$\frac{a}{b} = \frac{a_1}{b_1}, \quad \frac{c}{d} = \frac{c_1}{d_1} \qquad \text{(i)}$$

then

$$\frac{ad+bc}{bd} = \frac{a_1d_1+b_1c_1}{b_1d_1}$$

that is

$$a(d+bc)\,(b_1d_1) = bd(a_1d_1 + b_1c_1)$$

Now $(ad + bc)(b_1d_1) = adb_1d_1 + bcb_1d_1$

$= a(db_1)d_1 + b(cb_1)d_1$

$= ab_1dd_1 + bb_1cd_1$ (by commutativity of D)

$= ba_1dd_1 + bb_1c_1d$ (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

$$\begin{aligned} acb_1d_1 &= ab_1cd_1 \\ &= ba_1dc_1 \\ &= bda_1c_1 \end{aligned}$$

$\therefore$ 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

$$\frac{a}{b} + \left(\frac{c}{d}+\frac{e}{f}\right) = \frac{a}{b} + \frac{cf+de}{df}$$

$$= \frac{adf+bcf+bde}{bdf}$$

Therefore

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

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

Similarly $\frac{a}{b} + \frac{0}{b} = \frac{a}{b}$

Therefore $\frac{0}{b}$ is additive identity.

(iii) $\frac{a}{b} + \left(\frac{-a}{b}\right) = \frac{ab-ab}{b^2} = \frac{0}{b^2} = \frac{0}{b} = -\frac{a}{b} + \frac{a}{b}$

Thus every element of F is invertible.

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

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

(v) If $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in F$, then

$$\left(\frac{a}{b}.\frac{c}{d}\right).\frac{e}{f} = \frac{ace}{bdf} = \frac{a}{b}\left(\frac{c}{d}.\frac{e}{f}\right)$$

(vi) $\frac{a}{b}\left(\frac{c}{d}+\frac{e}{f}\right) = \frac{a}{b}.\left(\frac{cf+de}{df}\right)$

$$= \frac{acf}{bdf} + \frac{ade}{bdf}$$

$$= \frac{ac}{bd} + \frac{ae}{bf}.$$

Similarly it can be shown that

$$\left(\frac{a}{b}+\frac{c}{d}\right).\frac{e}{f} = \frac{ae}{bf} + \frac{ce}{df}$$

(vii)

$$\left(\frac{a}{b}\right)\left(\frac{a}{a}\right) = \left(\frac{aa}{ba}\right) = \frac{a}{b}$$

and $\frac{a}{a}.\frac{a}{b} = \frac{a}{b}$.

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 a 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 $f : Z \to K$ defined by $f(n) = ne$, $n \in \mathbf{Z}$ 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 homorphism. Then

$$A = \{n \mid f(n) = 0\}$$
$$= \{n \mid ne = 0\} \qquad \text{(i)}$$

and

$$Z/A \simeq \text{Im}(f) = f(z) .$$

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

If A = {0}, then

$$ne = 0 \Leftrightarrow n = 0 .$$

If A is a prime ideal then we can find a prime number p such that

$$A = \ker f = < p > \qquad \text{(ii)}$$

Hence from (i) and (ii)

$$ne = 0 \Leftrightarrow p \mid n .$$

Thus we have seen that if K is a field, then one of the following two cases, holds

(i) $ne = 0 \Leftrightarrow n = 0$

(ii) $ne = 0 \Leftrightarrow p \mid n$ where p 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 Z/A = Z and therefore $Z \simeq \text{Im}(f)$. Hence Im(f) and K are infinite

Example 1. The characteristic of the field Q of rational numbers is zero, since $ne = 0 \Rightarrow n = 0$ (Θ $e \neq 0$).

2. The characteristic of the field 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 **Z**/p**Z** is a prime field. Additive group **Z**/p**Z** . Hence **Z**/p**Z** is a prime field.

2. Field 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, $n \in K$, $n \neq 0 \Rightarrow \frac{1}{n} \in K$. Then $m \in K$, $\frac{1}{n} \in K \Rightarrow \frac{m}{n} \in K$. Hence K contains all rational numbers. Hence K = Q as a consequence of which Q is a prime field.

We have seen that the field Q of rational numbers and **Z**/p**Z** are prime fields. Now we shall prove that upto isomorphism there are only two prime fields Q and **Z**/p**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 $f : Z \to K$ defined by

$$f(n) = ne, \; n \in Z .$$

This mapping is a ring homomorphism. For,

$$f(n+m) = (n+m)e$$
$$= ne+me = f(n) + f(m)$$
$$f(nm) = (nm)e = (ne)(me) = f(n)f(m)$$

i.e. $A = \{n \mid f(n) = 0\}$

$= \{n \mid ne = 0\}$.

Let ker f = A. Since A is an ideal of Z and every ideal in Z is a principal ideal, therefore

$$A = \{0\} \text{ or } A = \langle p \rangle, \; p \neq 0 .$$

If ker f = A = {0}, then f is one-to-one. Hence f(Z) is a subring of K isomorphic to the integral domain **Z**. The prime field K, being now the quotient field of the integral domain f(z) is isomorphic to the quotient field of **Z.** But the quotient field of **Z** is the field Q of rational numbers. Hence K is isomorphic to Q.

If ker f = A = $\langle p \rangle$, $p \neq = 0$, then p is a prime number. If fact, if

$$p = mn, \; m \neq 1, n \neq 1$$

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

$$F(Z) \simeq \mathbf{Z}/p\mathbf{Z}$$

Since **Z**/p**Z** is a field, f(Z) is itself a field necessarily identical with K. Hence

$$K \simeq \mathbf{Z}/p\mathbf{Z}$$

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

$$a_n = b_n, \; n \in N$$

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

$$a_n = 0 \text{ for all } n \geq j \text{ and } b_n = 0 \text{ for all } n \geq k$$

then

$$a_n + b_n = 0 \text{ for all } n \geq \max(j, k)$$

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

$$(a_0, a_1, a_2, \ldots, a_n, \ldots) + (b_0, b_1, b_2, \ldots, b_n, \ldots) = (a_0 + b_0, a_1+b_1, \ldots, a_n+b_n, \ldots).$$

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

$$c_0 = a_0b_0$$
$$c_1 = a_0b_1 + a_1b_0$$
$$c_2 = a_0b_2 + a_1b_1 + a_2b_0$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$c_n = a_0b_n + a_1b_{n-1} + \ldots + a_nb_0 = \sum_{m=0}^{n} a_m b_{n-m}$$

If $a_n = 0$ for all $n \geq j$ and $b_n = 0$ for all $n \geq k$, then

$$c_n = 0 \quad \text{for all} \quad n \geq (j+k).$$

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) $$\begin{aligned}(a_0, a_1, a_2,\ldots) + [(b_0, b_1, b_2,\ldots) + (c_0, c_1, c_2,\ldots)] &= (a_0, a_1, a_2,\ldots) + [(b_0 + c_0, b_1+c_1, b_2+c_2,\ldots) \\ &= (a_0+b_0+c_0, a_1+b_1+c_1, a_2+b_2+c_2,\ldots) \\ &= (a_0+b_0, a_1+b_1, a_2+b_2,\ldots) + (c_0, c_1, c_2,\ldots) \\ &= [(a_0, a_1, a_2,\ldots) + (b_0, b_1, b_2,\ldots)] + (c_0, c_1, c_2,\ldots)\end{aligned}$$

(ii) $$\begin{aligned}(a_0, a_1, a_2,\ldots) + (0, 0, 0, \ldots) &= (a_0 + 0, a_1+ 0, a_2 + 0, \ldots) \\ &= (a_0, a_1, a_2,\ldots)\end{aligned}$$

and

$$\begin{aligned}(0, 0, 0,\ldots) + (a_0, a_1, a_2,\ldots) &= (0 + a_0, 0 + a_1, 0 + a_2,\ldots) \\ &= (a_0, a_1, a_2,\ldots)\end{aligned}$$

(iii) $$\begin{aligned}(a_0, a_1, a_2,\ldots) + (-a_0, -a_1, -a_2,\ldots) &= (a_0 - a_0, a_1-a_1, a_2-a_2,\ldots) \\ &= (0, 0, 0, \ldots)\end{aligned}$$

and

$$\begin{aligned}(-a_0, -a_1, -a_2,\ldots) + (a_0, a_1, a_2,\ldots) &= (0, 0, 0,\ldots)\end{aligned}$$

(iv) $$\begin{aligned}(a_0, a_1, a_2,\ldots) + (b_0, b_1, b_2,\ldots) &= (a_0 + b_0, a_1+b_1, a_2+b_2,\ldots) \\ &= (b_0 + a_0, b_1+a_1, b_2+a_2,\ldots) \\ &= (b_0, b_1, b_2,\ldots) + (a_0, a_1, a_2,\ldots)\end{aligned}$$

(v) $$\begin{aligned}[(a_0, a_1, a_2,\ldots) (b_0, b_1, b_2,\ldots)] (c_0, c_1, c_2,\ldots) &= (d_0, d_1, d_2,\ldots) (c_0, c_1, c_2,\ldots)\end{aligned}$$

where

$$d_n = \sum_{j+k=n} a_j b_k$$

$$= (e_0, e_1, e_2,\ldots)$$

where

$$\begin{aligned}e_m &= \sum_{p+q=m} d_p c_q \\ &= \sum_{p+q=m} \left(\sum_{j+k=p} a_j b_k \right) c_q \\ &= \sum_{j+k+q=m} a_j b_k c_q .\end{aligned}$$

Similarly, it can be shown that

$(a_0, a_1, a_2,\ldots.)\ [(b_0, b_1, b_2,\ldots.)\ (c_0, c_1, c_2,\ldots.)] = (f_0, f_1, f_2,\ldots)$

where

$$f_m = \sum_{j+k+q=m} a_j b_k c_q \ .$$

Hence

$$[(a_0, a_1, a_2,\ldots)\ (b_0, b_1,..)\ ]\ (c_0, c_1, c_2,\ldots.)$$
$$= (a_0, a_1, a_2,\ldots)\ [(b_0, b_1, b_2,..)\ (c_0, c_1, c_2,..)]$$

(vi) $(a_0, a_1, a_2,\ldots)\ [(b_0, b_1, b_2,\ldots) + (c_0, c_1, c_2,\ldots)]$

$$= (a_0, a_1, a_2,\ldots)\ (b_0 + c_0, b_1 + c_1, b_2 + c_2,\ldots.)$$
$$= (d_0, d_1, d_2,\ldots)$$

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

$(a_0, a_1, a_2,\ldots)\ (b_0, b_1, b_n\ ) = (f_0, f_1, f_2,\ldots.)$,

$(a_0, a_1, a_2,\ldots)\ (c_0, c_1, c_2,\ldots) = (g_0, g_1, g_2,\ldots)$

Hence

$(a_0, a_1, a_2,\ldots)\ [(b_0, b_1, b_2,\ldots) + (c_0, c_1, c_2,\ldots)]$

$= (a_0, a_1, a_2,\ldots)\ (b_0, b_1, b_2,\ldots) + (a_0, a_1, a_2,\ldots.)\ (c_0, c_1,\ldots)$

Hence P is a ring. We call this ring of polynomials as polynomial ring over R and it is denoted by R[x].

Let

$$Q = \{(a, 0, 0,\ldots) \mid a \in R\}$$

Then a mapping $f : R \to Q$ defined by $f(a) = (a, 0, 0,\ldots)$ is an isomorphism. In fact,

$$\begin{aligned} f(a+b) &= (a + b, 0, 0,\ldots) \\ &= (a, 0, 0, \ldots) + (b, 0, 0,\ldots) \\ &= f(a) + f(b), \\ f(ab) &= (ab, 0, 0, \ldots.) \\ &= (a, 0, 0, \ldots)\ (b, 0, 0, \ldots) \\ &= f(a)\ f(b) \end{aligned}$$

and

$$\begin{aligned} f(a) &= f(b) \Rightarrow (a, 0, 0,\ldots) = (b, 0, 0, \ldots.) \\ &\Rightarrow a = b\ . \end{aligned}$$

Hence

$$R \simeq Q \qquad\qquad (i)$$

So we can identify the polynomial $(a, 0, 0, \ldots)$ with a.

If we represent $(0, 1, 0, \ldots)$ by x then we can see that

$$x^2 = (0, 0, 1, 0, \ldots)$$

$$x^3 = (0, 0, 0, 1, \ldots)$$
$$\ldots\ldots\ldots\ldots$$
$$\ldots\ldots\ldots\ldots$$
$$x^n = (\underbrace{0, 0, 0, \ldots, 0}_{n \text{ terms}}\ 1, 0, \ldots.)$$

Therefore for $(a, 0, 0, \ldots.) \in Q$ we have

$$\left.\begin{array}{l} (a, 0, 0, \ldots)\, x = (0, a, 0, \ldots..) \\ (a, 0, 0, \ldots)\, x^2 = (0, 0, a, \ldots.) \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ (a, 0, 0, \ldots.)\, x^n = (\underbrace{0, 0, 0, \ldots, 0}_{n \text{ terms}}, a, 0, \ldots.) \end{array}\right\} \qquad \text{(ii)}$$

If $(a_0, a_1, .., a_n, 0, \ldots)$ be any arbitrary element of the polynomial ring P, then by (ii) we have

$$(a_0, a_1, a_2, \ldots., a_n, 0, \ldots) = (a_0, 0, \ldots.) + (0, a_1, \ldots) + \ldots + (\underbrace{0, 0, 0, \ldots, 0}_{n \text{ terms}}, a_n, 0, \ldots.)$$
$$= (a_0, 0, \ldots) + (a_1, 0, \ldots.)(0, 1, 0, \ldots) + \ldots.$$
$$+ (a_n, 0, 0, \ldots)\,((\underbrace{0, 0, 0, \ldots, 0, 0}_{n \text{ terms}}, 1, 0, \ldots)$$
$$= (a_0, 0, \ldots) + (a_1, 0, 0, \ldots)\, x + \ldots + (a_n, 0, 0, \ldots)\, x^n$$
$$= a_0 + a_1 x + a_n x^n \qquad \text{(by (i))}$$

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

$$f(x) = a_0 + a_1 x + a_2 x^2 + \ldots a_m x^m , \ a_m \neq 0$$

and

$$g(x) = b_0 + b_1 x + \ldots b_n x^n, b_n \neq 0$$

are two elements of R[x], then

$$\deg f(x) = m \text{ and } \deg g(x) = n \text{ and}$$
$$f(x) + g(x) = (a_0 + a_1 x + a_2 x^2 + \ldots + a_m x^m) + (b_0 + b_1 x + b_2 x^2 + \ldots + b_n x^n)$$

If $m = n$ and $a_m + b_n \neq 0$, 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

$$f(x) + g(x) = (a_0 + b_0) + (a_1+b_1)x + \dots + (a_n+b_n)x^n + a_{n+1} x^{n+1} + \dots + a_m x^m$$

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 ,

$$f(x)\, g(x) = a_0b_0 + (a_0b_1 + a_1b_0)x + \dots + a_mb_nx^{m+n}$$

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

$$\deg f(x) \leq \deg [f(x)\, g(x)] \qquad (\Theta \deg g(x) \geq 0).$$

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

$$f(x) = \sum_{i=0}^{m} a_i x^i , \quad a_m \neq 0$$

and

$$g(x) = \sum_{i=0}^{n} b_i x^i , \quad b_n \neq 0 ,$$

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

$$f(x) = \sum_{i=0}^{m} a_i x^i, \quad a_m \neq 0$$

$$g(x) = \sum_{i=0}^{n} b_i x^i, \; b_n \neq 0 \; .$$

Then either

(i) $\deg f(x) < \deg g(x)$

or

(ii) $\deg f(x) \geq \deg g(x)$

In the first case we write

$$f(x) = g(x)\,0 + f(x)$$

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

$$h(x) = f(x) - \left(\frac{a_m}{b_n}\right) x^{m-n}\, g(x) \qquad \text{(iii)}$$

$$\begin{aligned} f(x) &= a_0 + a_1x + \ldots + a_mx^m \\ &= a_m\, b_n^{-1}\, x^{m-n}\, (b_0 + b_1x + \ldots\, b_nx^n) \\ &\quad + (a_{m-1} - a_m\, b_n^{-1}\, b_{n-1})\, x^{m-1} + (a_{m-2} - a_m b_n^{-1}\, b_{n-2}\,)\, x^{m-2} \\ &= a_m\, b_n^{-1}\, x^{m-n}\, g(x) + h(x) \end{aligned}$$

then $\deg h(x) \leq m-1$.

Hence by supposition

$$h(x) = g(x)\, q_1(x) + r(x)\,, \qquad \text{(iv)}$$

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,

$$\begin{aligned} f(x) &= g(x)\, [q_1(x) + \left(\frac{a_m}{b_n}\right) x^{m-n}] + r(x) \\ &= g(x)\, q(x) + r(x) \end{aligned}$$

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

$$g(x)\, q(x) + r(x) = g(x)\, q_1(x) + r_1(x)\ ,$$

that is,

$$g(x)\, [\, q(x) - q_1(x)] = r_1(x) - r(x) \qquad \text{(v)}$$

But $\quad \deg g(x)\, [q(x) - q_1(x)] \ \geq n$

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

$$\deg f(x) + \deg g(x) = \deg q = 0 \qquad \text{(i)}$$
$$\deg f(x) + \deg h(x) = \deg x = 1 \qquad \text{(ii)}$$

From (ii) we get

$$\deg f(x) = 0 \text{ and } \deg g(x) = 0$$

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

$$f(x) = 1,\ g(x) = 2$$
$$f(x) = -1,\ g(x) = -2$$
$$f(x) = 2,\ g(x) = 1$$
$$f(x) = -2,\ g(x) = -1 .$$

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

$$a = 1.a \quad \text{for all } a \in D$$
$$\Rightarrow\ 1 \mid a \quad \text{for all } a \in D .$$

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

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

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 $a \mid 1$, 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 $a \mid 1$ and $1 \mid a$ for every $a \in D$ showing that a is a unit.

For example each non-zero element of a field is a unit thereof.

± 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 (indecomposible) 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

$$a = p_1p_2p_3 \dots p_n,$$

where p_i's are irreducible elements.

Definition. A F.D. is called a unique factorisation domain if whenever

$$a = p_1p_2p_3\dots p_n = q_1q_2 \dots q_s$$

then r = s and after rearrangement, if necessary,

$$p_1 \sim q_1, p_2 \sim q_2\dots, p_r \sim q_s .$$

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

$$a = bc$$

$$\Rightarrow \quad a \in (b)$$

$$\Rightarrow \quad (a) \subset (b)\ ,\ (b) \neq (a)\ .$$

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

$$b = cd$$

$$\Rightarrow \quad b \in (c)$$

$$\Rightarrow \quad (b) \subset (c) \quad (b) \neq (c)$$

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 $a_1, a_2,\dots, a_n,\dots$ such that

$$(a_1) \subset (a_2) \subset (a_3) \dots \subset (a_n) \subset \dots . \text{ (I)}$$

no two of these principal ideals being the same.

Consider the union

$$A = U(a_i)$$

We assert that A is an ideal of D. In fact

$$0 \in (a_1) \Rightarrow 0 \in A$$

$$\Rightarrow A \neq \phi .$$

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 β 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

$$\beta \in (a_n) \text{ for all } n \geq m$$

$$\Rightarrow (\beta) \subset (a_n) \text{ for all } n \geq m \qquad \text{(II)}$$

Also since (β) is the union of the ideals, we have

$$(\beta) \supset (a_n) \quad \text{for all } n \qquad \text{(III)}$$

Thus from (II) and (III)

$$(\beta) = (a_n) \text{ for all } n \geq m,$$

$$\Rightarrow \quad (a_m) = (a_{m+1}) = (a_{m+2}) = \ldots.$$

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

$$a = p_1p_2 \ldots p_r = q_1q_2\ldots q_s \qquad \text{(IV)}$$

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 $p_1p_2\ldots p_n \in (p_1)$

which implies $q_1q_2\ldots. q_s \in (p_1)$

Therefore one of the factors $q_1q_2\ldots. q_s$ 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

$$q_1 = e_1p_1 \qquad \text{(V)}$$

where e_1 is a unit.

From (IV) and (V) we have

$$p_2p_3 \ldots p_2 = (e_1q_2)\ q_3 \ldots q_s \qquad \text{(VI)}$$

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

$$\mathbf{p} = (p)$$

be an ideal of R generated by p.

Let $\mathbf{p} \underset{\neq}{\subset} Q$ 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 | a and so

$$a \in (p) = \mathbf{p}$$
$$\Rightarrow\ (a) \subseteq \mathbf{p}$$
$$\Rightarrow\ Q \subseteq \mathbf{p}$$

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 $bpy \in \mathbf{p} \subseteq Q$ and $bax \in Q$

$$\therefore\ b \in Q$$
$$\Rightarrow\quad R \subset Q$$

But Q being an ideal of R we have

$$Q \subset R .$$

Hence $\quad Q = R$

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 ϕ 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 ϕ 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 ϕ 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 ϕ 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 ϕ 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) is 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 $\{a_0, a_1, .., a_i, \ldots a_n\}$ 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 $3x^2 - 6x + 3$ 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

$$\begin{aligned} h(x) &= f(x)\, g(x) \\ &= c_0 + c_1x + c_2x^2\, x \ldots + c_{m+n}\, x^{m+n} \end{aligned}$$

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

$$c_{i+j} = a_ib_j + a_{i-1}\, b_{j+1} + a_{i-2}b_{j+2} + \ldots + a_0\, b_{i+j} + a_{i+1}\, b_{j-1} + a_{i+2}b_{j-2} + \ldots a_{i+j}\, b_0$$

$$\Rightarrow \; a_ib_j = c_{i+j} - (a_{i-1}\, b_{j+1} + a_{i-2}\, b_{j+2} + \ldots) - (a_{i+1}b_{j-1} + a_{i+2}\, b_{j-2} + \ldots)$$

Since p is a divisor of each of the terms on the right, we have

$$p \mid a_ib_j$$

$$\Rightarrow \; p \mid a_i \text{ or } p \mid b_j$$

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

$$f_1(x) = kf_2(x) \quad \text{where } 0 \neq k \in K$$

We have $k = gh^{-1}$ where $g \in D$, $h \in D$

$\therefore$ $hf_1(x) = gf_2(x)$

$\therefore$ $f_1(x) \sim f_2(x)$ in $D[x]$ (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

$$f(x) = c\, g(x)$$

$$f(x) = d\, h(x)$$

where g(x) and h(x) are primitive members of D[x].

We have therefore

$$cg(x) = dh(x)$$

$$\Rightarrow \quad cb_i = dc_i$$

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_1a_2. Also f(x) being irreducible in D[x] is primitive and the constant of the left hand side is b_1b_2. Therefore, $a_1a_2 = b_1b_2$. 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

$$a(x) = p_1 p_2 \ldots p_r\, a_1(x) \ldots a_s(x) = p_1' p_2' \ldots p_l'\, a_1'(x)\, a_2'(x) \ldots a_m'(x)$$

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 $p_1p_2\ \ldots\ p_r$. Therefore

$$p_1\ p_2\ldots\ p_r = p_1'p_2'\ \ldots\ p_l' \qquad (1)$$

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 $a_1'\ \ldots\ a_m'(x)$ 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].

Also, D being a u.f.d. we see from (i) that each p_i is associate of some p_i' and vice versa.

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

$$p \mid a_0\ ,\ p|a_1,\ldots,\ p \mid a_{n-1}$$

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,

$$a_0+a_1x + \dots a_nx^n = (b_0 + b_1x + \dots b_l x^l) (c_0 + c_1x + \dots c_m x^m)$$

where $l > 0$, $m > 0$.

We have

$$a_0 = b_0 c_0$$

Therefore $p \mid a_0 \Rightarrow p \mid b_0$ or $p \mid c_0$

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 $p \mid c_0$.

Also, we have

$$a_n = b_l c_m$$

implying that p is not a divisor of c_m .

Let $r \le m$ be the smallest index such that each of

$$c_0,\ c_1, \dots c_{r-1}$$

is divisible by p.

Also

$$a_r = b_0c_r + b_1c_{r-1} + \dots + b_r c_0$$

Since neither b_0 nor c_r is divisible by p, and each of

$$c_0, c_1, \dots, c_{r-1}$$

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

$$p \mid ab \Rightarrow p \mid a \quad \text{or } p \mid b.$$

Proof. Let

$$a = p_1p_2 \dots P_r$$
$$b = p_1'p_2' \dots p_s'$$

where each of $p_1, p_2, \dots, p_r$; p_1' p_2', …, p_s' is a prime element of D. Then we have

$$ab = p_1p_2 \dots p_r\, p'_1p'_2 \dots p_s' \qquad \text{(i)}$$

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 $p \mid a$ or $p \mid b$.

* 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 $p \mid ab \Rightarrow$ either $p \mid a$ or $p \mid b$.

The ring $Z[\sqrt{-5}\,]$ of numbers $a+b\sqrt{-5}$ where a and b are any integers is not a u.f.d. For,

$$9 = (2 + \sqrt{-5}\,)\,(2-\sqrt{-5}\,) = 3.3$$

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 $Z[\sqrt{-3}\,]$ is not a u.f.d. For,

$$12 = (3+\sqrt{-3})\,(3-\sqrt{-3}) = 3.4$$

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 ϕ 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

$$|p'-p| \le \frac{1}{2}, \quad |q'-q| \le \frac{1}{2}$$

We write

$$\lambda' = p' + iq'$$

so that λ' 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 α, β, λ' being Gaussian integers it follows that $(\lambda-\lambda')\beta$ is also Gaussian integer.

Here

$$\phi\{(\lambda-\lambda')\beta\} = \{(p'-p)^2 + (q'-q)^2\}\,\phi(\beta)$$
$$\le \left(\frac{1}{4}+\frac{1}{4}\right)\phi(\beta) < \phi(\beta)$$

Thus for every pair of Gaussian integers α, β there exist Gaussian integers λ' 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 $G = G_0 \Delta G_1 \Delta G_2 \Delta ---- \Delta G_r = (1)$

of a group G is called a **Composition series** of G if

(1) G_{i+1} 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 $\frac{S_5}{A_5} \cong Z_2$ is also simple, we see that $A_5 S_5 \Delta A_5 \Delta (1)$ 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

$S_4 \Delta A_4 \Delta V_4 \Delta E_4 \Delta (1)$, the composition peries of S_4.

$H_1 \Delta H_2 \Delta H_3 \Delta ---- \Delta H_r = (1)$

Recall $V_4 \equiv \{(1), (12)(34), (13)(24), (14)(23)\}$

is Klein's four group and

$E_4 = \{(1), (12)(34)\}$, Further

$$\left|\frac{S_4}{A_4}\right| = 2, \left|\frac{A_4}{V_4}\right| = 3, \left|\frac{V_4}{E_4}\right| = 2, \left|\frac{E_4}{(1)}\right| = 2 \text{ tells}$$

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 $G \; \Delta(1)$ 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

$G = G_0 \; \Delta H_1 \; \Delta H_2 \; \Delta ---- \Delta H_r = (1)$ is a composition series of G.

Note that infinite groups need **not** have composition series. We can consider infinite cyclic group Z.

As every non-trivial sub group of infinite cyclic group Z is isomorphic to Z; as Z is not simple, we see that Z has no simple subgroups. So we can not construct composition series of Z.

$Z \Delta 2Z \Delta 4Z \Delta 8Z \Delta 16Z \Delta$ ---------

We can not end to = (1).

Definition:

Let $G = G_0 \Delta G_1 \Delta G_2 \Delta ---- \Delta G_r = (1)$ be a composition series and suppose that $G = H_0 \Delta H_1 \Delta ---- \Delta H_r = (1)$

is another composition series of the **same** length r. We say that these series are **equivalent** if $\exists$ some 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 $G_1 = \langle x^2 \rangle$. and $H_1 = \langle x^3 \rangle$

We have two composition series:

$G \Delta G_1 \Delta G_2 = (1)$ and

$G \Delta H_1 \Delta H_2 = (1)$

These two series are **equivalent,** as

$G/G_1 \cong H_1/(1) \cong Z_2$ and

$G_1/(1) \cong G/H_1 \cong Z_3$

$$G/G_1 = \frac{\langle x \rangle}{\langle x^2 \rangle}, \left|G/G_1\right| = 2, G/H_1 = \frac{\langle x \rangle}{\langle x^3 \rangle}, \left|\frac{G}{H_1}\right| = 3$$

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 $G = G_0 > G_1 > ----> G_r = (1)$

and $G = H_0 > H_1 > ----> H_s = (1)$

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 is simple, so $G_1 \not\trianglelefteq H_1$, hence

and so because G/H_1 is simple.

Let $K = G_1 \cap H_1 \trianglelefteq G$. Now

$$\frac{G}{G_1} = \frac{G_1 H_1}{G_1} \cong \frac{H_1}{G_1 \cap H_1} = \frac{H_1}{K} \text{ and}$$

$$\frac{G}{H_1} = \frac{G_1\ H_1}{H_1} \cong \frac{G_1}{G_1 \cap H_1} = \frac{G_1}{K}$$

$\Theta\ K \trianglelefteq G$ and G has a composition series,

K has a composition series, say

$K_1 \ldots K_t \ldots = (1)$

G_1 now have two composition series

$G_1\ \Delta G_2\ \Delta G_3\ \Delta ---- \Delta G_r = (1)$ and

$G_1\ \Delta K\ \Delta K_1\ \Delta K_2\ \Delta ---- \Delta K_t = (1)$.

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:

$H_1\ \Delta H_2\ \Delta ---- \Delta H_s = (1)$ and

$H_1\ \Delta K\ \Delta K_1\ \Delta K_2\ \Delta ---- K_{r-2} = (1)$ $(\Theta\ t = r - 2)$

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 $G = H_0\ \Delta H_1\ \Delta K\ \Delta K_1\ \Delta ---- \Delta K_{s-2} = (1)$

are equivalent, because we have proved above

$G/G_1 \cong H_1/K$ and

.

Hence we finally conclude that our two initial composition series of B are equivalent.

Definition:

A series of sub groups

$G = G_0 \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq ---- \trianglerighteq G_s = (1)$ of group G is called a **subnormal** series of G if $G_{i+1} \trianglelefteq G_i$ 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 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_1 is the set of all possible products of the form $[a_1, b_1]$ ---- $[a_r, b_r]$, where $a_i, b_i \in G$, and r is a natural number. From

which, as a consequence, implies that $G^1 \trianglelefteq G$.

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

is abelian

From $[a, b]^2 = [a^g, b^g]$, 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 subgroups

(Here $G^{(0)} = G, G^{(1)} = G', G^{(2)} = G'', ----$)

Definition:

If for some k, we have $G^{(k)} = (1)$, then G is called **solvable** (Also soluble). Note that in the case of = A_n, n $\geq$ 5, all members of above sequence coincide. i.e. A_n, n 5 not soluable.

From unit I, we see that S_4, S_3 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 , then G is solvable N and ar solvable groups.
4. A_n group of p^m, where p is a prime number, is solvable.
5. If G and H are solvable, then G×H is solvable.

Proof:

$\Delta G^{(k)} \ \Delta ----$

1. for all k, and $G^{(k)} = (1)$ for some k, as G is solvable, $\therefore$ H is solvable.
2. Let ϕ: G 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 are solvable, so we get subnormal series

   and

$$G/N = G_0/N \trianglerighteq G_1/N \trianglerighteq ---- \trianglerighteq G_s/N = (1) \text{ such that } N_i/N_{i+1} \text{ and } \frac{(G_i/N)}{(G_{i+1}/N)} \cong G_i/G_{i+1}$$

are abelian $\forall\ i$. Now we get

$$G = G_0 \trianglerighteq G_1 \trianglerighteq ---- \trianglerighteq G_2 = N = N_0 \trianglerighteq N_1 \trianglerighteq ---- \trianglerighteq N_2 = (1)$$

is a subnormal series of G having abelian successive quotients. Hence G is solvable.

or

We can use

$$\left(G/N\right)^{(k)} \subset G^{(k)}N/N$$

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 thorem, 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 $G = G_0 \trianglerighteq G_1 \trianglerighteq ---- \trianglerighteq G_r = (1)$ of a group G is called a **central series** of G if, for each i, G/G_{i+1} is contained in the center of G/G_{i+1} i.e.

$$\frac{G_i}{G_{i+1}} \le Z\left(G/G_{i+1}\right) \forall\, i$$

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 $S_i, i = 3, 4, i.e.\ Z(S_i) = (1)$.

$$\therefore \frac{G_i}{G_{i+1}} \subseteq Z\left(G/G_{i+1}\right) \text{ does not hold } \forall\, i,$$

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 $G_i/G_{i+1} \subseteq Z\left(G/G_{i+1}\right)$ is equivalent to the Commutator condition that

   $\left[G_{i+1}x, G_{i+1}g\right] = G_{i+1} \;\forall\, x \in G_i$ and $\forall\, g \in G$.

$\left(G_{i+1}x \in G_i/G_{i+1}\right)$ for any $x \in G_i$, $\dfrac{G_i}{G_{i+1}} \subseteq Z\left(\dfrac{G}{G_{i+1}}\right)$

$$\Rightarrow (G_{i+1}x)(G_{i+1}g) = (G_{i+1}g)(G_{i+1}x) \; \forall \; g \in G$$

$$\Rightarrow [G_{i+1}x,\, G_{i+1}g] = G_{i+1},\; \forall\; x \in G_i,\; \forall\; x \in G.$$

However,

$$G_{i+1}x\; G_{i+1}g\; G_{i+1}x^{-1}\; G_{i+1}g^{-1} = G_{i+1}\,[x,\, g]$$

So the condition can be restated as

$$[x,\, g] \in G_{i+1} \;\; \forall\; i,\; \forall\; x \in G_i \;and\; \forall\; g \in G.$$

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 O.
2. Non-trivial abelian groups hare nilpotency class 1.

Theorem 6 : Nilpotent group are solvable.

Proof : Let G be a nilpotent group. So it has a central servies, which is a normal series with abelian successive quotients and hence G is solvable.

Converse is not true. There are solavble 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 ha non-trival center), by P/Z has a central series.

We get easily that the series

$$P = P_o \trianglerighteq P_1 \trianglerighteq P_2 \trianglerighteq ---- \trianglerighteq P_r = Z \trianglerighteq (1)$$

a central series of P.

Theorem 8 : Let G be a nilpotent group and suppose that $H<G$ is a propersubgroup of G. Then the normalzer of H in G is strictly larger than H i.e.

A niloptent group has no proper self-normlizing subgroups.

Proof : Let

be a Central Serie sof the nilpotent group G. Let \ and let k be such that G_{k+1} and $\nleq$ h such a k exists since $G_r=(1)$ Now

Let $x \in G_k$ *and* $g \in G$

Since $G_k / G_{k+1} \leq Z(G/G_{k+1})$, we get

Hence $[G_k, G] \leq G_{k+1}$ *and so* $[G_{k}, H] \leq H$

We now get that $G_k \leq N_g(H)$. But $G_k \not\leq H$

Hence we must have $H \lneq N_G(H)$

Corollary : Every maximal subgroup of nil potent *G* is normal in *G*.

Proof : Let *H* be a maximal subgroup of *G*. Since \ , by hypothesis we must have and hence $H \trianglelefteq G$

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 Z under addition:

1. $\{0\} \trianglelefteq 8Z \trianglelefteq 4Z \trianglelefteq Z$

2. $\{0\} \trianglelefteq 9Z \trianglelefteq Z$

Examples 2:

$$\{0\} \trianglelefteq 72Z \trianglelefteq 8Z \trianglelefteq Z$$

can be refined to a series

$\{0\} \trianglelefteq 72 \trianglelefteq 24Z \trianglelefteq 8Z \trianglelefteq 4Z \trianglelefteq$

Note that two new terms, 24Z and 4Z have been insertd.

Example 3 :

We consider two series of Z_{15} :

$$\{0\} \trianglelefteq \langle 5 \rangle \trianglelefteq Z_{15}$$

and $\{0\} \trianglelefteq \langle 3 \rangle \trianglelefteq Z_{15}$

These series are isomorphic

We see that $Z_{15}/\langle 5 \rangle \cong Z_5 \cong \langle 3 \rangle / \{0\}$ *and*

$Z_{15}/\langle 3 \rangle \cong Z_3 \cong \langle 5 \rangle / \{0\}$

Example 4 :

We now find isomorphic refinements of the series given in Example 1

i.e. (1)

$\{0\} \trianglelefteq 9Z \trianglelefteq Z$ (2)

we write the refinement

$$\{0\} \trianglelefteq 72Z \trianglelefteq 8Z \trianglelefteq 4Z \trianglelefteq Z \qquad (3)$$

of (1) and the refinement

$$\{0\} \trianglelefteq 72Z \trianglelefteq 18Z \trianglelefteq 9Z \trianglelefteq Z \qquad (4)$$

of (2)

Both refinements have four factor groups :

3. has $\frac{Z}{4Z} \cong Z_4, \frac{4Z}{8Z} \cong Z_2, \frac{8Z}{72Z} \cong Z_9$

$$\frac{72z}{\{0\}} \cong 72Z \text{ or } Z$$

4. has $\frac{Z}{9Z} \cong Z_9 \Big/ 9\ \frac{9Z}{18Z} \cong Z_2, \frac{18Z}{72Z} \cong Z_4,$

$$\frac{72Z}{\{0\}} \cong 72Z \text{ or } Z$$

Hence (3) and (4) have four factor groups isomorphic to Z_4, Z_2, Z_9 and 72Z or Z.

$$\frac{Z}{4Z} \cong Z_4 \cong \frac{18Z}{72Z},\ \frac{4Z}{8Z} \cong Z_2 \cong \frac{9Z}{18Z},$$

$$\frac{8Z}{72Z} \cong Z_9 \cong \frac{72Z}{9Z},\ \frac{72Z}{(0)} \cong 72Z \text{ (or } Z)$$

Note carefully the order in which the factor groups occur in (3) and (4) is different.

Exmple 5 :

Consider $G = V_4 = Z_2 \times Z_2$

We write a norml series for $G = V_4$:

$$G = Z_2 \times Z_2 \trianglelefteq Z_2 \times \{0\} \trianglelefteq \{0\} \times \{0\}$$

This is a composition series, because

$$Z_2 \times Z_2 / Z_2 \times \{0\} \cong Z_2,\ Z_2 \times \{0\} / \{0\} \times \{0\} \cong Z_2$$

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

Exmple 6 :

Let $G=S_3$, a normal series for G is given by

$$G = S_3 \trianglelefteq A_3 \trianglelefteq \{1\}$$

$$S_3 / A_3 \cong Z_2, A_3 / \{1\} \cong Z_3$$

Both Z_2 and Z_3 are simple group. 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

$$S_n \trianglerighteq A_n \trianglerighteq \{1\}$$

are

But A_n is simple. Hence above is a compositin 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 $N_1 \trianglelefteq G_1, N_2 \trianglelefteq G_2$ are normal subgroups. Then the product $N_1 \times N_2 \trianglelefteq G_1 \times G_2$ and

Solution

Let p_i : be the projection. Then defined by

is an epimorphism.

The Ker $(\psi) = N_1 \times N_2$ Hence

$$(G_1 \times G_2)/(N_1 \times N_2) \cong G_1/N_1 \times G_2/N_2$$

Illustration :

$$(R \times R)/(Z \times Z) \cong (R/Z) \times (R/Z)$$

Example 9 :

Consider the product let and . Then by above and

$$(G \times G')/(N \times N') \cong (G/N) \times (G'/N')$$

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 cyelic group generated by a and O (c) be of prime power order p^e. We write the composition series of length e:

of length e in which each C_i is the Cyclic subgroup generated by 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.

$$G = \langle a \rangle = \{e, a, a^2, a^3 ----, a^{28}, a^{29}\}$$

The only subgroups of G other than G itself are:

$$G_5 : \{e, a^6, a^{12}, a^{18}, a^{24}\}$$
$$G_6 : \{e, a^5, a^{10}, a^{15}, a^{20}, a^{25}\}$$
$$G_{10} : \{e, a^3, a^6, ---, a^{24}, a^{27}\}$$
$$G_{15} : \{e, a^2, a^4, ---, a^{26}, a^{28}\}$$

Note that the subscript i on $G^{i}s$ 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 :

$$G \Delta G_{15} \Delta G_5 \Delta G_1 = \{e\} \qquad (1)$$
$$G \Delta G_{15} \Delta G_3 \Delta G_1$$
$$G \Delta G_{10} \Delta G_5 \Delta G_1$$
$$G \Delta G_{10} \Delta G_2 \Delta G_1$$
$$G \Delta G_6 \Delta G_3 \Delta G_1 \qquad (2)$$
$$G \Delta G_6 \Delta G_2 \Delta G_1$$

The factor groups of (1) are

$$G/G_{15} : \{G_{15}, aG_{15}\}$$
$$G_{15}/G_5 : \{G_5, a^2G_5, a^4G_5\}$$
$$G_5/G_1 : \{G_1, a^6G_1, a^{12}G_1, a^{18}G_1, a^{24}G_1\}$$

The factor groups of (2) are

$$G/G_6 : \{G_6, aG_6, a^2G_6, a^3G_6, a^4G_6\}$$
$$G_6/G_3 : \{G_3, a^5G_3\}$$
$$G_3/G_1 : \{G_1, a^{10}G_1, a^{20}G_1\}$$

We are clearly, $G/G_{15} \cong G_6/G_3$ under the mapping

$$G_{15} \leftrightarrow G_3, \quad aG_{15} \leftrightarrow a^{5}G_3$$

$G_{15}/G_1 \cong G_5/G_1$ *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

	G_5	a^2G_5	a^4G_5
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

The multiplication table for G_3/G_1

	G_1	$a^{10}G_1$	$a^{20}G_1$
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	$a^{10}G_1$

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 $Z_k(G)/Z_k(G)$ is abelin, 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 of nilpotency of G) , so $Z_c(G) = G$. Now G'(. So we get the derived series

.

Hence G is solvable.

Note that the converse is not true i.e. a solvable group need not be nilpotent. For example :

$$G_3 \Delta A_3 \Delta (1)$$

S_3 is solvable but is not nilpolent because center of S_3 is (1). (Every nilpotent group has a non-trivial center)

Exmple 13 :

Consider . Now $Z_1(Z_2 \times S_3) = Z_2 \times (1)$ *and every* $Z_k(Z_2 \times S_3) = Z_2 \times (1)$. Therefore, ascending central series (or upper central series) never reach G. Hence $Z_2 \times S_3$ is not niloptent.

$G = Z_2 \times S_3$

$Z_c \Delta Z_{c-1} \Delta \cdots \Delta G^{(c)} \Delta (1)$, $G \Delta G' \Delta \cdots = (1)$

Unit-III

Modules

Definition

Let R be a commutative ring with identity 1. $(M,+\bullet_R)$ is called and R-module M if $(M, +)$ is an abelian group, together with a scalar multiplication $\longrightarrow M$, written $\longrightarrow$r.m satisfying

1. $r.(m_1+m_2)$ =
2. =
3. =
4. = m

for all and

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. $x+y\in M_1\forall\, x,y\in M_1$
2. $\alpha\, x\in M_1\forall x\in M_1\forall\alpha\in R$

Cyclic Modules

An R-module M is **cyclic** if in M there is a generating element x_o, such that

$$M=Rx_o=\{rx_0/r\in\boldsymbol{R}\}$$

Remark

Any ring R is both a left and a right R-module over itself and also a (R,R)-module. These modules are donated by ${}_RR, R_R, {}_RR_R$.

The submodules of the module ${}_RR$ are the left ideals, etc.

Simple (or irreducible) **module** *:* The R-module, M is called simple if it does not contain proper non-trival submodules.

Examples

1. When $\boldsymbol{R}\equiv Z$, the ring of integers :– Any abelian group V, with law of composition addition, is a module over the ring Z, if

$n.v =$

i.e. abelian group $\equiv Z$ -module

2. A vector space V over a field F is an F-module

3. A linear Vector space is an $M_n(F)$-module if $A.V$ is usual product, where

$$A = (a_{i_j})_{n\times n} \in M_n(F), \quad v = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}_{n\times 1}$$, the column vector v of length n from F^n.

4. Let V be a vector space over the field F. $T : V \longrightarrow V$ is a linear operator. V can be made $F[x]$-module by defining

$f(x).v = f(T)v,$.

Free modules

$F[x]$ $+\ldots+v,$ $r_k m_k$ is a + ve integer Let M be a module over a ring R, and S be a subset of M. S is said to be a **basis** of M if

$\rightarrow n\ times$

1.

$(-v)+(-v)+\ldots+(-v) = -(m.v), when\ n=-m$

2. S generates M

$= (-m).v \quad and\ m\ is + ve\ integer$

3. S is linearly independent.

$0\ if\ n = zero$

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 :

   , $r_i \in \boldsymbol{R}$

   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 Z-module M is finitely generated $\Leftrightarrow$ it is finitely generated abelian group.

2. Consider,

$(R^n +, \cdot_R)$ is a module over $\boldsymbol{R}$, where +,. are defined :

$$\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} + \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} = \begin{pmatrix} a_1 + b_1 \\ a_2 + b_2 \\ \vdots \\ a_n + b_n \end{pmatrix}$$ and .

3. A module isomorphic to any of the modules is called a **free module**.

   Thus a finitely generated module M is free if there is an isomorphism. $\phi : \boldsymbol{R}^n \xrightarrow{\sim} M$.

4. A set of elements $\{m_1, m_2, \ldots\ldots, m_k\}$ of a module M independent if

   $r_1 m_1 + r_2 m_2 + \ldots\ldots + r_k m_k = 0$, $r_i \in R$, the ring, then for each U.

5. Suppose a module M has a basis

   $\{m_1, m_2, \ldots\ldots, m_k\}$. Then $R^k \cong M$

Define $\longrightarrow M$

$(r_1, r_2 \ldots\ldots r_k) \longrightarrow r_1 m_1 + \ldots\ldots + r_k m_k \quad \forall r_i \in R$

ϕ is clearly module-homomorphism. ϕ is surjective : Let m be any element of M

then $m = a_1 m_1 + a_2 m_2 + \ldots\ldots + a_k m_k$, $a_i \in$ the ring

$\therefore$ such that

$$\phi(a_1, a_2, \ldots, a_k) = m$$

ϕ is injective :

$\Rightarrow \quad (a_1 - b_1) m_1 + \ldots\ldots + (a_k - b_k) m_k = 0,$

$\Rightarrow$ (since $\{m_1, \ldots\ldots m_k\}$ is a basis for M)

$\Rightarrow \quad a_i = b_i \; \forall \, i$

$\therefore \phi$ is a bijective $\Leftrightarrow M$ has a bases; in this case M is a free module . So a module M has a basis $\Leftrightarrow$ 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 $f : M \to N$ 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. Imf is a submodule of N, But N is simple, so Imf or . If then but . Therefore, Here f is an epimorphism.

   Corollary : (Shur's Lemma) If M is a simple R-module, then the ring End of R-morphisms. $f : M \longrightarrow M$ is a division ring.

Proof

From (1) and (2) above, every non-zero $f \in$ End is an isomorphism and so is an invertible element in the ring. Hence 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 :

$$\ldots\ldots\ldots \xrightarrow{f_o} M_o \xrightarrow{f_1} M_1 \xrightarrow{f_2} M_2 \xrightarrow{f_3} \ldots\ldots\ldots\ldots$$

This sequence is said to **exact** at M_1 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

$$(0) \xrightarrow{\alpha} M_1 \xrightarrow{\alpha} M \xrightarrow{\beta} M_2 \longrightarrow (0)$$

is called a **short exact sequence.**

Recall that every module over a general ring R is a homonorphic image of a free module. Every R-module M forms part of a short exact sequence.

$$(0) \longrightarrow G \longrightarrow F \longrightarrow M \longrightarrow (0)$$

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

$$(0) \longrightarrow R^m \longrightarrow R^n \longrightarrow M \longrightarrow (0)$$

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 :

, where $d_i / d_{i+1}, i = 1, ..., m-1$

(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

).

Proof

Suppose M is generated by n elements, then M has a presentation

$$(0) \longrightarrow R^m \xrightarrow{\phi} R^n \longrightarrow M \longrightarrow (0),$$

Where $m \leq n$, where M = CoKernel if a homomorphism $\phi : R^m \longrightarrow R^n$, 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

Where d_i / d_{i+1} for $i = 1, ..., r-1$; more precisely PAQ = 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', a', b'* $\in R$. 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

$$(h, o) = (a, b)\begin{pmatrix} a & -b' \\ c' & a' \end{pmatrix}$$

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 and we find that A is associated to

$$\begin{bmatrix} a_1 & 0 \ldots\ldots\ldots 0 \\ 0 & \\ \vdots & A_1 \\ 0 & \end{bmatrix}$$

where is an $(m\text{-}1) \times (n\text{-}1)$ matrix. Now by induction on $m+n$, A_1 is associated to a matrix in diagonal form, say diag $(a_2, a_3, \ldots\ldots a_r, o, o \ldots\ldots o)$. Now we combine this with previous statements we find that A is associated to a diagonal matrix :

$$SAT = \text{dig } (a_1, a_2, \ldots\ldots a_r, o, o \ldots\ldots o)$$

If a_1 / a_{i+1} for $i = 1, 2, \ldots\ldots r-1$, we get the required form. So we assume $a_1 \times a_2$ and consider the 2×2 matrix formed by first two rows and columns. We get an equation

[illegible]

If we reduce the matrix on the right to diagonal form as before we again reach the form SAT = diag , but with a_1 if shorter length than before. After a finite number of steps we have a_1 / a_2. By repeating this process we find that $a_1 / a_i, i = 2, \ldots\ldots, r$. The same process can be used for $a_2, a_3, \ldots\ldots, a_{n-1}$ and so we get the required form. Hence our claim is proved i.e.

$\exists$ invertible matrix P and Q such that PAQ = diag , where d_i / d_{i+1} for $i = 1, 2, \ldots\ldots\ldots\ldots, r-1$ and $r = m$, because ϕ is 1-1. Here P and Q correspond to changes if bases in and R^n respectively; but these changes do not affect the Cokernel, so if $v_1, \ldots\ldots\ldots v_n$ is the new basis in R^n, then the submodule R^m has the basis $d_1, v_1, \ldots\ldots d_m v_m$ and Cokernel takes the form

$$\frac{R}{Rd_1} \oplus \ldots\ldots\ldots\ldots \oplus \frac{R}{Rd_m} \oplus R^{n-m},\ d_i / d_{i+1}, i = 1, \ldots\ldots m-1,$$

Where Cokernel $\phi = M$, and

$$(o) \longrightarrow R^m \xrightarrow{\phi} R^n \longrightarrow M \longrightarrow (o),\ \frac{R^n}{m\phi} = \frac{R^n}{\phi(R^m)}$$

Corollary (application to finitely generated abelian groups)

Since every abelian group is 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 $= a = q_1 \, q_2 ....q_r$ be the factorization of a into powers of different primes, say $q_i = a$ power of . Put $s_i = \dfrac{a}{q_i}$. Now the $s_i^s, 1 \le i \le r$ have no common factor, so

$$s_1 c_1 + s_2 + c_2 + ...+ s_r c_r = 1, c_i \in R$$

Hence $x = xs_1 c_1 + xs_2 c_2 + ...+ xs_r c_r$ and $xs_i c_i q_i = xac_i = 0$. Therefore, $xs_i c_i \in M_{p_i}$

$\therefore$

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 $T(W) \subset W$ 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 eigen values in F. So let T have eigen value in $F. \exists$ a corresponding eigen vector such that Let $= \{\alpha_1 v_1 : \alpha_1 \in F\}$ be a one-dimensional

Vector space over F. Let $x \in W, x = \alpha_1 v_1, \alpha_1 \in F$ and $T(x) = \alpha_1 T(v_1) = \alpha_1 \lambda_1 v_1 \in W$. Hence W is T-invariant.

Let $\bar{V} = V/W$ = dim, dim $(\bar{V})$ = dim (V/W) = din V-din W = n-1.

T induces a linear transformation on = defined by

Also minimal polynomial over F of $\bar{T}$, divides the minimal polynomial of T over F. Hence all the roots of the minimal polynomial of are roots of minimal polynomial of T. Therefore all eigen values, of lie in F. Now satisfies the hypothesis of the theorem. Since dim so by induction hypothesis, $\exists$ a basis of $\bar{V}(V/W)$ over F such that is triangular.

i.e.

$$\bar{T}(\bar{v}_3) = \alpha_{32}\bar{v}_2 + \alpha_{33}\bar{v}_3$$

M M M M

$$\bar{T}(\bar{v}_n) = \alpha_{n_2}\bar{v}_2 + \alpha_{n_3}\bar{v}_3 + \dots\dots\dots + \alpha_{nn}\bar{v}_n$$

Let $v_2, v_3, \dots\dots\dots v_n$ be elements of V mapping to $\bar{v}_2, \bar{v}_3, \dots\dots \bar{v}_n$ respectively, then it is easy to prove that $v_1, v_2, \dots\dots\dots v_n$ form a basis of V. Now $\bar{T}(\bar{v}_2)[-\alpha_{22}\bar{v}_2 = \bar{0} = W$ $i.e.,$

].

$\in V/W$ Hence

M M M M

$$T(v_n) = \alpha_{n_1} v_1 + \alpha_{n_2} v_2 + \dots\dots\dots\dots + \alpha_{nn} v_n$$

$$\Rightarrow \quad T(v_2) = \alpha_{21} v_1 + \alpha_{22} v_2$$

Similarly,

Also $T(v_1) = \lambda_1 v_1 = \alpha_{11} v_1$ (Taking).

Hence a basis of V over F, such that $T(v_i)$ = linear combination of v_i and its predecessors in the basis. Therefore, matrix of T in this basis :

$$\begin{bmatrix} \alpha_{11} & & & & & \\ \alpha_{21} & \alpha_{22} & & & & \\ \alpha_{31} & \alpha_{32} & \alpha_{33} & & & \\ \alpha_{41} & \alpha_{42} & \alpha_{43} & \alpha_{44} & & \\ - & - & - & - & \ddots & \\ \alpha_{n1} & \alpha_{n2} & \alpha_{n3} & \dots & & \alpha_{nn} \end{bmatrix}$$

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,**

$$J = Q^{-1}AQ = \begin{bmatrix} J_1 & & & 0 \\ & J_2 & & \\ & & \ddots & \\ 0 & & & J_s \end{bmatrix}$$

in which each J_i called a **Jordan block**, is a triangular matrix of the form

$$J_i = \begin{bmatrix} \lambda_i & 1 & & 0 \\ & \lambda_i & \ddots & \\ & & \ddots & 1 \\ 0 & & & \lambda_i \end{bmatrix}$$

where λ_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 λ_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 $1x1$ 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 **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 5×5 matrix with eigen value λ 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

$$J = \begin{bmatrix} \lambda & 1 & 0 & 0 & 0 \\ 0 & \lambda & 1 & 0 & 0 \\ 0 & 0 & \lambda & 1 & 0 \\ 0 & 0 & 0 & \lambda & 1 \\ 0 & 0 & 0 & 0 & \lambda \end{bmatrix}$$

This Jordan canonical form consists of only one Jordan block with eigen value λ on the diagonal

2. two linearly independent eigen vectors belonging to .

Then the Jordan canonical form of A is either one of the forms

, or $$J = \begin{bmatrix} \lambda & & & & \\ & \lambda & 1 & 0 & 0 \\ & 0 & \lambda & 1 & 0 \\ & 0 & 0 & \lambda & 1 \\ & 0 & 0 & 0 & \lambda \end{bmatrix}$$

Each of which consists of two Jordan blocks with eigen value λ on the diagonal.

3. $\exists$ three linearly independent eigen vectors belonging to

Then the Jordan Canonical form of A is either one of the forms

$$J = \begin{bmatrix} \lambda & 1 & & & \\ 0 & \lambda & & & \\ & & \lambda & 1 & 0 \\ & & 0 & \lambda & 1 \\ & & 0 & 0 & \lambda \end{bmatrix}$$

, or $$J = \begin{bmatrix} \lambda & & & & \\ & \lambda & & & \\ & & \lambda & 1 & 0 \\ & & 0 & \lambda & 1 \\ & & 0 & 0 & \lambda \end{bmatrix}$$

Each of which consists of three Jordan blocks with eigen value λ on the diagonal.

4. four linearly independent eigen vectors belonging to .

Then the Jordan canonical form of A is of the form

This consists of four Jordan blocks with eigen value λ on the diagonal.

5. five linearly independent eigen vectors belonging to .

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 $| x |$ 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 λ 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 λ of the $n \times n$ matrix A is the dimension of the eigen space corresponding λ. i.e.maximum number of linearly independent eigen vectors corresponding to eigen value λ).

Useful Information to determine J :

1. The sum of the sizes of the blocks involving a particular eigen value of A = algebraic multiplicity of that eigen value.
2. The number of blocks involving a particular eigen value of A = the geometric multiplicity of the eigen value.
3. The largest block involving a particular eigen value of A = the 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 . The minimal polynomial of A always divides characteristic polynomial of A).

Example 2

1.

   A has only the eigen value λ which has algebraic multiplicity 3 and geometric multiplicity 1. $E(\lambda)$: Eigen space for $\lambda = 0 =$

2. $$A = \begin{bmatrix} -2 & -1 & -3 \\ 4 & 3 & 3 \\ -2 & 1 & -1 \end{bmatrix}$$

   Characteristic polynomial of $A = (2-\lambda)^2(-4-\lambda)$ $\lambda = 2$ occurs with geometric multiplicity

Hence $$J = \begin{bmatrix} -4 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{bmatrix}$$

3. Let A be a 7×7 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 2×2 Jordan block and 1×1 Jordan block.

Corresponding to $\lambda = 2$ there must be at least one 2×2 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 $\lambda = 2$:

$$J = \begin{bmatrix} 2 & 1 & 0 & 0 & & & 0 \\ 0 & 2 & 0 & 0 & & & 0 \\ 0 & 0 & 2 & 1 & & & \\ 0 & 0 & 0 & 2 & & & \\ & & & & 3 & 1 & 0 \\ & & & & 0 & 3 & 0 \\ 0 & 0 & & & 0 & 0 & 3 \end{bmatrix}$$

$xr = 0\ \forall x \in M, \forall r \in R.$

or $$J = \begin{bmatrix} 2 & 1 & 0 & 0 & & & 0 \\ 0 & 2 & 0 & 0 & & & 0 \\ 0 & 0 & 2 & 0 & & & \\ 0 & 0 & 0 & 2 & & & \\ & & & & 3 & 1 & 0 \\ & & & & 0 & 3 & 0 \\ 0 & 0 & & & 0 & 0 & 3 \end{bmatrix}$$

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, $yR = M$.

Example 2

Any homomorphic image of a module *M* is isomorphic to a quotient module of M.

Proof

Let $\longrightarrow M_1$ be a module epimorphism and let Ker $\psi = N$. Now we define a mapping

$f : \dfrac{M}{N} \longrightarrow M_1$ defined by $f(x+N) = \psi(x).\ \forall x + N \in M/N$

$f(x+y+N) = f(x+y+N) = \psi(x+y) =$

From above *f* is a module homomorphism. Further *f* is injective since Ker , the zero element of

f is surjective also since ψ is.

Hence $\quad$ Im $f = M_1 = \psi(M)$ i.e. $\dfrac{M}{N} \cong \psi(M)$

Q. 1. Let I be an ideal in a commutative ring *R* with 1. If *M* is an *R*-module, show that the set

$$S = \{xm / x \in I, m \in M\}$$

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 is an ***R*-module.**

Q. 3. Let *M* be a right *R*-module. Show that is an ideal of *R*. It is called **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 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 . Now the submodule *mS* is generated by the elements $ma_1, ma_2, ..., ma_k$,

i.e. $ms = \langle ma_1, ma_2, ...ma_k \rangle$ 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. $I_1 \leq I_2 \leq I_3 \leq .... \leq I_N = I_{N+1} = I_{N+2} ......$ for some integer *N*), 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 : $F[x_1, x_2, ...]$ 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.* . 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 . Then every submodule *N* & *M* is free and has a basis of $\leq n$ elements.
2. From (1) we can deduce that a submodule *N* & *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 $m_i > 1$, each a multiple of the next, for which there is an isomorphism.

   $$G \cong Z_{m_1} \oplus \ldots\ldots\ldots\ldots \oplus Z_{m_k}$$

   the first integer m_1 is the least +ve integer $m = m_1$ with $mG = (0)$ and the product

Example 7

The possible abelian group of order 36 are

$Z_{36}, Z_2 \oplus Z_{18}, \ldots, Z_3 \oplus Z_{12}, Z_6 \oplus Z_6$

No two of these group are isomorphic.

Unit-IV

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+bεR, a.bεR $\quad \forall$a, b ε R.
2. Commutative low with respect to +: a+b=b+a $\forall$a, b ε R.
3. Associative laws:

   a+(b+c) = (a+b)+c

   a.(b.c) = (a.b).c $\quad \forall$a, b, c ε R.
4. Distributive Laws:

   a. (b+c) = a.b+a.c
   (b+c).a = b.a+c.a $\quad \forall$a.b, c ε R.
5. Additive identity: R contains an **additive idenity element**, denoted by 0, such that a+o=a and o+a=a $\forall$a ε R.
6. Additive inverses: $\forall$a ε R, $\exists$ x ε 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 $a.b = b.a \quad \forall a,b \in R$
8. A ring (R, +, .) is called a ring **with identity** if such that a.1 = a and1.a = a

   In this case 1 is called a **multiplicative identity element** or simply an **identity element.**

Examples

1. (Z +, .) is commutative ring with identity 1 (Ring of integers under ordinary addition and multiplation.
2. E: set of even integers. (E, +, .) is a commutativering without identity element.

3.

then $(M_2(R), +, .)$ is a non-commutative ring with identity $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \Theta\ 1 \in R.$

whose +, ; are defined as addition of matrices and multiplication of matrices.

$A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} B = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \in M_2(R)$ and

$A.B \neq B.A.$

If IR, the set of real numbers is replaced by E, the set of even integers, then

(M_2 (E), + ;) is a **non-commutative ring without identity,** as

4. Z_4 : Set of integers module 4.

is a **commutative ring with** identity , where +, ; are defined shown in following tables:

$\cdot_4$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

Important Remark:

As we saw in a group that **Cancellation law** holds but in a ring the cancellation law **may fail for** multiplication:

In $(Z_6, +, .)$, $\bar{2}.\bar{3} = \bar{0} = \bar{4}.\bar{3}$ but $\bar{2} \neq \bar{4}$.

Definition Subring:

Let (R, +, .) is a ring and a non-empty subset of R. Then (S, +, .) (with same binary operations) is called a **subring** if

1. **Closure**

2. $\forall\, a \in R,\ -a \in R.$

Examples:

(1) $(Z_6, +, .)$ is a commutative ring with identity. (S, +, .) is a subring with identity (multiplicative) , since Note that parent ring $(Z_6, +;)$ has identity . 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 righ with identity 1.** An element $a \in R$ is said to be **invertible** if such that a.b = 1. The element $a \in R$ is called a **Unit of R.**

Divisiors 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 such that ab = 0 for some in R, is called a **divisor of zero.**

In is a divisor of zero.

In are divisors of zero.

2. Let IR be the set of real numbers, and

is acommutative ring wth identity. + : defined by

(Addition and multiplication are defined pointwise).

$I(x) = 1 \; \forall x \in IR$, I is identity of the ring R.

Note that (R, +, .) is a commutative ring with identity and also with divisors of zero.

$$If \;\; f(x) = \begin{cases} 0, & x < 0 \\ 1, & x \geq 0 \end{cases}$$

$$and \;\; g(x) = \begin{cases} 1, & x < 0 \\ 0, & x \geq 0 \end{cases}$$

$then \; (f.g)(x) = f(x)g(x) = 0 \;\; \forall x \in IR$. In above example, (f.I) (x)

$$\begin{aligned} &= f(x)I(x) && \forall \, x \in IR \\ &= f(x)1 && \forall \, x \in IR \\ &= f(x) && \forall \, x \in IR \end{aligned}$$

If $(f.g)(x) = f(x).g(x) = I(x) = 1 \quad \forall \, x \in IR$

and $f(x) \neq 0, \; g(x) \neq 0 \quad \forall \, x \in IR$, then f has a multiplicative inverse $\Leftrightarrow$

. Hence for example

$f(x) = 2 + \sin x$ has a multiplicative inverse, but $g(x) = Sin\, x$ does not.

Definition: Integral Domain:

If $(R, +, .)$ is a commutative ring with identity such that for all

Examples:

1. $(Z_6, +, .)$ is not an integral domain.

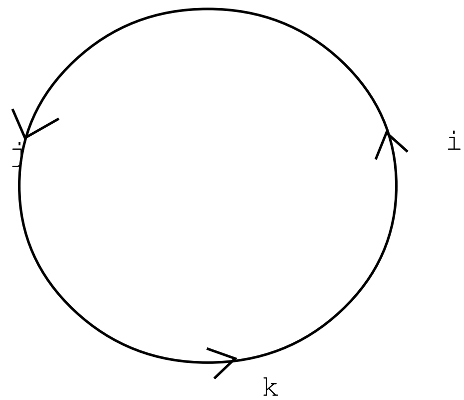
2. the ring of real valued functions, the example given on page 5 is not an Integral domain.

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:

$(D, +, .)$ is a division ring, where $+, .$ are defined as



$$D = \{\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k \mid \alpha_0, \alpha_1, \alpha_2, \alpha_3 \in R\}$$

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

where $i^2 = j^2 = k^2 = i\,j\,R = -1$, $ij = -ji = k$, $jk = -kj = i$, $ki = -ik = j$.

Let $x = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k \neq o$ in D.

Then $\exists\, y = \frac{\alpha_0}{\beta} - \frac{\alpha_1}{\beta} i - \frac{\alpha_2}{\beta} j - \frac{\alpha_3}{\beta} k \in D$, such that

$$x.y = 1,$$
$$\text{where } \beta = \alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2 \neq o$$

Definition:

A commutative ring with identity is a field if its every non-zero element has inverse in it.

Example:

$(R, +, .)$ the ring of real numbers 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

$$xy = \Rightarrow x^{-1}(xy) = x^{-1} = 0$$
$$\Rightarrow (x^{-1}x)y = 0$$
$$\Rightarrow y = 0$$

Similarly, if $y \neq 0$, then

$$xy = 0 \Rightarrow xyy^{-1} = 0.\ y^{-1}$$
$$\Rightarrow x.e = 0$$
$$\Rightarrow x = 0$$

Hence $xy = 0 \Rightarrow x = 0$ 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 $D^* = D - (o)$.

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 integar n.

Ring homomorphism:

Let R and S be rings. A function

$\psi : R \longrightarrow S$ is called **ring homomosphism**

if $\psi(a+b) = \psi(a) + \psi(b)$ and

for all

$a, b \in R.$

Kernel of ring homomorphism:

is called the zero elements of S.

, the kernel of , denoted by ker .

Examples

1. The polynomial is irreducible over Q, where p is a prime.

Proof

$(x-1)f(x) = x^p - 1$. Put $x = y+1$, then

$$= y^p + \binom{p}{1} y^{p-1} + \binom{p}{2} y^{p-2} + \ldots\ldots\ldots\ldots + \binom{p}{p-1} y \qquad (1)$$

Where $\binom{p}{i}$ = , $i < p$

Not that and divides the product . Hence p divides

Dividing (1) by y, we see that

satisfies the hypothesis of Eisentein criterion and so it is irreducible over Q. Hence $f(x)$ is irreducible

2. is irreducible over Q, since $p = 5$, , , 5 divide,

$f(y+1) = y^{p-1} + \binom{p}{1} y^{p-2} + \ldots\ldots\ldots\ldots + \binom{p}{p-1}$

3. is irreducible over Q, p is a prime number.

4. $f(x) = x^4 + x^3 + x^2 + x + 1$ is irreducible over Q. Put $x = (y+1)$

$=$

$= y^4 + 5y^3 + 10y^2 + 10y + 5$

Take $p = 5$, so is irreducible over Q, hence is irreducible over Q.

Field Extensions

Definition

Let k be a field. A field K is calld 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 a finite set, then $k(S) := k(a_1, a_2, \ldots\ldots\ldots, a_n)$.

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_k = degree of K 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 psynomial $f(x) \in k[x]$ 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 $f(x) \in k[x]$, 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 $p(x)$ be any irreducible polynomial in k[x] which has one root b in K. Let L be a splitting field of over K and let b_1 be any root of in L. Now from unit IV, we get a k-isomorphism of k(b) onto k(b_1) such that (b) = b_1. Also (f(x))=f(x), since and σ is k-isomorphism. Since K is a splitting field of So K is a splitting field of f(x) over k(b). Now $K(b_1) = k(a_1, a_2, \ldots, a_n, b_1)$ is a splitting field of f(x) over k(b_1). Hence from Unit IV, ∃ an isomorphism of K onto K(b_1) such that for all In particular, Since $a_1, a_2 \ldots a_n \in K$ are roots of f(x) over k, so (a_1), (a_2), ..., (a_n) are roots of in $K(b_1)$, so $\{\rho(a_1), \ldots, \rho(a_n)\} = \{a_1, a_2, \ldots, a_n\}$ may be indifferent order. Let $h(x_1, x_2, \ldots x_n)$ be a polynomial be a polynomial in k[x] such that $h(a_1, a_2, \ldots, a_n) = b$, say then

$$\rho(b) = \rho(h(a_1, a_2, \ldots, a_n)) = \rho(h)(\rho(a_1), \ldots, \rho(a_n)) = h(\rho(a_1), \ldots, \rho(a_n)) \in K.$$

Hence $\rho(b) \in K$, 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 same polynomial in k[x].

Proof:

Let $K = k(a_1, a_2, \ldots, a_n)$ and let $p_i(x)$ be irreducible polynomial over k such that ∀ i. Since K is a normal extension of k, each $p_i(x)$ splits in K[x]. So $p_1(x)\, p_2(x) \ldots p_n(x) = f(x)$ say, splits in K[x]. K is got by adjoincing roots of 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 o 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 additon, then the characteristic of R is O. If 1 has order n under addition, then the characteristic of R is n). Note that the characteristic of a field is O or a prime.

Theorem 3.

Every finite field is perfect.

Proof:

Let k be a finite field of characteristic p. Define .

$\forall\ a \in k$

Then

$= a^p + b^p \quad \left(\because\ p \,\Big/ \binom{p}{i},\ 1 \le i \le p-1\right)$

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

$\because\ a^p \neq 0$ *when* $a \neq 0$ *in k, so ker* $\psi = (0)$

Now ψ is one-to-one and since k is finite, so is onto,

$\psi(a+b) = (a+b)^p = a^p + \binom{p}{1} a^{p-1} b + \binom{p}{2} a^{p-2} b^2 + - - - - + \binom{p}{p-1} a b^{p-1} + b^p$

we get k=k, hence k is perfect.

Theorem 4.

If p(x) is irreducible polynomial over a perfect field k, then p(x) has no multiple roots.

Proof:

CaseI: Characteristic k =0 (i.e. 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) = Irr (k, a). Then and p^1 (x) is of smaller degree than p(x). Therefore . Hence Thus is seperable over k and so p(x) has no multiple roots.

Case II: Let char k = p.

Let p(x) have multiple roots

Since p'(a) = 0 and since deg p'(x) < deg p(x) so for k = 1, 2 -------, n,

where $p(x) = x^n + a_{n-1}x^{n-1} + - - - - - - + a_k x^k + - - - - - - + a_1 x + a_0,\ a_i \in k\ \forall$ i.

$\therefore\ a_k = 0$ when $p \times k$. Hence only powers of x that appear in

are those of the form $x^{pi} = \left(x^p\right)^i$. Hence $p(x) = g\left(x^p\right)$ for some $g(x) \in k[x]$. (for example: if $p(x) = x^{6p} + 3x^{4p} + 5x^{2p} + x^p + 1$, then $g(x) = x^6 + 3x^4 + 5x^2 + x + 1$).

Now $p(x) = g(x^p)$, $g(x) \in k[x]$ and $k^p = k$, 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

$$p(x) = g(x^p) = x^{pn} + b_{n-1}^p + x^{p(n-1)} + - - - - - + b_1^p x^p + b_0^p$$

$$= (x^n + b_{n-1}x^{n-1} + - - - - - + b_1 x + b_0)^p$$

(Char k = p and so $p_i = 0$ $\forall$ i)

=

But then p(x) is not irreducible over k.

Finite Fields:

We know $(\mathbb{Z}_p, +, \bullet)$ 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 char k = p. Then k has p^n elements, for some positive integer n.

Proof:

Define

$\forall\ n \in \mathbb{Z}$

Where

m times

Clearly ψ is a ring homomorphism.

ker = p$\mathbb{Z}$, p = char k

But $\dfrac{\mathbb{Z}}{p\mathbb{Z}} \cong \mathbb{Z}_p$, a field of p elements, so Im ψ is a subfield of k, isomorphic to . 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 $u_1, u_2, - - - - - - - u_n$ be a basis of k over F. Now each element x of k can be written as:

$x = \alpha_1 u_1 + \alpha_2 u_2 + - - - - - + \alpha_n u_n,\ \alpha_i \in F$ $\forall$ i.

As $|F| = p$ ($F \cong Z_p$), each $\alpha_i \in F$ 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 elements.
4. $\forall$ prime p and $\forall$ positive integer n, $\exists$ a field with elemetns.

Proof:

1. $\because$ k has elements, then k^*, the multiplicative group of k has $p^n - 1$ elements. Hence for any $x \in \overset{*}{k} \subset k$, $x^{p^n - 1} = 1$, so $x^{p^n} = x$ $\forall$. The polynomial has atmost p^n roots and so its roots must be precisely the elements of k. Hence k is the splitting field of $f(x)$ over the prime subfield of k.
2. is the corollary of (1). Let and k_2 be two finite fields with p^n elements, containing prime subfields F_1 and F_2 respectively. But $F_1 \cong Z_p \cong F_2$. 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), [illegible]
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) = $x^{p^m - 1} - 1$ is a divisor of As k is the splitting field of $x^{p^n} - x = xf(x)$ over F_1. We know that $\{a \in k : a^{p^n} = a\}$ 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 $xg(x) = x^{p^m} - x$. 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 Z_p. Now $x^{p^n} - x = x(x^{p^n - 1} - 1)$ *and* $p \times (p^n - 1)$. 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 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. $k^* = k - (0)$. $So \left|k^*\right| = p^n - 1 = m$ say. Let $a \in k^*$ be of maximal order, say m_1 i.e. $o(a) = m_1$. 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 satisfies $f(x) = x^{m_1} - 1$. Since k is a field, so there are at most m_1 roots of f(x), hence $m \leq m_1$. But $m_1 \leq m$, so $m = m_1$, 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 $\psi : K \to K$

$\forall$

such that

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

ψ is 1–1 and onto

and (C) = C $\forall$

Then 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 .

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 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 . This correspondence is given by

2. If $k \subseteq L \subseteq K$, then is Galois

   In this case $G(K/k) \cong \dfrac{G(K/k)}{G(K/L)}$.

Proof:

1. Define $\Psi : \{L : k \subseteq L \subseteq K\} \to \{G(K/L) : G(K/L) \leq G(K/k)\}$

   i.e. Ψ is a mapping from set of all fields between k and K into set of all subgroups as follows:

   Since K/k is Galois, is separable. Let M be another field such that and So we assume that Since K/k separable and is separable, hence such that This shows that $G(K/L) \neq G(K/M)$.

   Now $\Psi(L) = G(K/L)$ *and* $L \neq M \Rightarrow G(K/L) \neq G(K/M)$

   So $L \neq M \Rightarrow \Psi(L) \neq \Psi(M)$ Hence there is a one-one mapping $L \to G(K/L)$ from the set of all fields between k and K into the set of all subgroups of

To show Ψ is onto:

Let H be a subgroup of and let L be the fixed field of N. Since finite Galois extension, so is normal and separable, is normal and separable. Hence is Galois and L is the fixed field of Each element of H leaves each element of L fixed and so $H \leq G(K/L)$.

(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 seperate

Therefore and Hence ψ 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: $\forall$

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).

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

.

Now to show L/k 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 $\rho \in G(K/L)$, then an element such that , for some $\sigma \in G(K/k)$

.

Now $\rho\sigma = \sigma\tau \Rightarrow (\rho\sigma)(a) = (\sigma\tau)(a) = \sigma(\tau(a))$

$\Rightarrow \rho(\sigma(a)) = \sigma(a) \; \forall \; a \in L$ and $\tau \in G(K/L)$.

$\Rightarrow \sigma(a)$ is left fixed by each element of .

for all . Hence p(x) splits in L[x].

which implies is normal, is already separably, so is Galois extension.

Finally, to show :

Define $\Psi : G(L/k) \rightarrow G(K/K)$

$\sigma \; \alpha \quad \Psi(\sigma)$

such that = the restriction of $\forall \; \sigma \in G(L/k) = \sigma*$

(normal, $\forall \; \sigma \in G(L/k)$, so induces an automorphism of L defined by (l) =

(l) $\forall$ Further $\forall$ i.e. leaves every element of k fixed, hence

Now $\forall \; \sigma_1, \sigma_2 \in G(L/k)$

but $\forall \; l \in L$

= $\forall \; l \in L$

= $\forall \; l \in L$

=

$\forall$.

is a homomorphism.

$\forall \; l \in L$

$\Leftrightarrow \ \sigma_* \in G(K/L)$

Hence ker .

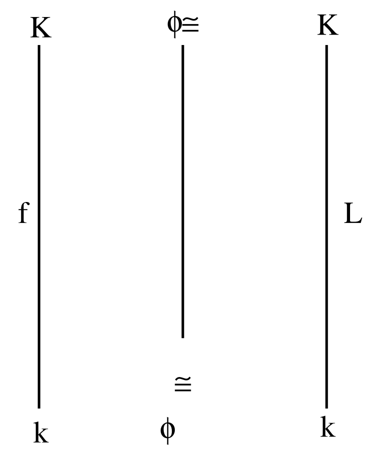
Therefore

$$\Rightarrow \ \frac{G(K/k)}{G(K/L)} \cong \operatorname{Im}\Psi \subseteq G(K/k)$$

Claim: Ψ 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 $\forall$

such that $\Psi(\sigma) = \sigma_*$, Hence ψ onto, so Im = .

Finally, we get

Solution 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. $K = k(\alpha_1, \ \alpha_2, \text{------}, \ \alpha_m)$ and

2.

For $f(x) \in k[x]$, the polynomial equaton 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.

is solvable by radicals over k $\Leftrightarrow$ the Galois group over k of f(x) is a solvable group.

Definition:

Let k be a field, let and let K be a splitting field for f(x) over k. Then $G(K/k)$ 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 defines a permutation of the roots of f(x) that lie in K.

as $\sigma(\alpha) = \alpha \ \forall \ \alpha \in k \ so \ \sigma f = \sigma$. 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 Hersteim.

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, -------a_n) is the field of rational functions in the n variables a_1, a_2, -------a_n, then the Galois group of the polynomial $f(x) = x^n + a_1 x^{n-1} + ------a_n$ over F(a_1, a_2, -------a_n) is S_n, the symmetric group of degree n (see thu 5.6.3, Hersteins Topics in Algebra). But S_n is not solvable group when $n \geq 5$. Hence by thu 9, f(x) is not solvable by radicals over F(a_1, a_2, -------a_n) when .

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

   $f(\alpha_i) = 0 \Rightarrow \sigma(f(\alpha_i)) = \sigma(0) \Rightarrow \sigma f(\sigma(\alpha_i)) = 0 \Rightarrow f(\sigma(\alpha_i)) = 0$

   [K : F] = n

   This is read, "the degree of K over F is equal to n."

2. Let 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(c) over F is equal to the degree of the minimal polynomial of e over F.**

   $[F(C) : F] = \deg I_{rr}(F, C)$

Example 1.

   $[Q(\sqrt{2}) : Q] =$ deg of irreducible

   polynomial p(x) = x^2–2 over Q = deg $I_{rr}(Q, \sqrt{2})$.

   .

3. If K is a finite extension of F and K = F(a_1, a_2, -------a_n), then a_1, a_2, -------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.

$$\left[Q(\sqrt{2}, \sqrt{3}) : Q\right] = \left[Q(\sqrt{2}, \sqrt{3}) : Q(\sqrt{2})\right]\left[Q(\sqrt{2}) : Q\right] = 4$$

Put $Q(\sqrt{2}) = L,\ Q(\sqrt{2}, \sqrt{3}) = L(\sqrt{3})$.

Then $\left[Q(\sqrt{2}, \sqrt{3}) : Q(\sqrt{2})\right] = \left[L(\sqrt{3}) : L\right] = 2,$

the degree of independent polynomial $p(x) = x^2 - 3 \text{ over } L = Q(\sqrt{2})$.

i.e. $\left[L(\sqrt{3}) : L\right] = \deg I_{rr}(L, \sqrt{3}) = 2$.

$\left[Q(\sqrt{2}) : Q\right] = \deg I_{rr}(Q, \sqrt{2}) = 2$ (from example 1)

Hence the result.

5. If p(x) is an irreducible polynomial of degree n in F[x], then $F[x]/\langle p(x)\rangle \cong F(c)$, where e is a root of p(x). By (2), F(c) is of degree n over F.

If are roots of the same inducible polynomial p(x) over F, then $F(\alpha) \cong F(\beta)$.

Example 3.

We construct a field of four elements. $p(x) = x^2 + x + 1$ is iredducible in $Z_2[x]$, as $p(\bar{0}) \neq \bar{0},\ p(\bar{1}) \neq \bar{0}$.

Hence $Z_2[x]/\langle p(x)\rangle \cong Z_2(c)$, where e 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:

$+_2$	0	1	c	$c+1$
0	0	1	c	$c+1$
1	1	0	$1+c$	c
c	c	$1+c$	0	1
$c+1$	$c+1$	c	1	0

$\bullet_2$	1	c	$c+1$
1	1	c	$c+1$
c	c	$c+1$	1
$c+1$	$c+1$	1	c