ALGEBRA.

Unit - I. Group Theory.

A counting principle - Normal subgraphs & Quotient - groups - Homomorphisms - Cayley's theorem - permutation groups - Another counting principle - Sylow's theorem.

Unit - II. Ring theory.

Homomorphisms - Ideals & Quotient - Rings - More Ideal and Quotient - Rings - Euclidean Rings - particular Euclidean ring.

Unit - III polynomial Rings.

polynomial rings - polynomials over the rational field - Polynomial rings over commutative rings.

Unit - IV. Field.

Extension field - Root of polynomials - More about roots.

Unit - V Finite Field.

The elements of Galois theory finite field

UNIT - I

GROUP THEORY

Group.

Let G be a non-empty set.

Atlest one element then it is called non-empty set.

Satisfying the following conditions,

i) closure law.

$a, b \in G \Rightarrow a \cdot b \in G$

$G = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

$2, 3 \in G \Rightarrow 2 \times 3 = 6 \in G$

$4, 6 \in G \Rightarrow 4 \times 6 = 24 \notin G$

ii) Associative law.

$a, b, c \in G \Rightarrow (a \cdot b) \cdot c = a \cdot (b \cdot c)$

+, x are true but −, ÷ need not be true.

2, 3, 4 are given by,

(+). $(a+b)+c = a+(b+c)$

$9 = 9$

(x) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

$24 = 24$

The value is statisfies by (x).

(−) $(2-3)-4 = 2-(3-4)$

$-5 = 3$

This value is not statisfies by (−)

(÷) $(2\div 3)\div 4 = 2\div (3\div 4)$

$\frac{1}{6} \neq \frac{8}{3}$

∴ This value is not statisfies by (÷).

Identity law.

$\forall\ e \in G \Rightarrow e \cdot a = a \cdot e = a \in G$

$\Rightarrow ea = ae = a$

e — × → 1

e — + → 0.

This identity element values is 1.

Inverse law.

There is to each from $a \in G$, then $a^{-1} \in G$.

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

∴ $(G, \cdot)$ is a group.

Abelian Group. (or) Commutative law.

+, × ~~are~~ true (but) ~~−~~, ÷ need not be true.

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

$(G, \cdot)$ is a Abelian group.

Properties	Structure
Closure	Quasi group (or) Groupoid
Closure, Associative	Semi Group
Closure, Associative, Identity	Monoid Group
Closure, Associative, Identity, Inverse	Group
Closure, Associative, Identity, Inverse, Commutative	Abelian Group.

Abelian Group (or) Commutative law.

Let $(G, \cdot)$ be a group. Then If, " $\forall\, a, b \in G \Rightarrow a \cdot b = b \cdot a$ " so G is called Abelian group.

Finite Group.

Let number of elements is called finite

Ex $G = \{1, -1, i, -i\}$ under $\times$.

Infinite Group.

Let number of elements in addition is called infinite group.

Ex $G = \{0, \pm 1, \pm 2, \ldots\}$ under $+$.

Order of Group.

Let number of distinct elements is called Order of group. It is denoted by $o(G)$

Ex. $G = \{2, 3, 4, 4, 5, 7, 2, 10, 3, 12\}$.

$o(G) = \{2, 3, 4, 5, 7, 10, 12\}$.

Order of Element.

Let least positive integer $n \ni$:

$a^m = e \rightarrow o(a)$. Hence $o(e) = 1$

Ex. $G = \{1, -1, i, -i\}$ under $\times$.

$\Rightarrow o(G) = 4$

$|||^{ly}$

$o(-1) = 2$, $(-1)^1 = -1$, $(-1)^2 = 1$, $(-1)^3 = -1$.

$o(1) = 1$ $(1)^1 = 1$

$o(-i) = 4$, $(-i)^1 = -i$, $(-i)^2 = -1$, $(-i)^3 = i$

$(-i)^4 = 1$.

$o(i) = 4$, $(i)^1 = i$, $(i)^2 = -1$, $(i)^3 = -i$,

$(i)^4 = 1$.

Scanned with CamScanner

A counting principle

Defn 1: S.m ①

As we have defined earlier, if it is subgroup of G and $a \in G$, the the consist of all elements in G of the form ha, where $h \in H$.

Let us generalize this notion. If H, k are two subgroups of G

Let $Hk = \{x \in G \mid x = hk,\ h \in H,\ k \in k\}$

~~Defn 2~~ Ex.

Let pause and look at an example

Let $H = \{e, \phi\}$, $k = \{e, \phi\psi\}$

$\because \phi^2 = (\phi\psi)^2 = e$, both H & k are subgroups

Since Hk consists of four elements and 4 is not a divisor of 6, the order of S_3 by Lagrange's theorem Hk could not be a subgroup of S_3.

we might try to find out Hk is not a subgroup.

Note that $kH = \{e, \phi, \phi\psi, \phi\psi\phi = \psi^{-1}\} \neq Hk$

This is precisely Hk fails to be a subgroup.

Notes : 1 (counting principle).

If $|HK| = \dfrac{|K||H|}{|H \cap K|}$

Then, H & K are finite subgroup of G

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

Remark (i)

If $H \cap K = \{e\}$.

$$\Rightarrow O(HK) = O(H)\, O(K)$$

(ii) $O(H) > \sqrt{O(G)}$ & $O(K) > \sqrt{O(G)}$ $\Rightarrow H \cap K \neq \{e\}$ (or) $O(H \cap K) > 1$ (or) $O(K)\, O(H \cap K) \geq 2$ (or) $H \cap K$ has atleast 2 elements.

Note 2 : (Group)

Let $G = S_3$ the group of all 1-1 mapping under the multiplication of real numbers. Then G is an abelian group of order 2.

If not just in S_3 but in any group G

let define us $a \in G$.

$a^0 = e$, $a^1 = a$, $a^2 = a \cdot a$, $a^3 = a \cdot a^2$, ...

$a^k = a \cdot a^{k-1}$

And, $a^{-2} = (a^{-1})^2$, $a^{-3} = (a^{-1})^3$, ...

Lemma 1 : S.m ① (A1)

Hk is a subgroup of G if and if $Hk = kH$

Proof:

Suppose first that $Hk = kH$

ie) $h \in H$ & $k \in k$, Then $hk = k_1 h_1$ for some $k_1 \in k$, $h_1 \in H$. (it need not be that $k_1 = k$ (or) $h_1 =$)

To prove that: Hk is a subgroup, we must verify that it is closed and every element in Hk has its inverse in Hk.

Let show that closure first

Suppose $x = hk \in Hk$ &

$y = h'k' \in Hk$

Then, $xy = hkh'k'$

$\because kh' \in kH = Hk$,

$kh' = h_2 k_2$ with $h_2 \in H$ & $k_2 \in K$.

Hence $xy = h(h_2 k_2)k'$

$xy = (hh_2)(k_2 k') \in Hk$ &

Hk is closed.

Also $x^{-1} = (hk)^{-1}$

$= k^{-1}h^{-1} \in KH = HK$

So, $x^{-1} \in HK$.

Thus HK is a subgroup of G

On other hand, if HK is subgroup of G,

Then $\forall\ h \in H, k \in K$, $h^{-1}k^{-1} \in HK$ &

$kh = (h^{-1}k^{-1})^{-1} \in HK$

Thus $KH \subset HK$

Now if x is any element of HK,

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

And so, $x = (x^{-1})^{-1}$

$= (hk)^{-1}$

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

So $HK \subset KH$

Thus $HK = KH$

An intersecting special case is situation when G is an abelian group for in that case trivally $HK = KH$

Hence the proof //

$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| -$
$|A \cap C| + |A \cap B \cap C|$.

① In a survey of 60 people of way found that 25 read news week magazine, 26 read time, 26 read fortune, 9 read both new week & fortune, 11 read both new week & time, 8 read both time & fortune, 3 ~~all~~ read all three magazine.

$|N| = 25$
$|T| = 26$
$|F| = 26$
$|N \cap F| = 9$
$|N \cap T| = 11$
$|T \cap F| = 8$
$|N \cap T \cap F| = 3$.

$|N \cup T \cup F| = |N| + |T| + |F| - |N \cap T| - |N \cap F| - |T \cap F| + |N \cap T \cap F|$

$= 25 + 26 + 26 - 9 - 11 - 8 + 3$

$|N \cup T \cup F| = 52$.

Corollary 1

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

If H, K are subgroups of a group G. We have seen that the subset HK need not be a subgroup of G. ~~Let it is a perfect meaningful question to ask:~~

If we denote this number by O(HK)

Theorem 1 10.m (A2)

WI If H & K are finite subgroup of G of order o(H) & o(K) respectively then,

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

Proof:

Although their is no need to pay special attention to the particular case in which $H \cap K = (e)$. Looking at this case which is devoid of some of the complexity of the general solution.

Here, we should seek to show that,

$o(HK) = o(H)\,o(K)$ (Corollary 1)

We list all the elements hk, $h \in H$, $k \in K$ there should be collapsing.

(ie) Some elements in the list must appear at least twice.

Equalently $\forall\ h \neq h_1 \in H$, $hk = h_1 k_1$.

But then, $h_1^{-1} h = k_1 k^{-1}$

Now since $h_1 \in H$, h_1^{-1} must also be in H

Thus $h_1^{-1} h \in H$

$|||^{ly}$ $k_1 k^{-1} \in K$.

$\because h_1^{-1}h = k_1 k^{-1}$, $h_1^{-1}h \in H \cap K = (e)$, so

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

Then, $h = h_1$. a contradiction, we have proved that no collapsing can occur and so here $O(H)$ is indeed $O(H)O(K)$.

We assert it must appear $O(H \cap K)$ times

To see this we first remark that if $h_1 \in H \cap K$. Then,

$hk = (hh_1)(h_1^{-1}k)$, where $hh_1 \in H$.

$h_1^{-1}k \in K$.

$\because h \in H$, $k_1 \in H \cap K \subset H$ &

$\because h_1^{-1} \in H \cap K \subset K$ & $k \in K$.

Thus hk is duplicated in the product atleast $O(H \cap K)$ times.

However if $hk = h'k'$.

Then, $h^{-1}k^{-1} = k(k')^{-1}$.

$= u$ & $u \in H \cap K$ & so $h' = hu$

$k' = u^{-1}k$.

They the number of distinct elements in HK is the total number in the listing of HK

(ie), $\dfrac{O(H)\,O(K)}{O(H \cap K)}$.

Suppose H, K are subgroup of the finite subgroup of G and $o(H) > \sqrt{o(G)}$, $o(K) > \sqrt{o(G)}$

$\because HK \subseteq G$, $o(HK) \leq o(G)$

However,

$$o(G) \geq o(HK) = \frac{o(H)\,o(K)}{o(H \cap K)} > \frac{\sqrt{o(G)}\sqrt{o(G)}}{o(H \cap K)}$$

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

Thus, $o(H \cap K) > 1$

$\therefore H \cap K \neq (e)$

Hence the Proof.

II. Normal Subgroups & Quotient Groups.

($\forall \to$ All element)

Normal subgroups.

Let N be a subgroup of G.

If " $\forall\ g \in G,\ n \in N \Rightarrow gng^{-1} \in N$ (or) $gNg^{-1} \in N$ " then N is called Normal subgroup of G.

Remark.

If G is finite than all subgroup are Normal subgroup.

Ex.

Consider the group $G = \{1, -1, i, -i\}$ under '$\times$'. Normal subgroup are $\{i\}$, $\{1, -1\}$ & $\{1, -1, i, -i\}$.

Results (Normal Subgroups)

1. If N is subgroup of G, then the following are equivalant.

(a). N is normal subgroup in G

(b). $gNg^{-1} \subseteq N \ \forall\ g \in G$

(c). $gNg^{-1} = N \ \forall \ g \in G$ ($gng^{-1} = n$ need not be true $\forall n$).

(d). $gN = Ng \ \forall \ g \in G$ (Left coset = Right coset).

(e). $NaNb = Nab \ \forall \ a, b \in G$ (product of two right cosets is also right coset).

Quotient Groups. (Factor Group).

If N is normal subgroup of G Then, $\frac{G}{N} = \{ Ng ; g \in G \}$ is called Quotient group.

Remark.

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

No. of cosets of N in $G = \frac{o(G)}{o(N)}$

Note :-

Consider Quartition group of G.

$\pm 1, \pm i, \pm j, \pm k$.

$\Rightarrow$ G is non-trivial normal subgroup

$\Rightarrow$ G is not simple.

Normal Subgroup.

A subgroup N of G is said to be a normal subgroup of G if $\forall\ g \in G$ & $n \in N$, $gng^{-1} \in N$.

Equivalently if by gNg^{-1} we mean the set of all gng^{-1}, $n \in N$. Then N is a normal subgroup of G. iff $gNg^{-1} \subset N$ $\forall\ g \in G$

Note 1.

Let G be the group S_3.

Let H be the subgroup $\{e, \phi\}$.

$\therefore$ The index of H in G is 3.

There are three right cosets of H in G & Three left cosets of H in G.

Right cosets	Left cosets.
$H = \{e, \phi\}$	$H = \{e, \phi\}$
~~$H\psi = \{\psi, \phi\psi\}$~~	$\psi H = \{\psi, \psi\phi = \phi\psi^2\}$
$H\psi^2 = \{\psi^2, \phi\psi^2\}$	$\psi^2 H = \{\psi^2, \psi^2\phi = \phi\psi\}$.

In $G = S_3$

Let us consider the subgroup $N = \{e, \psi, \psi^2\}$.

∴ The index of N in G is 2

There are two left cosets & two right cosets.

Right Cosets

$N = \{e, \psi, \psi^2\}$

$N\phi = \{\phi, \psi\phi, \psi^2\phi\}$

Left Cosets

$N = \{e, \psi, \psi^2\}$

$\phi N = \{\phi, \phi\psi, \phi\psi^2\}$

$\phi N = \{\phi, \psi^2\phi, \psi\phi\}$.

Lemma - 1

The subgroup N of G is a normal subgroup of G iff every left cosets of N in G a right cosets of N in G.

Proof:

If N is a normal subgroup of G

Then $\forall g \in G$, $gNg^{-1} = N$, whence $(gNg^{-1})g = Ng$; equivalently $gN = Ng$ and so the left coset gN is the right coset Ng.

∵ $g = ge \in gN$, whatever right coset gN turns out to be, it must contain the element g.

However, g is the right coset Ng, and two distinct right cosets have no element in common.

Then $gN = Ng$ follows In other words $gNg^{-1} = Ngg^{-1} = N$ and so N is a normal subgroup of G.

We have alread defined by HK Whenever H & K are subgroup of G.

Then for two subsets A & B of G.

$$AB = \{x \in G / x = ab, a \in A, b \in B\}.$$

AS special case of in $A = B = H$ a subgroup of G.

Then $HH = \{h_1 h_2 \mid h_1 \in H\} \subset H$

∵ H is closed under multiplication

But $HH = H$

Suppose that N is a normal subgroup of G, and that $a, b \in H \Rightarrow N(a)(N(b))$

∵ N is normal in G

∴ $aN = Na$

$$NaN.b = N(aN)b$$

$$= N(Na)b$$

$$= NNab$$

$$NaNb = Nab$$

Hence the proof //.

Theorem :- 1

If G is a group, N is a normal subgroup of G, then G/N is also a group. It is called the Quotient group (or) factor group of G by N

Proof :-

If in addition G is a finite group what is the order of G/N

∵ G/N has as its elements the right cosets of N in G &

∴ There are precisely

$$i_G(N) = \frac{o(G)}{o(N)} \text{ such cosets.}$$

Lemma - 2. (A4)

A subgroup N of G is a normal subgroup of G iff $gNg^{-1} = N \ \forall \ g \in G$

Proof:

If $gNg^{-1} = N \ \forall \ g \in G$.

Certainly $gNg^{-1} \subset N$, so N is a normal in G

Suppose that N is normal in G

Thus if $g \in G$, $gNg^{-1} \subset N$ &

$g^{-1}Ng = g^{-1}N(g^{-1})^{-1} \subset N$

Now, $g^{-1}Ng \subset N$

$N = g(g^{-1}Ng)g^{-1} \subset gNg^{-1} \subset N$.

whence $N = gNg^{-1}$

In order to avoid a point of confusion

Here let us stress that lemma does not say that for every $n \in N$ & every $g \in G$, $gng^{-1} = n$.

~~Then~~ the group G to be S_3 & N be the subgroup $\{e, \psi, \psi^2\}$.

If we compute $\phi N \phi^{-1}$ we obtain $\{e, \phi\psi, \phi^{-1} \cdot \phi\psi^{-1}, \phi^{-1}\}$

Then $\{e, \psi^2, \psi\}$

Yet $\phi\psi\phi^{-1} \neq \psi$.

All we require is that set of centers gNg^{-1} be the same as the set of elements N.

The equality of left cosets and right cosets.

Hence the proof/.

VVI **Lemma : 3.** (A5)

If G is a finite group and N is a normal subgroup of G. Then

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

Proof:

Let G be the group of integers under addition

Let N be the set of all multiples of 3.

∵ The operation in G is addition, we shall write the cosets of N in G as $N+a$ rather than as Na.

Consider the three cosets, N, $N+1$, $N+2$

We claim that these are all the cosets of N in G.

For given $a \in G$, $a = 3b + c$, where $b \in G$ & $c = 0, 1$ (or) 2 (c is the remainder of 'a' on division 3)

Thus $N + a = N + 3b + c$

$$= (N + 3b) + c$$

$$= N + c$$

$\because 3b \in N$.

Thus every coset is as one of $N, N+1$ (or) $N+2$ & $\frac{G}{N} = \{N, N+1, N+2\}$.

Our formula $NaNb = Nab$ translates into : $(N+1) + (N+2) = N+3 \in N$

$\because 3 \in N$

$(N+2) + (N+2) = N+4 = N+1$ and so on.

Without being specific one feels that $\frac{G}{N}$ is closely related to the integers mod 3. under addition.

Clearly, for any integers n in which case the factor group should suggest a relation to the integers mod n under addition.

Hence the Proof /.

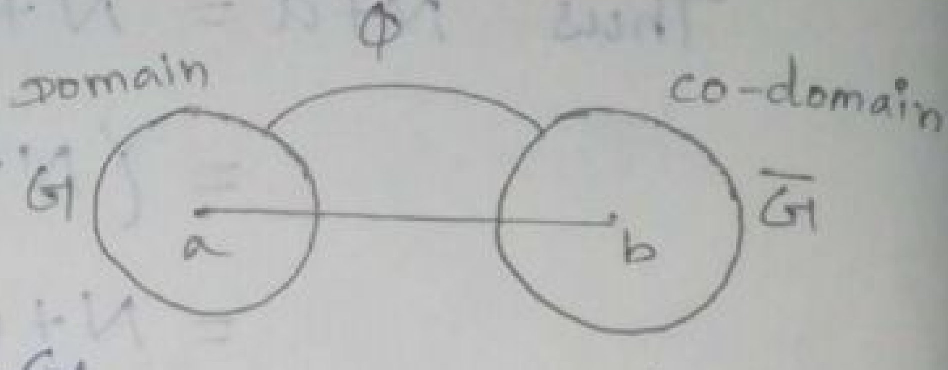
Explain.

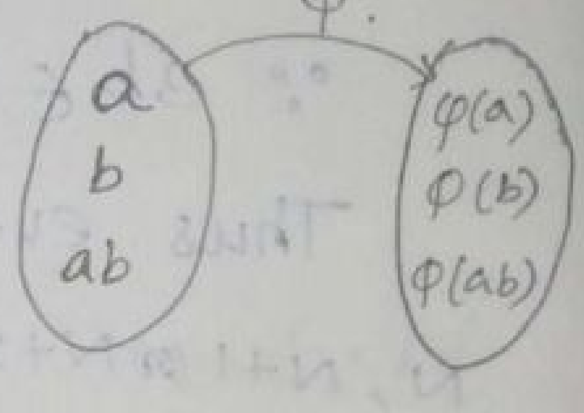
Homomorphism. (ϕ)

(1) Let G + $\bar{G}$ be two groups and $\varphi : G \to \bar{G}$ be a function

Then,

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





Example

Homomorphism

1. $\varphi(x) = x$

L.H.S $\Rightarrow \varphi(ab) = ab$

R.H.S $\Rightarrow \varphi(a)\varphi(b) = ab$

Not Homomorphism.

$\varphi(x) = 2x$

L.H.S $\Rightarrow \varphi(ab) = 2ab$

R.H.S $\Rightarrow \varphi(a)\varphi(b) = 2a \cdot 2b$

$= 4ab$.

It is not homomorphism.

2. $\varphi(x) = e^x$

~~L.H.S $\Rightarrow \varphi(ab) = e^{ab}$~~

$\varphi(a+b) = \varphi(a) + \varphi(b)$

L.H.S $\Rightarrow \varphi(a+b) = e^{a+b}$

$= e^a e^b$

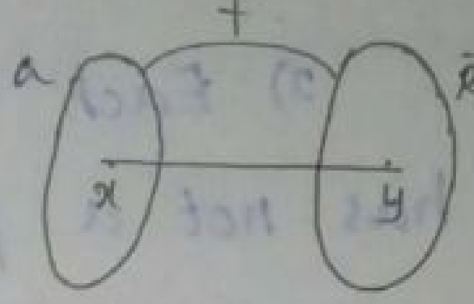
R.H.S $\Rightarrow$ $\varphi(ab) =$ $\varphi(a)\varphi(b) = e^a e^b$

It is hommorphism.

1. $\varphi : (G, \cdot) \to (G, \cdot) \Rightarrow \varphi(ab) = \varphi(a)\varphi(b)$.

2. $\varphi : (G, +) \to (G, +) \Rightarrow \varphi(a+b) = \varphi(a) + \varphi(b)$.

- **1-1 mapping**.



If consider a function

$f : a \to \bar{R}$

If $x \neq y \Rightarrow f(x) \neq f(y)$

(or)

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

Ex-1

$f(x) = x$.

$f(1) = 1$
$f(2) = 2$
$f(3) = 3$

so 1-1 is form of satisfied

Ex-2

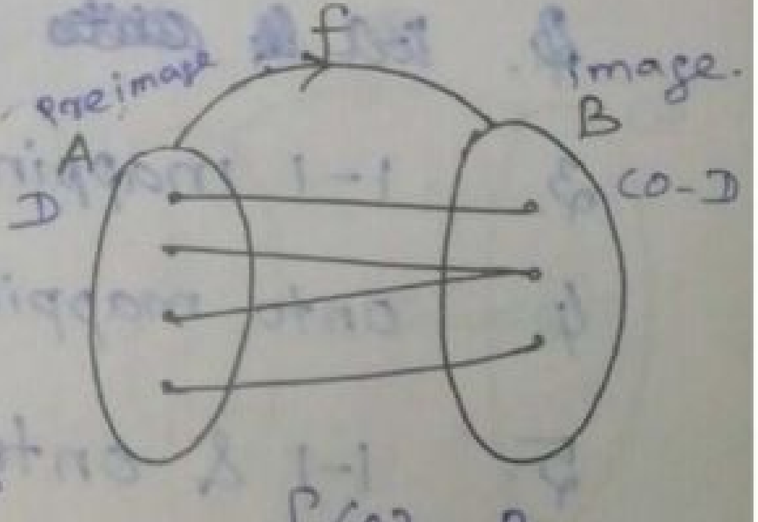
$f(x) = x^2$

$x^2 = 1$

$x = \pm 1$.

so 1-1 is form of not satisfied.

Onto mapping.



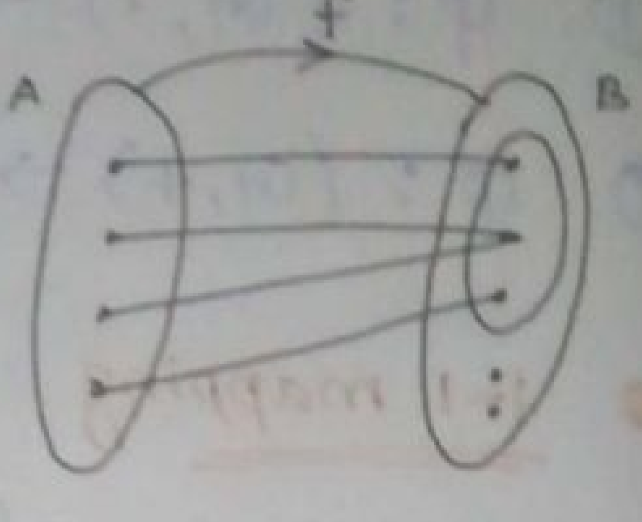
* Each element in B has a pre image in A

* ~~Each element in A has a pre image in B.~~

f(A) = B

* Consider function in has not extra element in B.

Into



1) Each element in B has not a preimage in A

2) Each element in A has not a preimage in B

3) consider a function in has extra element in B

$f(A) \neq B$.

Note1:-

1. Homomorphism & 1-1 ⇒ Isomorphism.

2. Homomorphism & 1-1 & onto (or) Isomorphism & onto ⇒ Isomorphic ($\cong$)

~~4. [illegible] ⇒~~

3. 1-1 mapping ⇒ Injective

4. onto mapping ⇒ Bijective

5. 1-1 & onto ⇒ Bijective.

Note 2:- (Addition).

1. Homomorphism + 1-1 ⇒ monomorphism

2. Homomorphism + onto ⇒ Epimorphism

Automorphism & Inner Automorphism.

1. Automorphism.

Consider the 3 condition in domain and co-domain is also same mapping.

2. Inner Automorphism :-

Consider the 3 condition in has changed are domain and co-domain in a mapping.

Then,

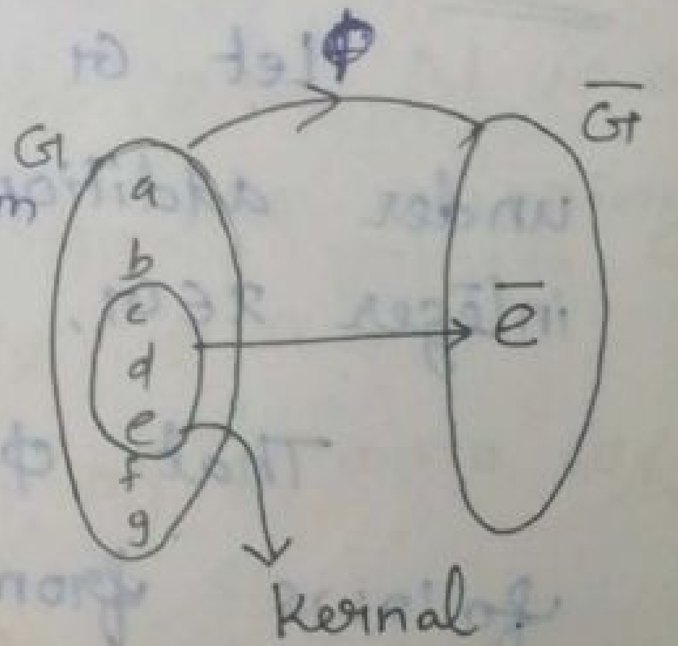
Ex. $T_g : G \to G$ by $x T_y = g^{-1} x y \ \forall x \in G$

so is called Automorphism & Inner Automorphism

Kernal.

$\Rightarrow G \to \overline{G}$ is homomorphism

$k = \{ x \in G : \phi(x) = \overline{e} \}$.



Defn:-

A mapping ϕ from a group G into a group $\bar{G}$ is said to be a homomorphism if $\forall$ $a, b \in G$,

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

Then $\phi(ab)$ the product of ab is completed in G using the product of element of G in the term of $\phi(a) \phi(b)$. the product is that of element in $\bar{G}$.

Ex 1:-

$\phi(x) = e$ all $x \in G$. This is trivially a homomorphism. Then $\phi(x) = x$ for every $x \in G$ is a homomorphism

Ex 2:-

Let G be the group of integers under addition and Let $\bar{G} = G$. For the integer $x \in G$, define ϕ by $\phi(x) = 2x$

That ϕ is a homomorphism then follows from

$$\phi(x+y) = 2(x+y)$$
$$= 2x + 2y$$
$$= \phi(x) + \phi(y).$$

Ex-3:

Let G be the group of positive real numbers under multiplication and let $\bar{G}$ be the group of all real numbers and addition. Define $\phi : G \to \bar{G}$ by $\phi(x) = \log_{10} x$. Thus $\phi(xy) = \log_{10}(xy)$

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

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

$\therefore$ The operation on the right side in $\bar{G}$ is infact addition. Thus ϕ is a homomorphism of G into $\bar{G}$ not only ϕ is a homomorphism but, in addition it is 1-1 & onto.

Lemma 1 :-

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

Proof :- In actuality, there is nothing to prove, for we already have proved. Then ϕ is onto is a trivial. for every element $x \in G/N$ is of the form.

$x = Ny$, $y \in G$ so $x = \phi(y)$.

To verify the multiplicative property required in order that ϕ be a homomorphism. Note that $x, y \in G$

$\phi(xy) = Nxy$

$= NxNy$

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

Then homomorphism need not be 1-1. but there is a certain uniformity in this process of derivating from 1-1 mapping

Hence the proof //.

Defn :- 2

If ϕ is a homomorphism of G into $\bar{G}$ the kernal of ϕ, k_ϕ is defined by $k_\phi = \{x \in G \mid \phi(x) = \bar{e}$, $\bar{e} = 1$ identity element of $\bar{G}\}$.

Before inverticating any propertes of k_ϕ it is advisable to establish that as a set k_ϕ is ~~not~~ empty.

5m U.G

(x) Lemma 2:

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

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

(ii) $\phi(x^{-1}) = \phi(x)^{-1} \ \forall \ x \in G$

Proof:

To prove: (i) The calculate $\phi(x)\bar{e} = \phi(x) = \phi(xe) = \phi(x)\phi(e)$, so the cancellation property in $\bar{G}$. We have that $\phi(e) = \bar{e}$

To establish (2), one note that $\bar{e} = \phi(e) = \phi(xx^{-1}) = \phi(x)\phi(x^{-1})$. So by the very definition of $\phi(x)^{-1}$ in $\bar{G}$, we obtain the result that $\phi(x^{-1}) = \phi(x)^{-1}$

Hence the proof.

Lemma 3:-

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

Proof:-

K is a subgroup of G

Show that K is closed under multiplication and has inverses in it for every element belonging to k.

If $x, y \in k$, then $\phi(x) = \bar{e}$, $\phi(y) = \bar{e}$ where $\bar{e}$ is the identity element of $\bar{G}$ and so, $\phi(xy) = \phi(x)\phi(y)$

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

$= \bar{e}$, whence $xy \in k$.

Also if $x \in k$, $\phi(x) = \bar{e}$.

To prove the normality of k one must establish that for any $g \in G$, $k \in k$, $gkg^{-1} \in k$.

Then prove that $\phi(gkg^{-1}) = \bar{e}$ whenever $\phi(k) = \bar{e}$.

But $\phi(gkg^{-1}) = \phi(g)\phi(k)\phi(g^{-1})$

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

$$= \phi(g)\phi(g^{-1})$$

$$= \bar{e}.$$

Hence the proof //.

Defn 3:

A homomorphism $\phi : G \xrightarrow{into} \overline{G}$ is said to be an isomorphism if ϕ is one-to-one.

Defn 4:

Two groups G, G^* are said to be Isomorphic if there is an Isomorphism of G onto G^*. In this case we write $G \approx G^*$

We leave to the reader to verify the following three facts.

i) $G \approx G$

ii) $G \approx G^* \Rightarrow G^* \approx G$

iii) $G \approx G^*$, $G^* \approx G^{**} \Rightarrow G \approx G^{**}$

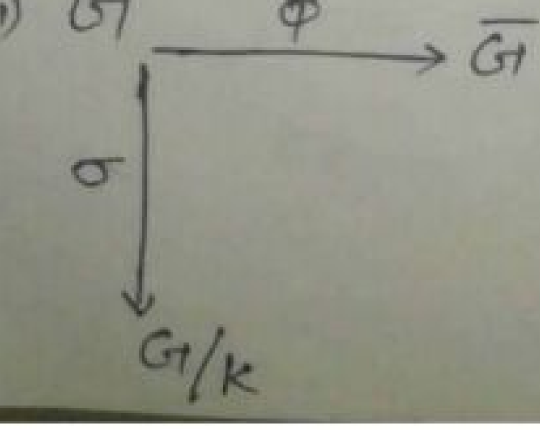
(*) 10m VVI

Theorem 1:

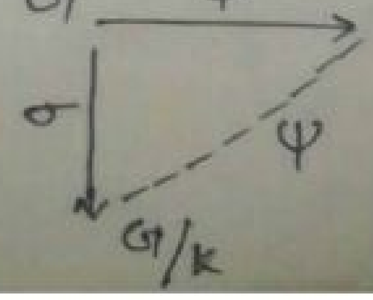
Let ϕ be a homomorphism of G onto $\overline{G}$ with kernal K. Then $G/K \approx \overline{G}$

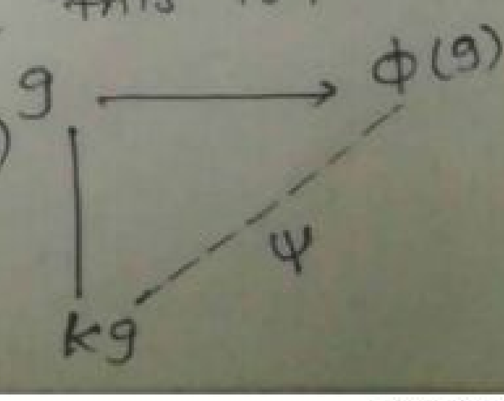
Proof:

Consider the diagram

(i) 

where $\sigma(g) = kg$ we should like to complete this to.

(ii) 

iii) 

with this preamble we formly define the mapping $\psi : G/k \rightarrow \bar{G}$ by if $x \in G/k$, $x = kg$ then $\psi(x) = \phi(g)$

If $x \in G/k$ it can be written as kg in several ways $(kg = k\,kg\ ,\ k \in k)$.

But $x = kg = kg'$, $g, g' \in G$

Then one hand $\psi(x) = \phi(g)$ and other $\psi(x) = \phi(g')$

For the mapping ψ to makes sense it had beffer be true that

$\phi(g) = \phi(kg^{-1}) = \phi(k)\phi(g^{-1})$

$= \bar{e}\,\phi(g^{-1}) = \phi(g^{-1})$

$\because k \in k$, the kernal of ϕ. We next determine that ψ is onto for if $\bar{x} \in \bar{G}$, $\bar{x} = \phi(g)$, $g \in G$ $(\because \phi$ is onto$)$.

so, $\bar{x} = \phi(g) = \psi(kg)$.

If $k, y \in G/k$, $x = kg$, $y = kf$, $g, f \in G$

Then $xy = kgkf$

$= kgf$

so that,

$\psi(xy) = \psi(gf) = \phi(g)\,\phi(f)$

∵ ϕ is a homomorphism of G onto $\bar{G}$

But $\psi(x) = \psi(kg) = \phi(g)$

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

So we that $\psi(xy) = \psi(x)\psi(y)$ & ψ is a homomorphism of G/k onto $\bar{G}$.

To prove that ψ is an Isomorphism of G/k onto $\bar{G}$ all that remains is to element of G/k is $k = k_e$, we must so that if $\psi(kg) = \bar{e}$. Then the kernal of ψ is the unit element of G/k.

Then $kg = k_e = k$ for $\bar{e} = \psi(kg) = \phi(g)$,

so that $\phi(g) = \bar{e}$, whence g is in the kernal of ϕ, namely k. But then

$kg = k$

∴ k is a subgroup of G

All the pieces have been put together we have exhibited a one-to-one homomorphism of G/k onto $\bar{G}$.

Thus $G/k \cong \bar{G}$

Hence the proof.

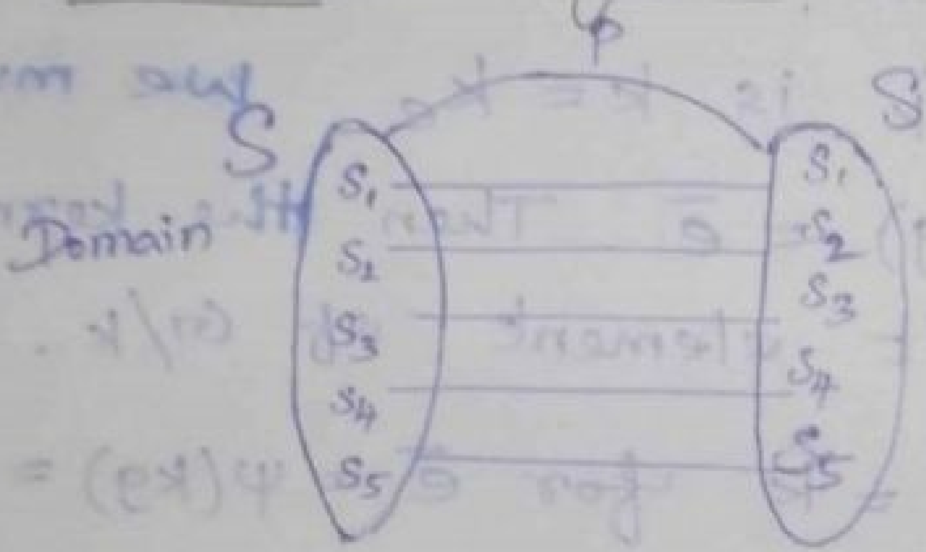
Gayley's Theorem. (Symmetric Group) A(S)

(i) Every group is isomorphic to a subgroup of A(S) for some appropriate S.

(ii) Every finite group is Isomorphic to a permutation group.

Ex:1

Permutation group



Let S be a finite set. If a map $p: S \to S$ is 1-1 and onto then p is called permutation group.

Defn: Gayley's theorem:

The group first arose in subgroup of S_n. $S_n = A(S)$ when S is finite set with n elements that group could be realised as a subgroup of A(S) for some S. Our concern in this section will be with a presentation is called Gayley's theorem.

Theorem 1 (★) 5m (★) V.VI.

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

Proof:-

Let G be a group. for the set S we will use the elements of G.

ie). put $S = G$ if $g \in G$, define $\tau_g : S = G \to S = G$ by $x\tau_g = xg \ \forall \ x \in G$.

If $y \in G$, then $y = (yg^{-1})g = (yg^{-1})\tau_g$ so that τ_g maps S onto itself. Moreover τ_g is 1-1 for if $x, y \in S$ & $x\tau_g = y\tau_g$ then $xg = yg$ which by the cancellation property of groups.

$\Rightarrow \boxed{x = y}$

We have proved that for every $g \in G$; $\tau_g \in A(S)$.

Hence the proof //

Theorem 2:-

If G is a group, H a subgroup of G and S is the set of all right cosets of X in G, then there is a homomorphism θ of G into $A(S)$ & the kernal of θ is the largest normal subgroup of G which is contained in H.

Proof :-

If H is subgroup of G and other than (e) in it, then θ must be an isomorphism of G into A(S).

Suppose that G has a subgroup of H, then the index i(H), the number of right cosets of H in G, satisfies $i(H)! < o(G)$

Let S be the set of all right cosets of H in G.

Hence the proof //.

Lemma 1 :-

If G is a finite group and $H \neq G$ is a subgroup of G such that $o(G) \nmid i(H)!$ then H must contain non trivial normal subgroup of G. in particular, G cannot to simple

Proof :- Let G has a subgroup of H of order 36

Then, $i(H) = 4$, $4! = 24 < 36 = o(G)$

so that in H there must be a normal subgroup $N \neq \{e\}$ of G of order of 9

i.e., of order 3 (or) 9.

Let G be a group of order 99 and suppose that H is a subgroup of G of order 11.

Then $i(H) = 9$ &

∴ 99 ∤ 9! there is a nontrivial normal subgroup $N \neq (e)$ of G in H.

∵ H is of order 11 which is a prime, its only subgroup other than (e) is itself implying that $N = H$

i.e., H itself is a normal subgroup of G.

Hence the proof //.

Permutation group (Symmetric group S_n)

1). Let S be a finite set. If a map $p: S \to S$ is 1-1 and onto then p is called permutation.

2). Set S_n of all permutation is group under permutation product and it is called symmetric group of deg n &

$O(S_n) = n!$.

3). $n \leq 2 \Rightarrow S_n$ is abelian (S_1 & S_2 are Abelian group) ; $n \geq 3 \Rightarrow S_n$ is not Abelian group.

4). permutation $\begin{pmatrix} a_1, a_2, \dots, a_n \\ a_2, a_3, \dots, a_1 \end{pmatrix} = (a_1, a_2, \dots a_n)$ is called cycle of length n (n-cycles).

② - Em

$S = \{1, 2, 3\}$, $O(S_n) = n!$.

$S_3 = 3!$

$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$.

$\Rightarrow S_3 = \{1, (1\,2\,3)\,(2\,3)\,(1\,3)\,(1\,3\,2)\,(1\,2)\}$

$\Rightarrow S_3$ is symmetric group of deg 3 &

$O(S_3) = 3!$, then $O(S_3) = 3! \Rightarrow 6$

$\Rightarrow S_3$ is non A.G of order 6.

5). If the length of cycle is 2 (2-cycle) then it is transposition (own inverse).

6). Disjoint cycles → cycles have number of elements in common.

Ex.

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

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

$= (1\ 2\ 3\ 4\ 5)(6)(7)(8\ 9)$ is called disjoint cycles.

$\Rightarrow (1\ 2\ 3\ 4\ 5)(8\ 9) = 2$

$\Rightarrow (1\ 2)(1\ 3)(1\ 4)(1\ 5)(8\ 9)$ is called odd permutation. $= 5$

length of cycle are $(2, 5)$.

~~Order~~ of permutation = Lcm of 2×5
$= 10$.

7) (i) Even permutation ⇒ permutation = product of even number of transposition

(ii) Odd permutation ⇒ permutation = product of odd number of transposition.

(i) Even per. is Even
(ii) Odd per. is Even
(iii) Even & odd per. is odd

} • product of even and odd transposition

Ex.

(i) Even Permutation.

P(1 2 3 4 5) ⇒ (1 2) (1 3) (1 4) (1 5) is called even permutation. (4)

(ii) odd Permutation

P(1 2 3 4) ⇒ (1 2) (1 3) (1 4) is called odd permutation. (3)

8). Identity permutation is even.

$\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$ ⇒ (1) = (1 2)(2 1) (Any cycle of length is identity per.)

9). No. of even per. = No. of odd per. = $\frac{n!}{2}$.
(An). (No symbol)

10). Conjugate per. → $C^{-1} P_1 C = P_2$

Two per. in S_n are conjugate iff there have same cyclic decomposition.

11). Any cycle of length n is expressed as product of (n-1) terms.

12). P = (1, 2 ... n-1) ⇒ P^{-1} = (n, n-1 ... , 2, 1)

$P\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \Rightarrow P^{-1}\begin{pmatrix} 1 & 3 & 2 \\ 1 & 2 & 3 \end{pmatrix}$

13). Order of permutation = LCM of length of cycles of a permutation.

Defn.

A permutation $\theta \in S_n$ is said to be an even permutation if it can be represented as a product of an even number of transposition. The definition given just insists that θ have one representation as product of an even number of transpositions is called permutation group (or) symmetric group (S_n).

1). The product of two even permutations is an even per.

(2). The product of an even per. and an odd one is ~~odd~~ odd the product of an odd and even per.

3). The product of two odd per. is an even per.

Lemma:

Every permutation is the product of its cycles.

Proof: Let θ be the permutation. Then its cycles are of the form $(s, s\theta, s\theta^{l-1})$

By the multiplication of cycles as defined above and since the cycles of θ

are disjoint, the image of $s' \in S$ which is $s'\theta$ is the same as the image of s' under the product, ψ of all the distinct cycles of θ.

So, $\theta \cdot \psi$ have the same effect on every element of S;

Hence $\theta = \psi$.

If the remarks above are still not transparent at their point, find its cycles. take their product is usually stated in the form every permutation can be uniquely expressed as a product of disjoint cycles.

Consider the m-cycle $(1, 2, \ldots, m) \ldots (a_1, a_m)$. A simple computation show that $(1, 2, \ldots, m) = (1,2)(1,3) \ldots (1,m)$

Then m-cycle,

$$(a_1, a_2, \ldots, a_m) = (a_1, a_2)(a_1, a_3), \ldots (a_1, a_m)$$

This discomposition is not unique. then the product of 2-cycles in more than one-way.

For $(1,2,3) = (1,2)(1,3) = (3,1)(3,2)$.

Since, Every permutation is a product of disjoint cycles and every cycle is a product of 2-cycles.

Hence the Proof //

Another Counting Principle :-

Defn:- 1

If $a, b \in G$, then b is said to be a conjugate of a in G if there exists an element $c \in G \ni: b = c^{-1}ac$. we shall write for this $a \sim b$ and shall refer to this relation as conjugacy.

Defn 2.

If $a \in G$, then $N(a)$, the normalizer of a in G, is the set $N(a) = \{x \in G / xa = ax\}$

$N(a)$ consists of precisely those elements in G which commute with a.

Lemma 1 :-

Conjugacy is an equivalence relation on G.

Proof

As usual, in order to establish this we must

1. $a \sim a$
2. $a \sim b \Rightarrow b \sim a$.
3. $a \sim b$, $b \sim c \Rightarrow a \sim c$ $\forall a, b, c$ in G

($\sim$ - similar to.)

we prove each of these in turn.

1. since $a = e^{-1}ae$, $a \sim a$ with $c = e$ serving as the c in the definition

of congugacy.

2). If $a \sim b$, then $b = x^{-1} a x$ for some $x \in G$.

Hence $a = (x^{-1})^{-1} b (x^{-1})$ &

$\because y = x^{-1} \in G$ &

$a = y^{-1}$ by $b \sim a$ as follows.

3). suppose that $a \sim b$ & $b \sim c$ where $a, b, c \in G$

Then $b = x^{-1} a x$, $c = y^{-1}$ by some $x, y \in G$.

For $a \in G$.

Let $C(a) = \{x \in G \mid a \sim x\}$. $C(a)$ the equivalence class of a in G under our relation. is usually conjugate class of a in G

Hence the proof //.

Theorem 1:

If G is a finite group then $C_a = o(G) / o(N(a))$; in other words the member of elements conjugate to a in G is the index of the normalizer of a in G.

let the conjugate class of a in G, C(a), consist exactly of all the element $x^{-1}ax$ as x ranges over in G

Then C_a measures the number of distincts $x^{-1}ax$.

Then two elements in the same right cosets of N(a) in G in the same conjugate of a whereas two elements in different right cosets of N(a) in G.

Suppose that $x, y \in G$ are in the same right cosets of N(a) in G.

Thus, $y = n\{x\}$, where $n \in N(a)$ and so $na = an$.

$\therefore y^{-1} = (nx)^{-1}$

$= x^{-1}n^{-1}$

$y^{-1}ay = x^{-1}n^{-1}$

$anx = x^{-1}n^{-1}$, $nax = x^{-1}ax$, whence x & y result in the same conjugate of a.

ie), $o(G) = \sum \frac{o(G)}{o(N(a))}$.

Where this sum runs over one element a in each conjugate class.

Hence the proof.

Corollary : 1

If $o(G) = p^2$, where p is a prime number, then G is a abelian.

Proof:

Let p is a prime number.

Show that $Z(G) = G$.

At any rate of $Z(G) \neq (e)$ is a subgroup of G.

So that $o(Z(G)) = p$ (or) p^2

If $o(Z(G)) = p^2$.

Then $Z(G) = G$.

~~Thus~~

Suppose that $o(Z(G)) = p$.

Let $a \in G$, $a \notin Z(G)$

Thus, $N(a)$ is a subgroup of G.

$Z(G) \subset N(a)$, $a \in N(a)$

Then $o(N(a)) / o(G) = p^2$

Thus $o(Z(G)) = p$ is an actual passibility

Hence the proof //.

Sylow's Theorem.

Defn : 1. P- sylow subgroup.

Let p be a prime number. If $p^n / o(G)$ and $p^{n+1} \nmid o(G)$, then G has a subgroup of order p^n. Then subgroup is called p-sylow subgroup of G.

(i). First type of sylows theorem :-

Let $p^\alpha / o(G) \Rightarrow G$ has a subgroup of order p^α. Then $p^\alpha \rightarrow 0 \leq \alpha \leq n$. (sylows theorem is partial converse of lagrange theorem). If G is abelian, then there is unique subgroup of G with order p^α.

Ex : 1

p- sylows subgroup in G.

$5/20$, $5^{+1} \nmid 20$ $5^{+1} \nmid 20$.

(ii) Second type of sylow's theorem :-

$p^n / o(G)$ & $p^{n+1} \nmid o(G)$

$\Rightarrow$ ~~Any~~ two subgroups of order p^n are conjugate. (or)

Any two p-sylow subgroup are conjugate.

(iii) Third type of sylow's theorem :-

Number of p-sylow subgroup in G is the form $\boxed{1+kp}$ for some non negative integer k.

Let p be a p-sylow subgroup in G. Then number of p-sylow subgroup in G.

$G = o(G) / o(N(p)) = 1+kp$.

then number of p-sylow subgroups in $G / o(G)$ & $N(N(p)) = N(p)$

Conjugate class (or) Equivalance class :-

(i) Let $a, b \in G$, If there is $c \in G$ such that $b = c^{-1}ac$. then b is conjugate of a & we write $a \sim b$. This is called conjugate relation.

(ii) Conjugacy is an equivalance relation.

(iii) Let $a \in G$.

Then $C(a) = \{x \in G : a \sim x\}$

$= \{y^{-1}ay : y \in G\}$ is

conjugate class of a.

If G is infinite then number of distinct elements on $C(a)$ is denoted by C_a.

Here $C_a = \frac{o(G)}{o(N(a))}$ (or) Number of elements conjugate to a in G

(ie) G = Index of normalizer of a in G.

(iv) Let $G = C(a_1) \cup C(a_2) \cup \ldots \cup C(a_k)$.

$\Rightarrow o(G) = \Sigma C_a$.

Conjugate Subgroup :-

Let A & B be two subgroup of G, $A = gBg^{-1}$ $\forall$ $g \in G$

$\Rightarrow$ A & B are called conjugate subgroup in G.

class equation :-

(i) Let $o(G) = \Sigma \frac{o(G)}{o(N(a))}$, where

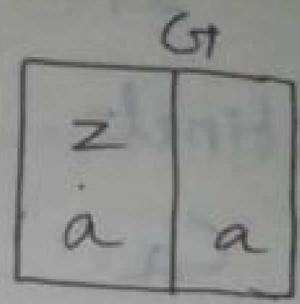
Sum runs over one element a in which conjugate class.

(ii) ~~Let~~ $o(G) = o(Z) + \sum_{N(a) \neq G} \frac{o(G)}{o(N(a))}$.

(iii) No. of conjugate class in S_n = partition function value.

If $P(n) = n_1 + n_2 + \ldots + n_r$. $1 < n_1 \leq n_2 \ldots \leq n_r$

Class equation



$$o(G) = \sum \frac{o(G)}{o(N(a))}$$

$$= \sum_{a \in z} \frac{o(G)}{o(N(a))} + \sum_{a \notin z} \frac{o(G)}{o(N(a))}$$

$$= \sum_{a \in z} \frac{o(G)}{o(G)} + \sum_{N(a) \notin G} \frac{o(G)}{o(N(a))}$$

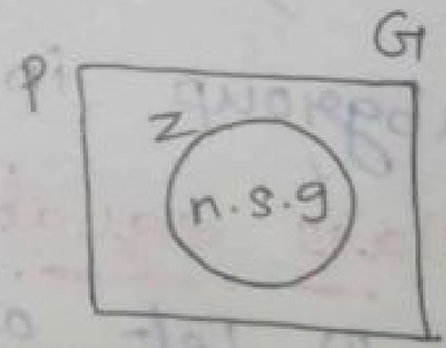
$$= \sum_{a \in z} (1) + \sum_{N(a) \neq G} \frac{o(G)}{o(N(a))}$$

$$= o(G) + \sum_{N(a) \neq G} \frac{o(G)}{o(N(a))}$$

Note :-

$a \in z$ iff $N(a) = G$

$a \notin z$ iff $N(a) \neq G$



(a). $o(G) = p \Rightarrow G$ is cyclic abelian.

(b). $o(G) = 2p \Rightarrow G$ has normal subgroup of order p.

Ex : $o(G) = 10$ $(2 \times 5 = 10)$.

(c). $o(G) = p^2 \Rightarrow G$ is abelian, G has normal subgroup of order p. and this normal subgroup is in centre of z.

(d). $o(G) = pq \ (p > q)$.

(i) G has only one normal subgroup of order q.

(ii) $p / q-1 \ (q \equiv 1 \mod p) \Rightarrow$ normal subgroup of order q.

(iii) $p \nmid q-1 \ (q \not\equiv 1 \mod p) \Rightarrow$ G is cyclic and abelian.

Ex: 2

$o(G) = 30 = 2 \times 3 \times 5$. then find possible sylow subgroup of G.

case (i)

2-sylow subgroup.

Number of 2-sylow subgroup of G $= 1+2k$.

$\Rightarrow 1+2k, \ 2 \times 3 \times 5$

$\Rightarrow 1+2k, \ 3 * 5 \Rightarrow 1+2k / 15$

$\Rightarrow k = 0, 1, 2, 7$.

∴ Number of 2-sylow subgroup $= 1, 3, 5, 15$.

Case (ii)

3-sylow subgroup.

Number of 3-sylow subgroup of G $= 1+3k$.

Now, $\Rightarrow 1+3k / 2 \times 3 \times 5$.

$\Rightarrow 1+3k / 2 \times 5 \Rightarrow 1+3k / 10 \Rightarrow \boxed{k = 0, 3}$

$\Rightarrow$ Number of 3-Sylow subgroup $= 1$ (or) 10

Every 3-sylow subgroup is normal in G.

Case (iii)

Every 5-sylow subgroup is normal in G

This is G has normal subgroup of order 15.

vvI Corollary-1.

If $p^m / o(G)$, $p^{m+1} \nmid o(G)$; then G has a subgroup of order p^m.

1st part in 2-sylow :-

A subgroup of G of order of p^m where $p^m / o(G)$ but $p^{m+1} \nmid o(G)$ is called a p-sylow subgroup of G

The corollary above asserts that a finite group has p-sylow subgroups for every prime p dividing its order The conjugate of a p-sylow subgroup is a p-sylow subgroup.

We shall also get some information on how many p-sylow subgroups there are in G for a given prime p.

ie). If we know that G possesses a subgroup of order p^m. when $p^m / o(G)$ but $p^{m+1} \nmid o(G)$, then We know that G has a subgroup of order p^m for any α such that $p^\alpha / o(G)$

This result states that any group of order p^m, p a prime has subgroup of order p^α for any $0 \leq \alpha \leq m$.

For us to prove the exitence of p-sylow subgroups of G, for every prime p. dividing the order of G

ie). $p / o(G)$ //

II - Second proof of sylow's theorem.

We prove by induction on the order of the group G, that for every prime p dividing the order of G. G has a p-sylow subgroups.

If the order of the group is 2. the only relavant prime is 2 and the group certainly has a subgroup of order 2

So we suppose the result to be correct forall groups of order less than, that $p^m / o(G)$, $p^{m+1} \not/ o(G)$, where p is a prime, ~~$m \geq 1$~~. If $p^m / o(H)$ forany subgroup H of G where $H \neq G$ then by the induction hypothesis H would have a subgroup T of order p^m.

ie), $o(G) = \sum \frac{o(G)}{o(N(a))}$, where this sum runs over one element a from each conjugate class. We separate the sum into this gives,

$$o(G) = z + \sum_{a \notin G} \frac{o(G)}{o(N(a))}, \text{ where}$$

$z = o(z)$. Now invoke the reduction we have made that $p^m \nmid o(H)$ for any subgroup $H \neq G$ of G the subgroups $N(a)$ for $a \notin z$.

Since in this case $p^m / o(G)$ and $p^m \nmid o(N(a))$

We must have. $\frac{p}{o(G)/o(N(a))}$

Restarting the result $\frac{p}{o(G)/o(N(a))}$ for every $a \in G$.

Where $a \notin G$. Then $\frac{p}{\sum_{a \notin z} \frac{o(G)}{o(N(a))}}$.

Hence we can form the quotient group $\bar{G} = G/B$.

Then $o(G)/o(B) = o(G)/p$ hence is certainely less than $o(G)$. we have

$p^{m-1} / o(\bar{G})$, but $p^m \nmid o(\bar{G})$.

(ie) $p^{m-1} = o(\bar{P}) = \frac{o(P)}{o(B)} = \frac{o(P)}{p}$.

This results in $o(P) = p^m$

$\therefore$ P is the required p-sylow subgroup of G. we have finished the second proof of sylow's theorem.

III rd proof of sylow's theorem :-

We will first show that the symmetric group S_{p^r}, P a prime, all have p-sylow subgroups.

Then G is contained in M & m has a p-sylow subgroup, then G has a p-sylow subgroup.

So we get down to our power of prime p exactly divides $(p^k)!$

But, it will be clearer and will suffic to do it only for $(p^k)!$

Let n(k) be defined by $p^{n(k)} / p^{(k)}$!.

~~But~~ $p^{n(k)+1} \nmid (p^k)!$.

Theorem : 1

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

Proof:-

Let A, B be subgroups of G, each of order p^n.

Show that $A = gBg^{-1}$ $\forall g \in G$

Decompose G into double cosets of A & B

$G = \bigcup A x B$

Now,

$$o(AxB) = \frac{o(A)\, o(B)}{o(A \cap xBx^{-1})}$$

If $A \neq xBx^{-1}$ for every $x \in G$ the $o(A \cap xBx^{-1}) = p^m$, where $m < n$.

Thus $o(AxB) = \frac{o(A)\, o(B)}{p^m}$

$$= \frac{p^n p^n}{p^m}$$

$$= \frac{p^{2n}}{p^m}$$

$o(AxB) = p^{2n-m}$ & $2n-m \geq n+1$.

~~And~~

$\therefore p^{n+1} / o(AxB)$ for every x and since

$o(G) = \Sigma o(AxB)$.

~~Hence the theorem~~ //

we would get the contradiction

$p^{n+1} / o(G)$

Thus $A = gBg^{-1}$ for some $g \in G$.

Hence the theorem //

<u>Theorem 2</u>

The number of p-sylow subgroup in G, for a given prime is of the form $1+kp$.

<u>Proof</u> :-

~~Let~~ p be a p-sylow subgroup of G

We decompose G into double cosets of P & P.

Thus $G = \bigcup PxP$

Then $o(PxP) = \dfrac{o(P)^2}{o(P \cap xPx^{-1})}$

Thus if $P \cap xPx^{-1} \neq P$

~~Then $p^{n+1} / o(PxP)$~~. where $p^n = o(P)$.

If $x \notin N(P)$ then $p^{n+1} / o(PxP)$.

Also, if $x \in N(P)$, then $PxP = PP(x)$

$= P^2x$

$= Px$.

So $o(PxP) = p^n$ in this case

Now $o(G) = \sum_{x \in N(P)} o(PxP) + \sum_{x \notin N(P)} o(PxP)$.

where ~~its some~~ each sum runs over one element from each double coset

However, if $x \in N(P)$.

$\because PxP = Px$, the first sum is $\sum_{x \in N(P)} o(Px)$ over the distinct cosets of P in $N(P)$.

Hence $p^{n+1} / \sum_{x \notin N(P)} o(PxP)$.

Then we write this second sum as $\sum_{x \notin N(P)} o(PxP) = p^{n+1} u$

$\therefore o(G) = o(N(P)) + p^{n+1} u$, so

$$o(G) = o(N(P)) \left[1 + \frac{p^{n+1} u}{o(N(P))} \right]$$

$$\Rightarrow \frac{o(G)}{o(N(P))} = 1 + \frac{p^{n+1} u}{o(N(P))}$$

Now $o(N(P)) / o(G)$

$\because P$ is a subgroup of G.

Hence $p^{n+1}u \,/\, o(N(P))$ is an integer.

Also, since $p^{n+1} \nmid o(G)$, p^{n+1} cannot divide $o(N(P))$.

We have, $\frac{o(G)}{o(N(P))} = 1 + kp$.

Then $\frac{o(G)}{o(N(P))}$ is the number of p-sylow subgroup in G.

Hence the theorem //

Unit - II

Ring Theory. (8)

Let R be a non-empty set and + & . be two binamary operation consider the following area,

I. $(R,+)$ is abelian group.

(a). $a,b \in R \Rightarrow a+b \in R$.

(b). $a,b,c \in R \Rightarrow (a+b)+c = a+(b+c)$.

(c). $0 \in R \ni: a+0 = 0+a = a \ \forall \ a \in R$.

(d). To each $a \in R$ there is $-a \in R \ni:$

$$a+(-a) = (-a)+a = 0.$$

(e). $a,b \in R \Rightarrow a+b = b+a$.

unit devision

II. $(R,\cdot)$ is semi group.

(a). $a,b \in R \Rightarrow a\cdot b \in R$.

(b). $a,b,c \in R \Rightarrow (a\cdot b)\cdot c = a\cdot(b\cdot c)$.

III. Distributive law.

(a). $a,b,c \in R \Rightarrow a\cdot(b+c) = a\cdot b + a\cdot c$ (LDL)

(b). $a,b,c \in R \Rightarrow (b+c)\cdot a = b\cdot a + c\cdot a$ (RDL)

$(R,+,\cdot)$ is called Ring.

Sub ring :-

Let S be a non-empty subset of (R,+,·). If (S,+,·) is ring then S is called subring

Ex :-

S is subring iff $a,b \in S \Rightarrow a+b \in S$ & $ab \in S$ (closed under + & ×).

(i) Z is subring of Q : Q is subring of R : R is subring of C under usual + & ×.

(ii) Set of even integer is subring of integers.

(iii) commutative ring

$a \cdot b = b \cdot a \quad \forall\, a,b \in R \Rightarrow$ R is commutative ring

Ex (Z,+,·).

Ring with unit element.

$1 \in R \Rightarrow a \cdot 1 = 1 \cdot a \;\forall\, a \in R$ is called Ring with unit element

Ex ~~(Z,+,·)~~ then (1 → unit element).

Zero divisor.

If $a \neq 0$ & $b \neq 0 \Rightarrow a \cdot b = 0$.

a has a zero divisor.

Ex:-

$3 \times 4 = 12$ then $\frac{12}{6} = 2$.

no zero divisor.

If $a = 0$ & $b = 0 \Rightarrow a \cdot b = 0$ is called no zero divisor. in R is Ring & $a, b \in R$.

character of integral domain.

(a). There is +ve integer $m \ni$: $ma = 0 \ \forall \ a \in D \Rightarrow D$ is finite character.

p is smallest +ve integer such that $pa = 0 \ \forall \ a \in D \Rightarrow D$ is character of p.

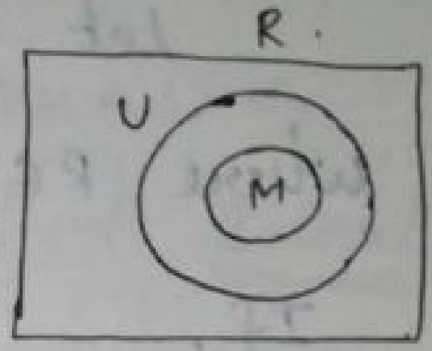
$\Rightarrow D$ has finite number of element.

(b). There is +ve integer $m \ni$: $m \neq 0 \ \forall$ $a \in D$ (or). ~~$a \neq 0$ in~~

$a \neq 0$ in ~~D~~ $\ni$: $m = 0$ only if $m = 0$.

$\Rightarrow D$ is of character $0 \Rightarrow D$ has infinite number of element.

Ideal & Maximal Ideal.



(a). Let U be a non-empty subset of R.

(i) $(U,+)$ is subgroup in R

(ii) $u \in U$ & $r \in R \Rightarrow ur$ & $ru \in U$, then U is called Ideal in R.

(b).

Let M be an Ideal in R $\ni$: $M \neq R$.

If "$M \subset U \subset R \Rightarrow U = M$ (or) $U = R$".

then M is called maximum Ideal in R.

Ex:-

Let R be the ring of all real valued continuous function on $[0,1]$. (unit closed integral). then

$M = \{ f(x) \in R : f(1/2) = 0 \}$ is called Ideal & maximal Ideal in R.

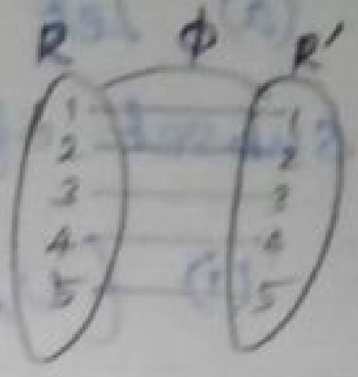
Prime Ideal :-

Let p be an Ideal in R, R & $a, b \in R$.

If "$ab \in p \Rightarrow a \in p$ (or) $b \in p$". then p is called prime ideal in R.

Homomorphism

Let $\phi : R \to R'$ be a function where R & R' are rings.



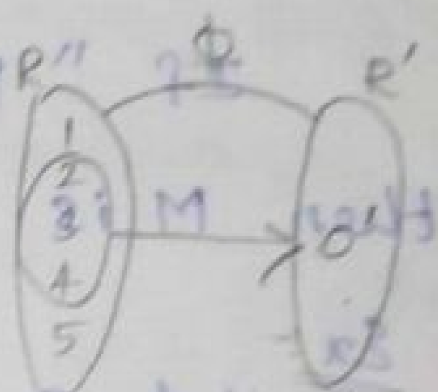
If,

(i) $\phi(a+b) = \phi(a) + \phi(b)$.

(ii) $\phi(ab) = \phi(a)\phi(b)$. $\forall\ a, b \in R$

then ϕ is called a homomorphism.

Kernal. $(I(\phi))$



If $\phi : R \to R'$ is homomorphism, then

$I(P) = \{ a \in R : \phi(a) = 0'$ &

$0'$ is zero element in $R \}$, then is called kernal.

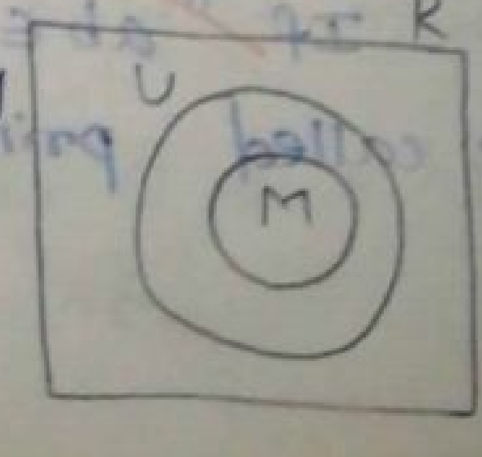
Remark :-

Homomorphism & 1-1 $\Rightarrow$ Isomorphism.

Homomorphism, 1-1 & onto $\Rightarrow$ Isomorphic $(R \cong R')$.

Ideal & Quotient Ring

Let U be a non empty subset of R



(i) $(U, +)$ is subgroup is R

(ii) $u \in U$ & $r \in R \Rightarrow ur$ & $ru \in U$.

($ur \in U \Rightarrow$ Right ideal & $ru \in U \Rightarrow$ left ideal), Then U is called Ideal in R.

* If U is a ideal in R, then

(i) $R/U = \{r+U, r \in R\}$ is called Quotient ring.

Binary operation $\Rightarrow$ (B. O)

$(a+u) + (b+u) = (a+b) + u$ &

$(a+u)(b+u) = ab + u$.

(ii). $\varphi : R \to R/U$ is homomorphism

(Homomorphism image of R is R/U).

Problem

1. Let $R = \{Z_6 \cdot +_6 \times_6\}$. be a ring. Then verify the following are ideal (or) not & subring (or) not,

(a). $\{0, 2, 4\}$, (b) $\{0, 3\}$, (c) $\{0, 3, 4, 5\}$.

Soln: Let $Z_6 = \{0, 1, 2, 3, 4, 5\}$ be ring under $+_6$ & $\times_6$.

(a). Let $S = \{0, 2, 4\}$. (inverse $\Rightarrow 0 \to 0$, $2 \to 4$, $4 \to 2$).

(i) ideal (or) not, ~~$0 \in S : Z_6$~~ =

$0 \in S : Z_6 = \{0, 1, 2, 3, 4, 5\} \Rightarrow \{0, 0, 0, 0, 0, 0\}$

$2 \in S : Z_6 = \{0, 1, 2, 3, 4, 5\} \Rightarrow \{0, 2, 4, 0, 2, 4, 0, 2, 4\} \in S$.

$4 \in S : Z_6 = \{0, 1, 2, 3, 4, 5\} \Rightarrow \{0, 4, 2, 0, 4, 2, 0, 4, 2\} \in S$.

(ii) Subring (or) not $\Rightarrow$ Every ideal is subring $\Rightarrow$ S is subring.

(b). Let $S = \{0, 3\}$. (inverse $0 \to 0$, $3 \to 3$)

(i) ideal (or) not,

$0 \in S : Z_6 = \{0, 1, 2, 3, 4, 5\} \Rightarrow \{0, 0, 0, 0, 0, 0\} \in S$.

$3 \in S : Z_6 = \{0, 1, 2, 3, 4, 5\} \Rightarrow 0, 3, 0, 3, 0, 3, 0, 3 \in S$

(ii) subring (or) not $\Rightarrow$ Every ideal is subring $\Rightarrow$ S is subring.

Q. verification

Let $a = 0$ & $b = 3 \Rightarrow a - b = a + (-b)$

$= 0 + 3 = 3 \in S$

$ab = 0.3 = 0 \in S$.

Let $a = 3$ & $b = 0 \Rightarrow a - b = a + (-b)$

$= 3 + 0 = 3 \in S$.

$ab = 3 \cdot 0 = 0 \in S$.

(c). Let $S = \{0, 3, 4, 5\}$. Inverse of $5 = 6 - 5 = 1 \notin S$.

$\Rightarrow S$ is not ideal and not subring.

Book work.

Ring Theory.

A nonempty set R is said to be an associate ring. If in R there are defined two operations. denoted by + & · respectively such that for all a, b, c in R

i) $a + b$ is in R.

ii) $a + b = b + a$.

iii). $(a + b) + c = a + (b + c)$.

iv). There is an element 0 in R $\ni$: $a + 0 = a$ $(\forall a \in R)$

v). $\exists$ an element $-a \in R \ni$: $a + (-a) = 0$.

vi). $a \cdot b$ is in R.

vii). $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

viii). $a \cdot (b + c) = a \cdot b + a \cdot c$ &

$(b + c) \cdot a = b \cdot a + c \cdot a$

(The two distributive laws).

Ring with unit element :-

If R is the set of integers, positive, negative, and 0. + is the usual addition & . the usual multiplication of integers, then R is commutative is called ring with unit element.

No unit element :-

If R is the set of even integers under the usual operations of + & . R is a commutative ring but has no unit element.

Field :-

If R is the set of rational numbers under the usual operation and multiplication of rational numbers. R is a commutative ring with unit element. But even more than that note that the elements of R different from 0 from an abelian group under (.) A ring with this latter property is called field.

Homomorphism :-

A mapping ϕ from the ring R into the ring R' is said to be a homomorphism if,

(i) $\phi(a+b) = \phi(a) + \phi(b)$.

(ii) $\phi(ab) = \phi(a)\phi(b)$.

Isomorphism :-

A homomorphism of R in R' is said to be an Isomorphism if it is a 1-1 mapping is called Isomorphism.

(H & 1-1 ⇒ Isomorphism)

Isomorphic :-

If two rings are said to be isomorphic if there is an Isomorphism of one onto mapping is called isomorphic.

(Isomorphism & onto ⇒ Isomorphic.

Lemma : 1

If ϕ is a homomorphism of R into R'. with kernal $I(\phi)$, then

(i) $I(\phi)$ is a subgroup of R under addition.

(ii) If $a \in I(\phi)$ & $r \in R$ then both ar & ra are in $I(\phi)$.

Proof :-

Since ϕ is in perticular a homomorphism of R, as an additive group into R is an additive group.

Suppose that $a \in I(\phi)$, $r \in R$

Then $\phi(a) = 0$.

so that $\phi(ar) = \phi(a)\phi(r)$.

$$\Rightarrow \phi(ar) = 0\,\phi(r) = 0.$$

Thus, by defining property of $I(\phi)$ both ar & ra are in $I(\phi)$. //

Ex

Let R & R' be two arbitrary rings. and define $\phi(a) = 0$ $\forall a \in R$. Trivially ϕ is a homomorphism and $I(\phi) = R$. Then ϕ is called the Zero-homomorphism.

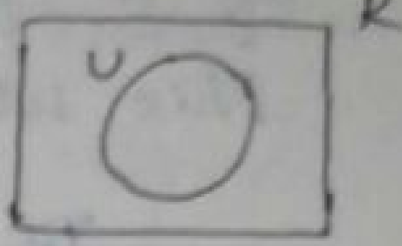
Hence the proof //

Ideals and Quotient Rings :-

A non-empty subset U of R is said to be (two-sided) ideal of R if,

(i) U is a subgroup of R under addition

(ii) For every $u \in U$ & $r \in R$, both ur & ru are in U.



then is called Ideal.

Notes :- (Ideal).

The homomorphism ϕ of R into R' is an isomorphism iff one onto the order of from mapping.

Defn :-

If ϕ is a homomorphism of R into R' then the kernal of ϕ, $I(\phi)$ is the set of all elements $a \in R \ni$: $\phi(a) = 0$, the zero element of R'. then is called ideal of zero element.

More Ideal & Quotient Ring :-

Defn :-

An ideal $M \neq R$ in a ring R is said to be a maximal Ideal of R if whenever U is an ideal of $R \ni$: $M \subset U \subset R$, then either $R = U$ (or) $M = U$. then is called Maximal Ideal.

Ex :-

Let R be the ring of integers and let U be ideal of R. since U is a

subgroup of R under addition.
W.K.T, U consists of all the multiples of a fixed integer n_0, we write this as $U = (n_0)$

If p is a prime number then $P = (p)$ is a maximal ideal of R.

Lemma 1:-

Let R be a commutative ring with unit element whose only ideals are (0) & R itself. Then R is a field.

Proof:-

Let $a \neq 0 \in R$ we must produce an element $b \neq 0 \in R \ni: ab = 1$.

So suppose that $a \neq 0$ is in R.

Consider the set $Ra = \{xa / x \in R\}$.

We claim that Ra is an ideal of R.

Now, if $u, v \in Ra$, then $u = r_1 a$, $v = r_2 a$ for some $r_1, r_2 \in R$. Thus

$u + v = r_1 a + r_2 a = (r_1 + r_2) a \in Ra$.

|||ly
$-u = -r_1 a$
$= (-r_1) a \in Ra$.

Hence Ra is an additive subgroup of R.

Moreover, if $r \in R$, $ru = r(r_1 a)$

$= (r r_1) a \in Ra$

$\therefore R_a$ satisfies all the defining condition for an ideal of R

Hence is an ideal of R.

By assumptions on R, $R_a = (0)$ (or) $R_a = R$.

Since $0 \neq a = I_a \in R_a$, $R_a (0)$ thus we are left with the only other possibility $R_a = R$

This last equation states that every element in R is a multiple of a by some element of R.

In particular $I \in R$ & so it can be realized as a multiple of a.

ie) An element $b \in R \ni: ba = 1$.

Hence the proof.

Theorem :1.

(2) If R is commutative ring with unit element and M is an ideal of R, then M is maximal ideal of R iff R/M is a field.

Proof :-

Suppose that M is an ideal of $R \ni: R/M$ is a field.

Scanned with CamScanner

Since R/M is a field its only ideal are (0) & R/M itself.

But there is a one-to-one correspondence between the set of ideal of R/M and the set of ideals of R which contain M.

The ideal M of R correspondence to the ideal (0) of R/M whereas the ideal R of R correspondence to the ideal R/M of R/M in the one-to-one mapping.

Thus there is no ideal between M & R other than these two, whence M is a maximal ideal.

Hence the proof //.

Euclidean Ring :- (E).

An integral domain R is said to be a Euclidean ring if for every $a \neq 0$ in R there is defined a non-negative integer $d(a)$ ∋:

(i) $\forall\ a, b \in R$, both non-zero, $d(a) \leq d(ab)$

(ii) $\forall\ a, b \in R$, both non-zero $\exists$ $t, r \in R$ ∋: $a = tb + r$, where either

$r = 0$ (or) $d(r) \leq d(b)$, then the above conditions in satisfies is called Euclidean ring.

Theorem 1 :-

(1) (3) Let R be a Euclidean ring and Let A be an ideal of R. Then there exist ∃ an element $a_0 \in A$ ∋: A is consists exactly of all $a_0 x$ as x ranges over R.

Proof :-

If A just consists of the element 0. Put $a_0 = 0$ and the conclusion of the theorem holds.

Thus we many assume that $A \neq 0$.

Hence there is an $a \neq 0$ in A.

The element is an $a_0 \in A$ ∋: $d(a_0)$ (d is) minimal

Since (d takes on non-negative integer values this is always possibles).

Suppose that $a \in A$.

By the properties of Euclidean ring ∃ $t, r \in R$ ∋: $a = ta_0 + r$ where $r = 0$ (or) $d(r) < d(a_0)$.

Since $a_0 \in A$ & A is an ideal of R, ta_0 is an A.

Combined with $a \in A$ this results in $a - ta_0 \in A$. But $r = a - ta_0$, whence $r \in A$.

If $r \neq 0$ then $d(r) < d(a_0)$ giving the element r in A whose d-value is smaller than that of a_0, in contradiction to element of a_0 in A of minimal d-value consequently $r = 0$ & $a = ta_0$.

Hence the proof //

Defn :-

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

(i) d/a & d/b.

(ii) Whenever c/a & c/b then c/d.

We shall use the notation $d = (a, b)$ to denote that d is a greatest common divisor of a & b. Then we write $d(a, b)$.

Ex :-

(i) Consider $(10, 20)$. Hence greatest common divisor are 10 & 20 $\Rightarrow$

$GCD = (1, 2, 5, 10) \Rightarrow (10, 20)$ in GCD.

(ii) Consider $(14, 21)$, Here greatest common divisor are $(14, 21) \Rightarrow$

$GCD = (1 \& 7) \Rightarrow (14, 21)$ in GCD.

Principle Ideal of Ring.

An integral domain R with unit element is a principle ideal ring if every ideal A in R is of the form A = (a) for some $a \in R$.

We establish that a Euclidean ring has a unit element, in varies of we know that a Euclidean ring is a principle ideal ring.

Unit :-

In the Euclidean ring R a non unit π is said to be a prime element of R if whenever $\pi = ab$, where a, b are in R. then one of a (or) b is a unit in R.

A prime element is thus an element in R which cannot be factored in R in a non trivial way. then is called unit.

Ring with unit element :-

Let R be a commutative ring with ~~unit~~ element An element $a \in R$ is a unit in R if there exist an element $b \in R \ni: ab = 1$.

Do not confuse a unit with a

unit element. A unit in a ring is an element whose inverse is also in the ring is called ring with unit element.

Theorem 2 :-

Unique Factorization Theorem.

State :-

Let R be a Euclidean ring and $a \neq 0$ a non-unit in R. Suppose that $a = \pi_1 \pi_2 \dots \pi_n = \pi_1' \pi_2' \dots \pi_m'$, where the π_i & π_j' are prime elements of R. Then $n = m$ and each π_i, $1 \leq i \leq n$ is an associate of some π_j', $1 \leq j \leq m$ and conversely each π_k' is an associate of some π_q.

Proof :-

If the relation $a = \pi_1 \pi_2 \dots \pi_n$

But $\pi_1 / \pi_1 \pi_2 \dots \pi_n$

Hence $\pi_1 / \pi_1' \pi_2' \dots \pi_m'$.

If π is a prime element in the Euclidean ring R & π / ab, where $a, b \in R$ then π divides atleast one of a (or) b.

Suppose that π does not divide a :
then $(\pi, a) = 1$

$\therefore$ π_1 & π_i' are both prime elements of R and π_1 / π_i' they must be associates and $\pi_i' = u_1 \pi_1$, where u_1 is a unit in R.

Thus $\pi_1 \cdot \pi_2 \cdots \cdot \pi_n = \pi_1' \pi_2' \cdots \pi_m' =$
$u_1 \pi_1 \pi_2' \cdots \pi_{i-1}' \pi_{i+1}'$ cancel off π_1 and we are left with $\pi_2 \cdots \pi_n = u_1 \pi_2' \cdots \pi_{i-1}' \pi_{i+1}' \cdots \pi_m'$

Then the argument on this relation with π_2, after n^{th} steps, the left side becomes 1.

The right side a product of a certain number of π'

This would force $n \leq m$.

Since the π' are not units

Illy, $m \leq n$ so that $n = m$.

In the process we have also showed that every π_i has some π_i' as an associate and conversely.

The proof is by induction on $d(a)$

If $d(a) = d(1)$ then a is a unit in R

We assume that the for all element x in R $\ni$: $d(x) < d(a)$.

If a is a prime element of R there is nothing to prove suppose that $a = bc$ where neither b (or) c is unit in R

i.e. $d(b) < d(bc) = d(a)$ &

$d(c) < d(bc) = d(a)$.

The product of a finite number of prime elements of R.

Consequently $a = bc = \pi_1 \pi_2 \ldots \pi_n \pi_1' \pi_2' \ldots \pi_m'$ and in this way has been factored as a product of a prime elements.

Let R be an integral domain with unit element and suppose that for $a, b \in R$ both a/b & b/a are true

Then $a = ub$, where u is a unit in R

Since, a/b, $b = xa$ for some $x \in R$.

then b/a, $a = yb$ for some $y \in R$.

Thus $b = x(yb) = (xy)b$.

But these are element of an integral domain, so that we can cancel the b and obtain $xy = 1$

Thus a unit in R & $a = yb$.

We have that every non-zero element in a Euclidean ring R can be uniquely written as a product of prime element (or) is a unit in R.

Hence the theorem //

A particular Euclidean Ring :-

Non zero element :- (Gaussian integer).

Let J[i] denote the set of all complex number of the form $a+bi$ where a & b are integers. Under the usual addition and multiplication of complex number J[i] forms an integral domain called the domain of Gaussian integers.

Then J[i] as Euclidean ring.

In order to do this function $d(x)$ defined for every non-zero element in J[i] satisfies

(i) $d(x)$ is a non negative integer for every $x \neq 0 \in J[i]$.

(ii) $d(x) \leq d(xy)$ for every $y \neq 0$ in J[i]

(iii) Given $u, v \in J[i]$ ∃ $t, r \in J[i]$ ∋: $v = tu + r$, where $r = 0$ (or) $d(r) < d(u)$.

Fermat's Theorem

State:-

If P is a prime number of the form $4n+1$ then $P = a^2 + b^2$ for some integers a, b.

Proof:-

There exist an $x \ni$:

$x^2 \equiv -1 \bmod p$ [i]

The x can be choosen so that $0 \leq x \leq p-1$:

∴ We only need to use the remainder of x on divison by P

We can restrict the size of x even further namely, to satisfy $|x| \leq P/2$.

For if $x > P/2$, then $y = P - x$ satisfies $y^2 \equiv -1 \bmod p$.

But $|y| \leq P/2$

Thus we may assume that we have an integer $x \ni : |x| \leq P/2$ & x^2+1 is multiple of P, say cp.

Now $CP = x^2 + 1 \leq P^2/4 + 1 < P^2$

Hence $c < P$ and so $P \nmid c$

Let P be a prime integer and suppose that for some integer C relatively prime to P. we can find integers x & y. ∋: $x^2+y^2 = CP$.

Then P can be written as the sum of squares of two integers.

ie), $P = a^2+b^2$.

The ring of integers is a subring of J[i].

Suppose that the integer P is also a prime element of J[i].

∴ $CP = x^2+y^2 = (x+yi)(x-yi)$.

Then $P/(x+yi)$ (or) $P/(x-yi)$ in J[i]

But if $P/(x+yi)$ then $x+yi = p(u+vi)$

Which would say that $x = pu$ & $y = pv$, so that p also would divide $x-yi$.

But then $p^2/(x+iy)(x-iy) = CP$.

from we would conclude that P/C in assumption.

$|||^{ly}$, If $P/(x-yi)$. Thus p is not a prime element in J[i] (ie) $p = (a+bi)(g+di)$, where $a+bi$ & $g+di$ are in $J[i]$ and where neither $a+bi$ (or) $g+di$ is a unit in $J[i]$.

But this means that neither a^2+b^2 (or) $g^2+d^2 = 1$.

It follows easily that $p = (a-bi)(g-di)$

Thus $p^2 = (a+bi)(g+di)(a-bi)(g-di)$

$$p^2 = (a^2+b^2)(g^2+d^2)$$

$\therefore (a^2+b^2)/p^2$, so $a^2+b^2 = 1 \cdot p$ (or) p^2, $a^2+b^2 \neq 1$.

Since $a+bi$ is not a unit in $J[i]$

$\Rightarrow a^2+b^2 \neq p^2$ otherwise $g^2+d^2 = 1$, contrary to the fact that $g+di$ is not unit in $J[i]$.

Thus the only left is that $a^2+b^2 = p$ & we obtain that $p = a^2+b^2$ for some integers a & b

Hence the theorem //

Lemma 1 :-

If p is a prime number of the form $4n+1$, then we can solve the congruence $x^2 \equiv -1 \bmod p$.

Proof :-

Let $x = 1.2.3 \ldots (p-1)/2$

since, $p-1 = 4n$ in this product for x there are an even number of terms, in consequences of which is

$$x = (-1)(-2)(-3) \ldots \left(-\left(\frac{p-1}{2}\right)\right)$$

But $p-k \equiv -k \bmod p$, so that

$$x^2 \equiv \left(1.2 \ldots \frac{p-1}{2}\right)(-1)(-2) \ldots \left(-\left(\frac{p-1}{2}\right)\right)$$

$$\equiv 1.2 \ldots \frac{p-1}{2} \, \frac{p+1}{2} \ldots (p-1)$$

$$\equiv (p-1)! \equiv -1 \bmod p.$$

We are using here wilson's theorem proved earlier namely that if p is a prime number $(p-1)! \equiv -1 (p)$

To illustrate this result if $p = 13$.

$x = 1.2.3.4.5.6 = 720 \equiv 5 \bmod 13$ &

$5^2 \equiv -1 \bmod 13$.

Hence the proof.

25/8/19 V.good

UNIT - III

Polynomial Ring :- $F[x]$

Explain

The term of $a_0 + a_1 x + a_2 x^2 + \dots +$ $a_n x^n$ (n is non integer) is called polynomial ring in x.

(a). Let $p(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n$,

$q(x) = b_0 + b_1 x + b_2 x^2 + \dots + b_n x^n$ in

$F[x]$. Then $p(x) = q(x)$ iff $a_i = b_i$ $\forall$ integer $i \geq 0$.

$p(x) + q(x) = c_0 + c_1 x + \dots + c_t x^t$, where

$c_i = a_i + b_i$ for each $i \geq 0$.

$p(x)\, q(x) = c_0 + c_1 x + \dots + c_k x^k$, where

$c_k = a_k b_0 + a_{t-1} b_1 + a_{t-2} b_2 + \dots + a_0 b_k$.

(b). If $f(x) = a_0 + a_1 x + \dots + a_n x^n \neq 0$, then

$\deg f(x) = n$.

$\text{Deg} = 0 \Rightarrow$ constant polynomial (or)
Scalar polynomial (or) Trivial polynomial
$(f(x) = 7)$.

Deg (+ive) $\Rightarrow$ Non zero polynomial
$(x^2 + 2x + 7)$;

zero polynomial $\Rightarrow$ Deg not defined. (2)

(c). Let $p(x) \in F(x)$

If $p(x) = a(x)\, b(x) \Rightarrow a(x)$ (or) $b(x)$ is constant ($\deg a(x) = 0$ (or) $\deg b(x) = 0$).
where $a(x)$ & $b(x) \in F(x)$, the $p(x)$ is called irreducible (Not factorizable) over F.

(d). Let $f(x) = a_0 + a_1 x + \dots + a_n x^n$ be a polynomial, where $a_0, a_1, \dots, a_n$ are integers

(i) gcd of $a_0, a_1, \dots, a_n$ is $1 \Rightarrow f(x)$ is said to be primative polynomial (G.C.D $\Rightarrow$ constant).

(ii). Highest co-efficient is $1 \Rightarrow f(x)$ is said to be integer monic polynomial.

(e). If $p(x)$ is polynomial over F of Lowest degree satisfied by a, then $p(x)$ is called minimum polynomial over F and $p(a) = 0$.

(f). Let R be commutative ring with unit element, then $R[x]$ is polynomial ring in x over R.

Let $R[x_1] = R_1$ ∴ $R_1[x_2] = R_2$ (polynomial ring x_2 over R_1), $R_{n-1}[x_n] = R_n$

Then R_n is called ring of polynomial in $x_1, x_2, \ldots, x_n$ over R and it is denoted by $R[x_1, x_2, \ldots, x_n]$.

Ex. G.C.D.

$x^2 - 5x + 6 = (x-2)(x-3)$

$x^2 - 6x + 8 = (x-2)(x-4)$

G.C.D $= (x-2)$.

Book work.

The ring of polynomial.

Defn 1:- If $p(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_m x^m$ &

$q(x) = b_0 + b_1 x + b_2 x^2 + \cdots + a_n x^n$

are in $F[x]$, then $p(x) = q(x)$ iff for ~~each~~ every integer $i \geq 0$, $a_i = b_i$

Defn 2:-

If $p(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_m x^m$ &

$q(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_n x^n$

are both in $F[x]$, then $p(x) + q(x) = c_0 + c_1 x + c_2 x^2 + \ldots + c_t x^t$ where for each i, $c_i = a_i + b_i$.

If $p(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_m x^m$ &

$q(x) = b_0 + b_1 x + b_2 x^2 + \dots + a_n x^n$, then

$p(x) q(x) = c_0 + c_1 x + c_2 x^2 + \dots + c_k x^k$,

where, $c_t = a_t b_0 + a_{t-1} b_1 + a_{t-2} b_2 + \dots + a_0 b_t$

This definition says nothing more than: multiply the two polynomials by multiplying out the symbols formally use the relation $x^\alpha x^\beta = x^{\alpha+\beta}$ and collect terms.

Let us illustrate the defn with an example,

$p(x) = 1 + x - x^2$, $q(x) = 2 + x^2 + x^3$.

Here, $a_0 = 1$, $a_1 = 1$, $a_2 = -1$, $a_3 = a_4 = \dots = 0$

$b_0 = 2$, $b_1 = 0$, $b_2 = 1$, $b_3 = 1$, $b_4 = b_5 = \dots = 0$

Thus, $c_0 = a_0 b_0 = 1.2 = 2$,

$c_1 = a_1 b_0 + a_0 b_1 = 1(2) + 1(0) = 2$.

$c_2 = a_2 b_0 + a_1 b_1 + a_0 b_2 = (-1)(2) + 1(0) + 1(1)$

$= -1$

$c_3 = a_3 b_0 + a_2 b_1 + a_1 b_2 + a_0 b_3$

$= (0)(2) + (-1)(0) + 1(1) + 1(1)$

$\Rightarrow c_3 = 2$

$c_4 = a_4 b_0 + a_3 b_1 + a_2 b_2 + a_1 b_3 + a_0 b_4$

$= (0)(2) + (0)(0) + (-1)(1) + (1)(1) + (1)(0)$

$\Rightarrow c_4 = 0$.

$c_5 = a_5b_0 + a_4b_1 + a_3b_2 + a_2b_3 + a_1b_4 + a_0b_5$ (5)

$= (0)(2) + (0)(0) + (0)(1) + (-1)(1) + (1)(0) + (0)(0)$

$\Rightarrow c_5 = -1$

$c_6 = a_6b_0 + a_5b_1 + a_4b_2 + a_3b_3 + a_2b_4 + a_1b_5 + a_0b_6.$

$= (0)(2) + (0)(0) + (0)(1) + (0)(1) + (-1)(0) + (1)(0) + (1)(0)$

$\Rightarrow c_6 = 0.$

$c_7 = c_8 = \cdots = 0$

∴ According to our defn,

$(1+x-x^2)(2+x^2+x^3) = c_0 + c_1x + \cdots$

$= 2 + 2x - x^2 + 2x^3 - x^5$

If you multiply these together high-school style you will see that you get the same answer. Our defn of product is the one the reader has always known.

Lemma : 1

The Divison Algorithm.

(6) Given two polynomials $f(x)$ & $g(x) \neq 0$ in $F[x]$, then there exist two polynomials $t(x)$ & $r(x)$ in $F[x]$ ∋: $f(x) = t(x)g(x) + r(x)$, where $r(x) = 0$ (or) degree $r(x) <$ degree $g(x)$.

Proof :-

If the "long division" to divide one polynomial by another.

If the degree of $f(x)$ is smaller than that of $g(x)$ there is nothing to prove.

put $t(x) = 0$, $r(x) = f(x)$ and we have that $f(x) = 0\, g(x) + f(x)$, where $\deg f(x) < \deg g(x)$ (or) $f(x) = 0$.

So we many assume that,

$f(x) = a_0 + a_1 x + \dots + a_m x^m$ &

$g(x) = b_0 + b_1 x + \dots + b_n x^n$, where $a_m \neq 0$, $b_n \neq 0$. & $m \geq n$.

Let $f_1(x) = f(x) - (a_m/b_n)\, x^{m-n} g(x)$.

thus, $\deg f_1(x) \leq m-1$, so by induction on the degree of $f(x)$ we many assume that $f_1(x) = t_1(x)\, g(x) + r(x)$, where $r(x) = 0$ (or) $\deg r(x) < \deg g(x)$.

But $f(x) - (a_m/b_n)\, x^{m-n} g(x) = t_1(x) \cdot g(x) + r(x)$, by transposing, we arrive at $f(x) = \left[(a_m/b_n)\, x^{m-n} + t_1(x) \right] g(x) + r(x)$.

If we put $t(x) = (a_m/b_n)\, x^{m-n} + t_1(x)$

We do indeed have that $f(x) = t(x)g(x) + r(x)$, where $t(x), r(x) \in F[x]$ & where $r(x) = 0$ (or) $\deg r(x) < \deg g(x)$.

Hence the proof //

VVI

Lemma 2:-

This ideal $A = (p(x))$ in $F[x]$ is a maximal ideal iff $p(x)$ is irreducible over F.

Proofs:-

Let F be the field of rational numbers & consider the polynomial $p(x) = x^3 - 2$ in $F[x]$.

As is easily verified, it is irreducible over F, whence $F[x]/(x^3-2)$ is a fields.

Let $A = (x^3-2)$, the ideal in $F[x]$ generated by x^3-2.

Any element in $F[x]/(x^3-2)$ is a coset of the form $f(x)+A$ of the ideal A with $f(x)$ in $F[x]$.

Now, given any polynomial $f(x) \in F[x]$ by the division algorithm,

$f(x) = t(x)(x^3-2) + r(x)$, where $r(x) = 0$.

(or) $\deg r(x) < \deg(x^3-2) = 3$

Thus, $r(x) = a_0 + a_1 x + a_2 x^2 + \dots$, where a_0, a_1, a_2 are in F.

Consequently $f(x) + A = a_0 + a_1 x + a_2 x^2 + t(x)(x^3-2) + A$.

$= a_0 + a_1 x + a_2 x^2 + A$.

Since $t(x)(x^3-2)$ is in A, hence by the addition & multiplication in $F[x]/(x^3-2)$,

$f(x) + A = (a_0 + A) + a_1(x+A) + a_2(x+A)^2$

If we put $t = x + A$.

Then every element in $F[x]/(x^3-2)$ is of the form,

$a_0 + a_1 t + a_2 t^2$ with a_0, a_1, a_2 in F.

What about t?

Since, $t^3 - 2 = (x+A)^3 - 2$

$= x^3 - 2 + A$

$= A$.

$= 0$ ($\because$ A is the zero element of $F[x]/(x^3-2)$ we see that t^3-2

Hence the proof.

Polynomials over the Rational Field :-

Defn 1

The polynomial $f(x) = a_0 + a_1 x + \dots + a_n x^n$, where $a_0, a_1, a_2, \dots, a_n$ are integer is said to be primitine if the greatest common divisor of $a_0, a_1, \dots a_n$ is 1.

Defn : 2.

A polynomial is said to be integer monic if all its co-efficients are integers and its highest co-efficient is 1.

Thus an integer monic polynomial is one of the form $x^n + a_1 x^{n-1} + \dots + a_n$, where the 'a' n is integers.

Lemma : 1

(8) If $f(x)$ & $g(x)$ are primitive polynomials, then $f(x) g(x)$ is a primitive polynomial.

Proof :- Let $f(x) = a_0 + a_1 x + \dots + a_n x^n$ &

$g(x) = b_0 + b_1 x + \dots + b_m x^m$.

Suppose that all the co-efficient of $f(x)g(x)$ would be divisible by some integer 1.

Hence by some prime number p.

Since $f(x)$ is primitive. p does not divide some co-efficient a_i.

Let a_j be the first co-efficient of $f(x)$ which p does not divide.

|||ly. Let b_k be the first co-efficient of $g(x)$ which p does not divide.

In $f(x)g(x)$ the co-efficient of x^{j+k}, c_{j+k} is.

$$c_{j+k} = a_j b_k + (a_{j+1} b_{k-1} + a_{j+2} b_{k-2} + \dots + a_{j+k} b_0) + (a_{j-1} b_{k+1} + a_{j-2} b_{k+2} + \dots + a_0 b_{j+k}).$$

Now,

b_k, $p / b_{k-1}, b_{k-2}, \dots$ so that

$$p / (a_{j+1} b_{k-1} + a_{j+2} b_{k-2} + \dots + a_{j+k} b_0)$$

|||ly

a_j, $p / a_{j-1}, a_{j-2}, \dots$ so that

$$p / (a_{j-1} b_{k+1} + a_{j-2} b_{k+2} + \dots + a_0 b_{k+j})$$

is by assumption p / c_{j+k}.

Thus by ① $p / a_j b_k$.

since $p \nmid a_j$ & $p \nmid b_k$.

Hence the proof //.

Theorem.

(9) The Eisenstein criterion

State:-

Let $f(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n$ be a polynomial with integer co-efficients suppose that for some prime number p, $p \nmid a_n$, $p | a_1$, $p | a_2$, $p | a_3 \dots p | a_0$, $p^2 \nmid a_0$. Then $f(x)$ is irreducible over the rationals.

Proof:-

Without loss of generality we may assume that $f(x)$ is primitive.

For taking out the greatest common factor of its co-efficient does not disturb the hypothesis.

since, $p \nmid a_n$

If $f(x)$ factors as a product of two rational polynomials.

Scanned with CamScanner

Scanned with CamScanner

By Gauss Lemma it factors as the product of two polynomials having integer co-efficients.

Thus if we assume that $f(x)$ is reducible.

Then,

$$f(x) = (b_0 + b_1 x + b_2 x^2 + \dots + b_r x^r)$$
$$(c_0 + c_1 x + c_2 x^2 + \dots + c_s x^s)$$

where, the b's & c's are integers & where $r > 0$ & $s > 0$.

Reading off the co-efficient we first get $a_0 = b_0 c_0$.

since p / a_0,

p must divide one of b_0 or c_0.

since p^2 / a_0,

p cannot divide both b_0 & c_0.

suppose that p / a_0, p / c_0

Not all the co-efficient $b_0, b_1, \dots, b_r$ can be divisible by p.

otherwise all the co-efficient of $f(x)$ would be divisible by p.

Which is manifestly false.

since $p \nmid a_n$.

Let b_k be the first b not divisible by p, $k \leq r < n$.

Thus p / b_{k-1} and the earlier b's

But $a_k = b_k c_0 + b_{k-1} c_1 + \dots + b_0 c_k$ &

p / a_k, $p / b_{k-1}, b_{k-2}, \dots, b_0$.

So that $p / b_k c_0$.

However $p \nmid c_0$, $p \nmid b_k$;

Which conflicts with $p / b_k c_0$

This contradiction proves that we could not have factored $f(x)$ and so $f(x)$ is indeed irreducible.

Hence the proof //.

Polynomial Rings over Commutative Rings :-

UNI (X) 10m

Theorem 1. 10

If R is a unique factorization domain, then so is $R[x]$.

Proof:-

Let $f(x)$ be an arbitrary element in $R[x]$.

We can write $f(x)$ in $F[x]$ is primitive.

If R is a unique factorization domain if $p(x)$ is a primitive polynomial in $F[x]$.

Then it can be factored in a unique way of the product of irreducible element in $R[x]$.

We consider $p(x)$ as an element in $F[x]$, we can factor it as :

$p(x) = p_1(x) \cdots p_k(x)$, where $p_1(x), p_2(x), \ldots p_k(x)$ are irreducible polynomials in $F[x]$.

Each $p_i(x) = \left(f_i(x)/a_i \right)$, where $f_i(x) \in R[x]$ & $a_i \in R$, moreover $f_i(x) = c_i q_i(x)$, where $c_i = c(f_i)$ & where $q_i(x)$ is primitive in $R[x]$.

Thus each $p_i(x) = \left(c_i q_i(x)/a_i \right)$, where $a_i, c_i \in R$ & $q_i(x) \in R[x]$ is primitive.

Since, $p_i(x)$ is irreducible in $F[x]$, $q_i(x)$ must also be irreducible in $F[x]$.

Now,

$$p(x) = p_1(x) \cdot p_2(x) \cdots p_k(x)$$

$$= \frac{c_1 c_2 \cdots c_k}{a_1 a_2 \cdots a_k} q_1(x) \cdots q_k(x).$$

Whence $a_1 a_2 \cdots a_k (p(x)) = c_1 c_2 \cdots c_k\, q(x)$ (15)

Using $p(x)$ & of $q_1(x) \cdots q_k(x)$.

Thus,

$a_1 a_2 \cdots a_k = c_1 c_2 \cdots c_k$

Hence $p(x) = q_1(x) \cdots q_k(x)$

We factored $p(x)$, in $R[x]$ as a product of irreducible elements.

We can decompose $f_1(x)$ in unique way as the product of irreducible elements of $R[x]$.

Then,

$0 = \deg c = \deg(a_1(x)) + \deg(a_2(x)) + \cdots + \deg(a_n(x))$

$\therefore$ Each $a_i(x)$ must be of degree 0.

i.e., must be element of R.

In otherwords the factorization of c as an element of R.

Since R is a unique factorization domain, c has a unique factorization as a product of irreducible element of R.

Hence of $R[x]$.

Hence the proof //.

Page no. (1)

5

Fields

Unit – IV

In our discussion of rings we have already singled out a special class which we called fields. A field, let us recall, is a commutative ring with unit element in which every nonzero element has a multiplicative inverse. Put another way, a field is a commutative ring in which we can divide by any nonzero element.

Fields play a central role in algebra. For one thing, results about them find important applications in the theory of numbers. For another, their theory encompasses the subject matter of the theory of equations which treats questions about the roots of polynomials.

In our development we shall touch only lightly on the field of algebraic numbers. Instead, our greatest emphasis will be on aspects of field theory which impinge on the theory of equations. Although we shall not treat the material in its fullest or most general form, we shall go far enough to introduce some of the beautiful ideas, due to the brilliant French mathematician Evariste Galois, which have served as a guiding inspiration for algebra as it is today.

I. 5.1 Extension Fields

In this section we shall be concerned with the relation of one field to another. Let F be a field; a field K is said to be an *extension* of F if K contains F. Equivalently, K is an extension of F if F is a subfield of K. *Throughout this chapter F will denote a given field and K an extension of F.*

As was pointed out earlier, in the chapter on vector spaces, if K is

Scanned with CamScanner

Scanned with CamScanner

Page no. (2)

an extension of F, then, under the ordinary field operations in K, K is a vector space over F. As a vector space we may talk about linear dependence, dimension, bases, etc., in K relative to F.

2.m (x)

DEFINITION The *degree* of K over F is the dimension of K as a vector space over F.

We shall always denote the degree of K over F by $[K:F]$. Of particular interest to us is the case in which $[K:F]$ is finite, that is, when K is finite-dimensional as a vector space over F. This situation is described by saying that K is a *finite extension* of F.

We start off with a relatively simple but, at the same time, highly effective result about finite extensions, namely,

10.m

THEOREM 5.1.1 *If L is a finite extension of K and if K is a finite extension of F, then L is a finite extension of F. Moreover, $[L:F] = [L:K][K:F]$.*

Proof. The strategy we employ in the proof is to write down explicitly a basis of L over F. In this way not only do we show that L is a finite extension of F, but we actually prove the sharper result and the one which is really the heart of the theorem, namely that $[L:F] = [L:K][K:F]$.

Suppose, then, that $[L:K] = m$ and that $[K:F] = n$. Let $v_1, \ldots, v_m$ be a basis of L over K and let $w_1, \ldots, w_n$ be a basis of K over F. What could possibly be nicer or more natural than to have the elements v_iw_j, where $i = 1, 2, \ldots, m$, $j = 1, 2, \ldots, n$, serve as a basis of L over F? Whatever else, they do at least provide us with the right number of elements. We now proceed to show that they do in fact form a basis of L over F. What do we need to establish this? First we must show that every element in L is a linear combination of them with coefficients in F, and then we must demonstrate that these mn elements are linearly independent over F.

Let t be any element in L. Since every element in L is a linear combination of $v_1, \ldots, v_m$ with coefficients in K, in particular, t must be of this form. Thus $t = k_1v_1 + \cdots + k_mv_m$, where the elements $k_1, \ldots, k_m$ are all in K. However, every element in K is a linear combination of $w_1, \ldots, w_n$ with coefficients in F. Thus $k_1 = f_{11}w_1 + \cdots + f_{1n}w_n, \ldots, k_i = f_{i1}w_1 + \cdots + f_{in}w_n, \ldots, k_m = f_{m1}w_1 + \cdots + f_{mn}w_n$, where every f_{ij} is in F.

Substituting these expressions for $k_1, \ldots, k_m$ into $t = k_1v_1 + \cdots + k_mv_m$, we obtain $t = (f_{11}w_1 + \cdots + f_{1n}w_n)v_1 + \cdots + (f_{m1}w_1 + \cdots + f_{mn}w_n)v_m$. Multiplying this out, using the distributive and associative laws, we finally arrive at $t = f_{11}v_1w_1 + \cdots + f_{1n}v_1w_n + \cdots + f_{ij}v_iw_j + \cdots + f_{mn}v_mw_n$. Since the f_{ij} are in F, we have realized t as a linear combination over F of the elements v_iw_j. Therefore, the elements v_iw_j do indeed span all of L over F, and so they fulfill the first requisite property of a basis.

We still must show that the elements $v_i w_j$ are linearly independent over F. Suppose that $f_{11}v_1w_1 + \cdots + f_{1n}v_1w_n + \cdots + f_{ij}v_iw_j + \cdots + f_{mn}v_mw_n = 0$, where the f_{ij} are in F. Our objective is to prove that each $f_{ij} = 0$. Regrouping the above expression yields $(f_{11}w_1 + \cdots + f_{1n}w_n)v_1 + \cdots + (f_{i1}w_1 + \cdots + f_{in}w_n)v_i + \cdots + (f_{m1}w_1 + \cdots + f_{mn}w_n)v_m = 0$.

Since the w_i are in K, and since $K \supset F$, all the elements $k_i = f_{i1}w_1 + \cdots + f_{in}w_n$ are in K. Now $k_1v_1 + \cdots + k_mv_m = 0$ with $k_1, \ldots, k_m \in K$. But, by assumption, $v_1, \ldots, v_m$ form a basis of L over K, so, in particular they must be linearly independent over K. The net result of this is that $k_1 = k_2 = \cdots = k_m = 0$. Using the explicit values of the k_i, we get

$$f_{i1}w_1 + \cdots + f_{in}w_n = 0 \qquad \text{for} \quad i = 1, 2, \ldots, m.$$

But now we invoke the fact that the w_i are linearly independent over F; this yields that each $f_{ij} = 0$. In other words, we have proved that the v_iw_j are linearly independent over F. In this way they satisfy the other requisite property for a basis.

We have now succeeded in proving that the mn elements v_iw_j form a basis of L over F. Thus $[L:F] = mn$; since $m = [L:K]$ and $n = [K:F]$ we have obtained the desired result $[L:F] = [L:K][K:F]$.

Suppose that L, K, F are three fields in the relation $L \supset K \supset F$ and, suppose further that $[L:F]$ is finite. Clearly, any elements in L linearly independent over K are, all the more so, linearly independent over F. Thus the assumption that $[L:F]$ is finite forces the conclusion that $[L:K]$ is finite. Also, since K is a subspace of L, $[K:F]$ is finite. By the theorem, $[L:F] = [L:K][K:F]$, whence $[K:F] \mid [L:F]$. We have proved the

COROLLARY *If L is a finite extension of F and K is a subfield of L which contains F, then* $[K:F] \mid [L:F]$.

Thus, for instance, if $[L:F]$ is a prime number, then there can be no fields properly between F and L. A little later, in Section 5.4, when we discuss the construction of certain geometric figures by straightedge and compass, this corollary will be of great significance.

DEFINITION An element $a \in K$ is said to be *algebraic over* F if there exist elements $\alpha_0, \alpha_1, \ldots, \alpha_n$ in F, not all 0, such that $\alpha_0a^n + \alpha_1a^{n-1} + \cdots + \alpha_n = 0$.

If the polynomial $q(x) \in F[x]$, the ring of polynomials in x over F, and if $q(x) = \beta_0x^m + \beta_1x^{m-1} + \cdots + \beta_m$, then for any element $b \in K$, by $q(b)$ we shall mean the element $\beta_0b^m + \beta_1b^{m-1} + \cdots + \beta_m$ in K. In the expression commonly used, $q(b)$ is the *value* of the polynomial $q(x)$ obtained by substituting b for x. The element b is said to *satisfy* $q(x)$ if $q(b) = 0$.

In these terms, $a \in K$ is algebraic over F if there is a nonzero polynomial $p(x) \in F[x]$ which a satisfies, that is, for which $p(a) = 0$.

Let K be an extension of F and let a be in K. Let $\mathcal{M}$ be the collection of all subfields of K which contain both F and a. $\mathcal{M}$ is not empty, for K itself is an element of $\mathcal{M}$. Now, as is easily proved, the intersection of any number of subfields of K is again a subfield of K. Thus the intersection of all those subfields of K which are members of $\mathcal{M}$ is a subfield of K. We denote this subfield by $F(a)$. What are its properties? Certainly it contains both F and a, since this is true for every subfield of K which is a member of $\mathcal{M}$. Moreover, by the very definition of intersection, every subfield of K in $\mathcal{M}$ contains $F(a)$, yet $F(a)$ itself is in $\mathcal{M}$. *Thus $F(a)$ is the smallest subfield of K containing both F and a.* We call $F(a)$ the subfield obtained by *adjoining a* to F.

Our description of $F(a)$, so far, has been purely an external one. We now give an alternative and more constructive description of $F(a)$. Consider all these elements in K which can be expressed in the form $\beta_0 + \beta_1 a + \cdots + \beta_s a^s$; here the β's can range freely over F and s can be any nonnegative integer. As elements in K, one such element can be divided by another, provided the latter is not 0. Let U be the set of all such quotients. We leave it as an exercise to prove that U is a subfield of K.

On one hand, U certainly contains F and a, whence $U \supset F(a)$. On the other hand, any subfield of K which contains both F and a, by virtue of closure under addition and multiplication, must contain all the elements $\beta_0 + \beta_1 a + \cdots + \beta_s a^s$ where each $\beta_i \in F$. Thus $F(a)$ must contain all these elements; being a subfield of K, $F(a)$ must also contain all quotients of such elements. Therefore, $F(a) \supset U$. The two relations $U \subset F(a)$, $U \supset F(a)$ of course imply that $U = F(a)$. In this way we have obtained an internal construction of $F(a)$, namely as U.

We now intertwine the property that $a \in K$ is algebraic over F with macroscopic properties of the field $F(a)$ itself. This is

THEOREM 5.1.2 *The element $a \in K$ is algebraic over F if and only if $F(a)$ is a finite extension of F.*

Proof. As is so very common with so many such "if and only if" propositions, one-half of the proof will be quite straightforward and easy, whereas the other half will be deeper and more complicated.

Suppose that $F(a)$ is a finite extension of F and that $[F(a):F] = m$. Consider the elements $1, a, a^2, \ldots, a^m$; they are all in $F(a)$ and are $m+1$ in number. By Lemma 4.2.4, these elements are linearly dependent over F. Therefore, there are elements $\alpha_0, \alpha_1, \ldots, \alpha_m$ in F, not all 0, such that $\alpha_0 1 + \alpha_1 a + \alpha_2 a^2 + \cdots + \alpha_m a^m = 0$. Hence a is algebraic over F and satisfies the nonzero polynomial $p(x) = \alpha_0 + \alpha_1 x + \cdots + \alpha_m x^m$ in $F[x]$ of degree at most $m = [F(a):F]$. This proves the "if" part of the theorem.

Now to the "only if" part. Suppose that a in K is algebraic over F. By assumption, a satisfies some nonzero polynomial in $F[x]$; let $p(x)$ be a polynomial in $F[x]$ of smallest positive degree such that $p(a) = 0$. We claim that $p(x)$ is irreducible over F. For, suppose that $p(x) = f(x)g(x)$, where $f(x), g(x) \in F[x]$; then $0 = p(a) = f(a)g(a)$ (see Problem 1) and, since $f(a)$ and $g(a)$ are elements of the field K, the fact that their product is 0 forces $f(a) = 0$ or $g(a) = 0$. Since $p(x)$ is of lowest positive degree with $p(a) = 0$, we must conclude that one of $\deg f(x) \geq \deg p(x)$ or $\deg g(x) \geq \deg p(x)$ must hold. But this proves the irreducibility of $p(x)$.

We define the mapping ψ from $F[x]$ into $F(a)$ as follows. For any $h(x) \in F[x]$, $h(x)\psi = h(a)$. We leave it to the reader to verify that ψ is a ring homomorphism of the ring $F[x]$ into the field $F(a)$ (see Problem 1). What is V, the kernel of ψ? By the very definition of ψ, $V = \{h(x) \in F[x] \mid h(a) = 0\}$. Also, $p(x)$ is an element of lowest degree in the ideal V of $F[x]$. By the results of Section 3.9, every element in V is a multiple of $p(x)$, and since $p(x)$ is irreducible, by Lemma 3.9.6, V is a maximal ideal of $F[x]$. By Theorem 3.5.1, $F[x]/V$ is a field. Now by the general homomorphism theorem for rings (Theorem 3.4.1), $F[x]/V$ is isomorphic to the image of $F[x]$ under ψ. Summarizing, we have shown that the image of $F[x]$ under ψ is a subfield of $F(a)$. This image contains $x\psi = a$ and, for every $\alpha \in F$, $\alpha\psi = \alpha$. Thus the image of $F[x]$ under ψ is a subfield of $F[a]$ which contains both F and a; by the very definition of $F(a)$ we are forced to conclude that the image of $F[x]$ under ψ is *all* of $F(a)$. Put more succinctly, $F[x]/V$ is isomorphic to $F(a)$.

Now, $V = (p(x))$, the ideal generated by $p(x)$; from this we claim that the dimension of $F[x]/V$, as a vector space over F, is precisely equal to $\deg p(x)$ (see Problem 2). In view of the isomorphism between $F[x]/V$ and $F(a)$ we obtain the fact that $[F(a):F] = \deg p(x)$. Therefore, $[F(a):F]$ is certainly finite; this is the contention of the "only if" part of the theorem. Note that we have actually proved more, namely that $[F(a):F]$ is equal to the degree of the polynomial of least degree satisfied by a over F.

The proof we have just given has been somewhat long-winded, but deliberately so. The route followed contains important ideas and ties in results and concepts developed earlier with the current exposition. No part of mathematics is an island unto itself.

We now redo the "only if" part, working more on the inside of $F(a)$. This reworking is, in fact, really identical with the proof already given; the constituent pieces are merely somewhat differently garbed.

Again let $p(x)$ be a polynomial over F of lowest positive degree satisfied by a. Such a polynomial is called a *minimal polynomial* for a over F. We may assume that its coefficient of the highest power of x is 1, that is, it is monic; in that case we can speak of *the* minimal polynomial for a over F for any two minimal, monic polynomials for a over F are equal. (Prove!)

Page No. 6

Suppose that $p(x)$ is of degree n; thus $p(x) = x^n + \alpha_1 x^{n-1} + \cdots + \alpha_n$ where the α_i are in F. By assumption, $a^n + \alpha_1 a^{n-1} + \cdots + \alpha_n = 0$, whence $a^n = -\alpha_1 a^{n-1} - \alpha_2 a^{n-2} - \cdots - \alpha_n$. What about a^{n+1}? From the above, $a^{n+1} = -\alpha_1 a^n - \alpha_2 a^{n-1} - \cdots - \alpha_n a$; if we substitute the expression for a^n into the right-hand side of this relation, we realize a^{n+1} as a linear combination of the elements $1, a, \ldots, a^{n-1}$ over F. Continuing this way, we get that a^{n+k}, for $k \geq 0$, is a linear combination over F of $1, a, a^2, \ldots, a^{n-1}$.

Now consider $T = \{\beta_0 + \beta_1 a + \cdots + \beta_{n-1}a^{n-1} \mid \beta_0, \beta_1, \ldots, \beta_{n-1} \in F\}$. Clearly, T is closed under addition; in view of the remarks made in the paragraph above, it is also closed under multiplication. Whatever further it may be, T has at least been shown to be a ring. Moreover, T contains both F and a. We now wish to show that T is more than just a ring, that it is, in fact, a field.

Let $0 \neq u = \beta_0 + \beta_1 a + \cdots + \beta_{n-1}a^{n-1}$ be in T and let $h(x) = \beta_0 + \beta_1 x + \cdots + \beta_{n-1}x^{n-1} \in F[x]$. Since $u \neq 0$, and $u = h(a)$, we have that $h(a) \neq 0$, whence $p(x) \nmid h(x)$. By the irreducibility of $p(x)$, $p(x)$ and $h(x)$ must therefore be relatively prime. Hence we can find polynomials $s(x)$ and $t(x)$ in $F[x]$ such that $p(x)s(x) + h(x)t(x) = 1$. But then $1 = p(a)s(a) + h(a)t(a) = h(a)t(a)$, since $p(a) = 0$; putting into this that $u = h(a)$, we obtain $ut(a) = 1$. The inverse of u is thus $t(a)$; in $t(a)$ all powers of a higher than $n - 1$ can be replaced by linear combinations of $1, a, \ldots, a^{n-1}$ over F, whence $t(a) \in T$. We have shown that every nonzero element of T has its inverse in T; consequently, T is a field. However, $T \subset F(a)$, yet F and a are both contained in T, which results in $T = F(a)$. We have identified $F(a)$ as the set of all expressions $\beta_0 + \beta_1 a + \cdots + \beta_{n-1}a^{n-1}$.

Now T is spanned over F by the elements $1, a, \ldots, a^{n-1}$ in consequence of which $[T:F] \leq n$. However, the elements $1, a, a^2, \ldots, a^{n-1}$ are linearly independent over F, for any relation of the form $\gamma_0 + \gamma_1 a + \cdots + \gamma_{n-1}a^{n-1}$, with the elements $\gamma_i \in F$, leads to the conclusion that a satisfies the polynomial $\gamma_0 + \gamma_1 x + \cdots + \gamma_{n-1}x^{n-1}$ over F of degree less than n. This contradiction proves the linear independence of $1, a, \ldots, a^{n-1}$, and so these elements actually form a basis of T over F, whence, in fact, we now know that $[T:F] = n$. Since $T = F(a)$, the result $[F(a):F] = n$ follows.

2.m

DEFINITION The element $a \in K$ is said to be *algebraic of degree* n over F if it satisfies a nonzero polynomial over F of degree n but no nonzero polynomial of lower degree.

In the course of proving Theorem 5.1.2 (in each proof we gave), we proved a somewhat sharper result than that stated in that theorem, namely,

THEOREM 5.1.3 *If $a \in K$ is algebraic of degree n over F, then $[F(a):F] = n$.*

This result adapts itself to many uses. We give now, as an immediate consequence thereof, the very interesting

THEOREM 5.1.4 *If a, b in K are algebraic over F then $a \pm b$, ab, and a/b (if $b \neq 0$) are all algebraic over F. In other words, the elements in K which are algebraic over F form a subfield of K.*

Proof. Suppose that a is algebraic of degree m over F while b is algebraic of degree n over F. By Theorem 5.1.3 the subfield $T = F(a)$ of K is of degree m over F. Now b is algebraic of degree n over F, *a fortiori* it is algebraic of degree at most n over T which contains F. Thus the subfield $W = T(b)$ of K, again by Theorem 5.1.3, is of degree at most n over T. But $[W:F] = [W:T][T:F]$ by Theorem 5.1.1; therefore, $[W:F] \leq mn$ and so W is a finite extension of F. However, a and b are both in W, whence all of $a \pm b$, ab, and a/b are in W. By Theorem 5.1.2, since $[W:F]$ is finite, these elements must be algebraic over F, thereby proving the theorem.

Here, too, we have proved somewhat more. Since $[W:F] \leq mn$, every element in W satisfies a polynomial of degree at most mn over F, whence the

COROLLARY *If a and b in K are algebraic over F of degrees m and n, respectively, then $a \pm b$, ab, and a/b (if $b \neq 0$) are algebraic over F of degree at most mn.*

In the proof of the last theorem we made two extensions of the field F. The first we called T; it was merely the field $F(a)$. The second we called W and it was $T(b)$. Thus $W = (F(a))(b)$; it is customary to write it as $F(a, b)$. Similarly, we could speak about $F(b, a)$; it is not too difficult to prove that $F(a, b) = F(b, a)$. Continuing this pattern, we can define $F(a_1, a_2, \ldots, a_n)$ for elements $a_1, \ldots, a_n$ in K.

DEFINITION The extension K of F is called an *algebraic extension* of F if every element in K is algebraic over F.

We prove one more result along the lines of the theorems we have proved so far.

THEOREM 5.1.5 *If L is an algebraic extension of K and if K is an algebraic extension of F, then L is an algebraic extension of F.*

Proof. Let u be any arbitrary element of L; our objective is to show that u satisfies some nontrivial polynomial with coefficients in F. What information do we have at present? We certainly do know that u satisfies some

Page No. (8)

polynomial $x^n + \sigma_1 x^{n-1} + \cdots + \sigma_n$, where $\sigma_1, \ldots, \sigma_n$ are in K. But K is algebraic over F; therefore, by several uses of Theorem 5.1.3, $M = F(\sigma_1, \ldots, \sigma_n)$ is a finite extension of F. Since u satisfies the polynomial $x^n + \sigma_1 x^{n-1} + \cdots + \sigma_n$ whose coefficients are in M, u is algebraic over M. Invoking Theorem 5.1.2 yields that $M(u)$ is a finite extension of M. However, by Theorem 5.1.1, $[M(u):F] = [M(u):M][M:F]$, whence $M(u)$ is a finite extension of F. But this implies that u is algebraic over F, completing proof of the theorem.

A quick description of Theorem 5.1.5: algebraic over algebraic is algebraic.

The preceding results are of special interest in the particular case in which F is the field of rational numbers and K the field of complex numbers.

DEFINITION A complex number is said to be an *algebraic number* if it is algebraic over the field of rational numbers.

A complex number which is not algebraic is called *transcendental*. At the present stage we have no reason to suppose that there are any transcendental numbers. In the next section we shall prove that the familiar real number e is transcendental. This will, of course, establish the existence of transcendental numbers. In actual fact, they exist in great abundance; in a very well-defined way there are more of them than there are algebraic numbers.

Theorem 5.1.4 applied to algebraic numbers proves the interesting fact that *the algebraic numbers form a field*; that is, the sum, products, and quotients of algebraic numbers are again algebraic numbers.

Theorem 5.1.5 when used in conjunction with the so-called "fundamental theorem of algebra," has the implication that the roots of a polynomial whose coefficients are algebraic numbers are themselves algebraic numbers.

Problems

1. Prove that the mapping $\psi: F[x] \to F(a)$ defined by $h(x)\psi = h(a)$ is a homomorphism.
2. Let F be a field and let $F[x]$ be the ring of polynomials in x over F. Let $g(x)$, of degree n, be in $F[x]$ and let $V = (g(x))$ be the ideal generated by $g(x)$ in $F[x]$. Prove that $F[x]/V$ is an n-dimensional vector space over F.
3. (a) If V is a finite-dimensional vector space over the field K, and if F is a subfield of K such that $[K:F]$ is finite, show that V is a finite-dimensional vector space over F and that moreover $\dim_F(V) = (\dim_K(V))([K:F])$.
   (b) Show that Theorem 5.1.1 is a special case of the result of part (a).

(Prove!) whence we can find a prime number larger than both c_0 and n and large enough to force $|c_1\varepsilon_1 + \cdots + c_n\varepsilon_n| < 1$. But $c_1\varepsilon_1 + \cdots + c_n\varepsilon_n = c_0F(0) + \cdots + c_nF(n)$, *so must be an integer*; since it is smaller than 1 in size our only possible conclusion is that $c_1\varepsilon_1 + \cdots + c_n\varepsilon_n = 0$. Consequently, $c_0F(0) + \cdots + c_nF(n) = 0$; this however is sheer nonsense, since we know that $p \nmid (c_0F(0) + \cdots + c_nF(n))$, whereas $p \mid 0$. This contradiction, stemming from the assumption that e is algebraic, proves that e must be transcendental.

Problems

1. Using the infinite series for e,

$$e = 1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \cdots + \frac{1}{m!} + \cdots,$$

prove that e is irrational.

2. If $g(x)$ is a polynomial with integer coefficients, prove that if p is a prime number then for $i \geq p$,

$$\frac{d^i}{dx^i}\left(\frac{g(x)}{(p-1)!}\right)$$

is a polynomial with integer coefficients each of which is divisible by p.

3. If a is any real number, prove that $(a^m/m!) \to 0$ as $m \to \infty$.
4. If $m > 0$ and n are integers, prove that $e^{m/n}$ is transcendental.

Page No. 9

5.3 Roots of Polynomials

In Section 5.1 we discussed elements in a given extension K of F which were algebraic over F, that is, elements which satisfied polynomials in $F[x]$. We now turn the problem around; given a polynomial $p(x)$ in $F[x]$ we wish to find a field K which is an extension of F in which $p(x)$ has a root. No longer is the field K available to us; in fact it is our prime objective to construct it. Once it is constructed, we shall examine it more closely and see what consequences we can derive.

DEFINITION If $p(x) \in F[x]$, then an element a lying in some extension field of F is called a *root* of $p(x)$ if $p(a) = 0$.

2 m

We begin with the familiar result known as the *Remainder Theorem*.

LEMMA 5.3.1 *If $p(x) \in F[x]$ and if K is an extension of F, then for any element $b \in K$, $p(x) = (x - b)q(x) + p(b)$ where $q(x) \in K[x]$ and where* $\deg q(x) = \deg p(x) - 1$.

Proof. Since $F \subset K$, $F[x]$ is contained in $K[x]$, whence we can consider $p(x)$ to be lying in $K[x]$. By the division algorithm for polynomials in $K[x]$, $p(x) = (x - b)q(x) + r$, where $q(x) \in K[x]$ and where $r = 0$ or $\deg r < \deg (x - b) = 1$. Thus either $r = 0$ or $\deg r = 0$; in either case r must be an element of K. But exactly what element of K is it? Since $p(x) = (x - b)q(x) + r$, $p(b) = (b - b)q(b) + r = r$. Therefore, $p(x) = (x - b)q(x) + p(b)$. That the degree of $q(x)$ is one less than that of $p(x)$ is easy to verify and is left to the reader.

COROLLARY *If $a \in K$ is a root of $p(x) \in F[x]$, where $F \subset K$, then in $K[x]$, $(x - a) \mid p(x)$.*

Proof. From Lemma 5.3.1, in $K[x]$, $p(x) = (x - a)q(x) + p(a) = (x - a)q(x)$ since $p(a) = 0$. Thus $(x - a) \mid p(x)$ in $K[x]$.

DEFINITION The element $a \in K$ is a root of $p(x) \in F[x]$ of *multiplicity* m if $(x - a)^m \mid p(x)$, whereas $(x - a)^{m+1} \nmid p(x)$.

A reasonable question to ask is, How many roots can a polynomial have in a given field? Before answering we must decide how to count a root of multiplicity m. *We shall always count it as m roots.* Even with this convention we can prove

LEMMA 5.3.2 *A polynomial of degree n over a field can have at most n roots in any extension field.*

Proof. We proceed by induction on n, the degree of the polynomial $p(x)$. If $p(x)$ is of degree 1, then it must be of the form $\alpha x + \beta$ where α, β are in a field F and where $\alpha \neq 0$. Any a such that $p(a) = 0$ must then imply that $\alpha a + \beta = 0$, from which we conclude that $a = (-\beta/\alpha)$. That is, $p(x)$ has the unique root $-\beta/\alpha$, whence the conclusion of the lemma certainly holds in this case.

Assuming the result to be true in any field for all polynomials of degree less than n, let us suppose that $p(x)$ is of degree n over F. Let K be any extension of F. If $p(x)$ has no roots in K, then we are certainly done, for the number of roots in K, namely zero, is definitely at most n. So, suppose that $p(x)$ has at least one root $a \in K$ and that a is a root of multiplicity m. Since $(x - a)^m \mid p(x)$, $m \leq n$ follows. Now $p(x) = (x - a)^m q(x)$, where $q(x) \in K[x]$ is of degree $n - m$. From the fact that $(x - a)^{m+1} \nmid p(x)$, we get that $(x - a) \nmid q(x)$, whence, by the corollary to Lemma 5.3.1, a is not a root of $q(x)$. If $b \neq a$ is a root, in K, of $p(x)$, then $0 = p(b) = (b - a)^m q(b)$; however, since $b - a \neq 0$ and since we are in a field, we conclude that $q(b) = 0$. That is, any root of $p(x)$, in K, other than a, must be a root of

$q(x)$. Since $q(x)$ is of degree $n - m < n$, by our induction hypothesis, $q(x)$ has at most $n - m$ roots in K, which, together with the other root a, counted m times, tells us that $p(x)$ has at most $m + (n - m) = n$ roots in K. This completes the induction and proves the lemma.

One should point out that commutativity is essential in Lemma 5.3.2. If we consider the ring of real quaternions, which falls short of being a field only in that it fails to be commutative, then the polynomial $x^2 + 1$ has at least 3 roots, i, j, k (in fact, it has an infinite number of roots). In a somewhat different direction we need, even when the ring is commutative, that it be an integral domain, for if $ab = 0$ with $a \neq 0$ and $b \neq 0$ in the commutative ring R, then the polynomial ax of degree 1 over R has at least two distinct roots $x = 0$ and $x = b$ in R.

The previous two lemmas, while interesting, are of subsidiary interest. We now set ourselves to our prime task, that of providing ourselves with suitable extensions of F in which a given polynomial has roots. Once this is done, we shall be able to analyze such extensions to a reasonable enough degree of accuracy to get results. The most important step in the construction is accomplished for us in the next theorem. The argument used will be very reminiscent of some used in Section 5.1.

THEOREM 5.3.1 *If $p(x)$ is a polynomial in $F[x]$ of degree $n \geq 1$ and is irreducible over F, then there is an extension E of F, such that $[E:F] = n$, in which $p(x)$ has a root.*

Proof. Let $F[x]$ be the ring of polynomials in x over F and let $V = (p(x))$ be the ideal of $F[x]$ generated by $p(x)$. By Lemma 3.9.6, V is a maximal ideal of $F[x]$, whence by Theorem 3.5.1, $E = F[x]/V$ is a field. This E will be shown to satisfy the conclusions of the theorem.

First we want to show that E is an extension of F; however, in fact, it is not! But let $\bar{F}$ be the image of F in E; that is, $\bar{F} = \{\alpha + V \mid \alpha \in F\}$. We assert that $\bar{F}$ is a field isomorphic to F; in fact, if ψ is the mapping from $F[x]$ into $F[x]/V = E$ defined by $f(x)\psi = f(x) + V$, then the restriction of ψ to F induces an isomorphism of F onto $\bar{F}$. (Prove!) Using this isomorphism, we identify F and $\bar{F}$; *in this way we can consider E to be an extension of F.*

We claim that E is a finite extension of F of degree $n = \deg p(x)$, for the elements $1 + V, x + V, (x + V)^2 = x^2 + V, \ldots, (x + V)^i = x^i + V, \ldots, (x + V)^{n-1} = x^{n-1} + V$ form a basis of E over F. (Prove!) For convenience of notation let us denote the element $x\psi = x + V$ in the field E as a. Given $f(x) \in F[x]$, what is $f(x)\psi$? We claim that it is merely $f(a)$, for, since ψ is a homomorphism, if $f(x) = \beta_0 + \beta_1 x + \cdots + \beta_k x^k$, then $f(x)\psi = \beta_0\psi + (\beta_1\psi)(x\psi) + \cdots + (\beta_k\psi)(x\psi)^k$, and using the identification indicated above of $\beta\psi$ with β, we see that $f(x)\psi = f(a)$.

In particular, since $p(x) \in V$, $p(x)\psi = 0$; however, $p(x)\psi = p(a)$. *Thus the element $a = x\psi$ in E is a root of $p(x)$.* The field E has been shown to satisfy all the properties required in the conclusion of Theorem 5.3.1, and so this theorem is now proved.

An immediate consequence of this theorem is the

COROLLARY *If $f(x) \in F[x]$, then there is a finite extension E of F in which $f(x)$ has a root. Moreover, $[E:F] \leq \deg f(x)$.*

Proof. Let $p(x)$ be an irreducible factor of $f(x)$; any root of $p(x)$ is a root of $f(x)$. By the theorem there is an extension E of F with $[E:F] = \deg p(x) \leq \deg f(x)$ in which $p(x)$, and so, $f(x)$ has a root.

Although it is, in actuality, a corollary to the above corollary, the next theorem is of such great importance that we single it out as a theorem.

THEOREM 5.3.2 *Let $f(x) \in F[x]$ be of degree $n \geq 1$. Then there is an extension E of F of degree at most $n!$ in which $f(x)$ has n roots (and so, a full complement of roots).*

Proof. In the statement of the theorem, a root of multiplicity m is, of course, counted as m roots.

By the above corollary there is an extension E_0 of F with $[E_0:F] \leq n$ in which $f(x)$ has a root α. Thus in $E_0[x]$, $f(x)$ factors as $f(x) = (x - \alpha)q(x)$, where $q(x)$ is of degree $n - 1$. Using induction (or continuing the above process), there is an extension E of E_0 of degree at most $(n - 1)!$ in which $q(x)$ has $n - 1$ roots. Since any root of $f(x)$ is either α or a root of $q(x)$, we obtain in E all n roots of $f(x)$. Now, $[E:F] = [E:E_0][E_0:F] \leq (n-1)!n = n!$ All the pieces of the theorem are now established.

Theorem 5.3.2 asserts the existence of a finite extension E in which the given polynomial $f(x)$, of degree n, over F has n roots. If $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n$, $a_0 \neq 0$ and if the n roots in E are $\alpha_1, \ldots, \alpha_n$, making use of the corollary to Lemma 5.3.1, $f(x)$ can be factored over E as $f(x) = a_0(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$. Thus $f(x)$ splits up completely over E as a product of *linear* (first degree) factors. Since a finite extension of F exists with this property, a *finite extension of F of minimal degree* exists which also enjoys this property of decomposing $f(x)$ as a product of linear factors. For such a minimal extension, no proper subfield has the property that $f(x)$ factors over it into the product of linear factors. This prompts the

DEFINITION If $f(x) \in F[x]$, a finite extension E of F is said to be a *splitting field* over F for $f(x)$ if over E (that is, in $E[x]$), but not over any proper subfield of E, $f(x)$ can be factored as a product of linear factors.

We reiterate: *Theorem 5.3.2 guarantees for us the existence of splitting fields.* In fact, it says even more, for it assures that given a polynomial of degree n over F there is a splitting field of this polynomial which is an extension of F of degree at most $n!$ over F. We shall see later that this upper bound of $n!$ is actually taken on; that is, given n, we can find a field F and a polynomial of degree n in $F[x]$ such that the splitting field of $f(x)$ over F has degree $n!$.

Equivalent to the definition we gave of a splitting field for $f(x)$ over F is the statement: *E is a splitting field of $f(x)$ over F if E is a minimal extension of F in which $f(x)$ has n roots, where $n = \deg f(x)$.*

An immediate question arises: given two splitting fields E_1 and E_2 of the same polynomial $f(x)$ in $F[x]$, what is their relation to each other? At first glance, we have no right to assume that they are at all related. Our next objective is to show that they are indeed intimately related; in fact, that they are isomorphic by an isomorphism leaving every element of F fixed. It is in this direction that we now turn.

Let F and F' be two fields and let τ be an isomorphism of F onto F'. For convenience let us denote the image of any $\alpha \in F$ under τ by α'; that is, $\alpha\tau = \alpha'$. We shall maintain this notation for the next few pages.

Can we make use of τ to set up an isomorphism between $F[x]$ and $F'[t]$, the respective polynomial rings over F and F'? Why not try the obvious? For an arbitrary polynomial $f(x) = \alpha_0 x^n + \alpha_1 x^{n-1} + \cdots + \alpha_n \in F[x]$ we define τ^* by $f(x)\tau^* = (\alpha_0 x^n + \alpha_1 x^{n-1} + \cdots + \alpha_n)\tau^* = \alpha'_0 t^n + \alpha'_1 t^{n-1} + \cdots + \alpha'_n$.

It is an easy and straightforward matter, which we leave to the reader, to verify.

LEMMA 5.3.3 *τ^* defines an isomorphism of $F[x]$ onto $F'[t]$ with the property that $\alpha\tau^* = \alpha'$ for every $\alpha \in F$.*

If $f(x)$ is in $F[x]$ we shall write $f(x)\tau^*$ as $f'(t)$. Lemma 5.3.3 immediately implies that factorizations of $f(x)$ in $F[x]$ result in like factorizations of $f'(t)$ in $F'[t]$, and vice versa. In particular, $f(x)$ is irreducible in $F[x]$ if and only if $f'(t)$ is irreducible in $F'[t]$.

However, at the moment, we are not particularly interested in polynomial rings, but rather, in extensions of F. Let us recall that in the proof of Theorem 5.1.2 we employed quotient rings of polynomial rings to obtain suitable extensions of F. In consequence it should be natural for us to study the relationship between $F[x]/(f(x))$ and $F'[t]/(f'(t))$, where $(f(x))$ denotes the ideal generated by $f(x)$ in $F[x]$ and $(f'(t))$ that generated by $f'(t)$ in $F'[t]$. The next lemma, which is relevant to this question, is actually part of a more general, purely ring-theoretic result, but we shall content ourselves with it as applied in our very special setting.

Page no. 14

LEMMA 5.3.4 *There is an isomorphism τ^{**} of $F[x]/(f(x))$ onto $F'[t]/(f'(t))$ with the property that for every $\alpha \in F$, $\alpha\tau^{**} = \alpha'$, $(x + (f(x)))\tau^{**} = t + (f'(t))$.*

Proof. Before starting with the proof proper, we should make clear what is meant by the last part of the statement of the lemma. As we have already done several times, we can consider F as imbedded in $F[x]/(f(x))$ by identifying the element $\alpha \in F$ with the coset $\alpha + (f(x))$ in $F[x]/(f(x))$. Similarly, we can consider F' to be contained in $F'[t]/(f'(t))$. The isomorphism τ^{**} is then supposed to satisfy $[\alpha + (f(x))]\tau^{**} = \alpha' + (f'(t))$.

We seek an isomorphism τ^{**} of $F[x]/(f(x))$ onto $F'[t]/(f'(t))$. What could be simpler or more natural than to try the τ^{**} defined by $[g(x) + (f(x))]\tau^{**} = g'(t) + (f'(t))$ for every $g(x) \in F[x]$? We leave it as an exercise to fill in the necessary details that the τ^{**} so defined is well defined and is an isomorphism of $F[x]/(f(x))$ onto $F'[t]/(f'(t))$ with the properties needed to fulfill the statement of Lemma 5.3.4.

For our purpose—that of proving the uniqueness of splitting fields—Lemma 5.3.4 provides us with the entering wedge, for we can now prove

THEOREM 5.3.3 *If $p(x)$ is irreducible in $F[x]$ and if v is a root of $p(x)$, then $F(v)$ is isomorphic to $F'(w)$ where w is a root of $p'(t)$; moreover, this isomorphism σ can so be chosen that*

1. $v\sigma = w$.
2. $\alpha\sigma = \alpha'$ *for every* $\alpha \in F$.

Proof. Let v be a root of the irreducible polynomial $p(x)$ lying in some extension K of F. Let $M = \{f(x) \in F[x] \mid f(v) = 0\}$. Trivially M is an ideal of $F[x]$, and $M \neq F[x]$. Since $p(x) \in M$ and is an irreducible polynomial, we have that $M = (p(x))$. As in the proof of Theorem 5.1.2, map $F[x]$ into $F(v) \subset K$ by the mapping ψ defined by $q(x)\psi = q(v)$ for every $q(x) \in F[x]$. We saw earlier (in the proof of Theorem 5.1.2) that ψ maps $F[x]$ onto $F(v)$. The kernel of ψ is precisely M, so must be $(p(x))$. By the fundamental homomorphism theorem for rings there is an isomorphism ψ^* of $F[x]/(p(x))$ onto $F(v)$. Note further that $\alpha\psi^* = \alpha$ for every $\alpha \in F$. Summing up: ψ^* is an isomorphism of $F[x]/(p(x))$ onto $F(v)$ leaving every element of F fixed and with the property that $v = [x + (p(x))]\psi^*$.

Since $p(x)$ is irreducible in $F[x]$, $p'(t)$ is irreducible in $F'[t]$ (by Lemma 5.3.3), and so there is an isomorphism θ^* of $F'[t]/(p'(t))$ onto $F'(w)$ where w is a root of $p'(t)$ such that θ^* leaves every element of F' fixed and such that $[t + (p'(t)]\theta^* = w$.

We now stitch the pieces together to prove Theorem 5.3.3. By Lemma 5.3.4 there is an isomorphism τ^{**} of $F[x]/(p(x))$ onto $F'[t]/(p'(t))$ which coincides with τ on F and which takes $x + (p(x))$ onto $t + (p'(t))$. Consider the mapping $\sigma = (\psi^*)^{-1}\tau^{**}\theta^*$ (motivated by

$$F(v) \xrightarrow{(\psi^*)^{-1}} \frac{F[x]}{(p(x))} \xrightarrow{\tau^{**}} \frac{F'[t]}{(p'(t))} \xrightarrow{\theta^*} F'(w))$$

of $F(v)$ onto $F'(w)$. It is an isomorphism of $F(v)$ onto $F'(w)$ since all the mapping ψ^*, τ^{**}, and θ^* are isomorphisms and onto. Moreover, since $v = [x + (p(x))]\psi^*$, $v\sigma = (v(\psi^*)^{-1})\tau^{**}\theta^* = ([x + (p(x)]\tau^{**})\theta^* = [t + (p'(t))]\theta^* = w$. Also, for $\alpha \in F$, $\alpha\sigma = (\alpha(\psi^*)^{-1})\tau^{**}\theta^* = (\alpha\tau^{**})\theta^* = \alpha'\theta^* = \alpha'$. We have shown that σ is an isomorphism satisfying all the requirements of the isomorphism in the statement of the theorem. Thus Theorem 5.3.3 has been proved.

A special case, but itself of interest, is the

COROLLARY *If $p(x) \in F[x]$ is irreducible and if a, b are two roots of $p(x)$, then $F(a)$ is isomorphic to $F(b)$ by an isomorphism which takes a onto b and which leaves every element of F fixed.*

We now come to the theorem which is, as we indicated earlier, the foundation stone on which the whole Galois theory rests. For us it is the focal point of this whole section.

THEOREM 5.3.4 *Any splitting fields E and E' of the polynomials $f(x) \in F[x]$ and $f'(t) \in F'[t]$, respectively, are isomorphic by an isomorphism ϕ with the property that $\alpha\phi = \alpha'$ for every $\alpha \in F$. (In particular, any two splitting fields of the same polynomial over a given field F are isomorphic by an isomorphism leaving every element of F fixed.)*

Proof. We should like to use an argument by induction; in order to do so, we need an integer-valued indicator of size which we can decrease by some technique or other. We shall use as our indicator the degree of some splitting field over the initial field. It may seem artificial (in fact, it may even be artificial), but we use it because, as we shall soon see, Theorem 5.3.3 provides us with the mechanism for decreasing it.

If $[E:F] = 1$, then $E = F$, whence $f(x)$ splits into a product of linear factors over F itself. By Lemma 5.3.3 $f'(t)$ splits over F' into a product of linear factors, hence $E' = F'$. But then $\phi = \tau$ provides us with an isomorphism of E onto E' coinciding with τ on F.

Assume the result to be true for any field F_0 and any polynomial $f(x) \in F_0[x]$ provided the degree of some splitting field E_0 of $f(x)$ has degree less than n over F_0, that is, $[E_0:F_0] < n$.

Suppose that $[E:F] = n > 1$, where E is a splitting field of $f(x)$ over F. Since $n > 1$, $f(x)$ has an irreducible factor $p(x)$ of degree $r > 1$. Let $p'(t)$ be the corresponding irreducible factor of $f'(t)$. Since E splits $f(x)$, a full complement of roots of $f(x)$, and so, *a priori*, of roots of $p(x)$, are in E. Thus there is a $v \in E$ such that $p(v) = 0$; by Theorem 5.1.3, $[F(v):F] = r$. Similarly, there is a $w \in E'$ such that $p'(w) = 0$. By Theorem 5.3.4 there is an isomorphism σ of $F(v)$ onto $F'(w)$ with the property that $\alpha\sigma = \alpha'$ for every $\alpha \in F$.

Since $[F(v):F] = r > 1$,

$$[E:F(v)] = \frac{[E:F]}{[F(v):F]} = \frac{n}{r} < n.$$

We claim that E is a splitting field for $f(x)$ considered as a polynomial over $F_0 = F(v)$, for no subfield of E, containing F_0 and hence F, can split $f(x)$, since E is assumed to be a splitting field of $f(x)$ over F. Similarly E' is a splitting field for $f'(t)$ over $F_0' = F'(w)$. By our induction hypothesis there is an isomorphism ϕ of E onto E' such that $a\phi = a\sigma$ for all $a \in F_0$. But for every $\alpha \in F$, $\alpha\sigma = \alpha'$ hence for every $\alpha \in F \subset F_0$, $\alpha\phi = \alpha\sigma = \alpha'$. This completes the induction and proves the theorem.

To see the truth of the "(in particular . . .)" part, let $F = F'$ and let τ be the identity map $\alpha\tau = \alpha$ for every $\alpha \in F$. Suppose that E_1 and E_2 are two splitting fields of $f(x) \in F[x]$. Considering $E_1 = E \supset F$ and $E_2 = E' \supset F' = F$, and applying the theorem just proved, yields that E_1 and E_2 are isomorphic by an isomorphism leaving every element of F fixed.

In view of the fact that any two splitting fields of the same polynomial over F are isomorphic and by an isomorphism leaving every element of F fixed, we are justified in speaking about *the* splitting field, rather than *a* splitting field, for it is essentially unique.

Examples

1. Let F be any field and let $p(x) = x^2 + \alpha x + \beta$, $\alpha, \beta \in F$, be in $F[x]$. If K is any extension of F in which $p(x)$ has a root, a, then the element $b = -\alpha - a$ also in K is also a root of $p(x)$. If $b = a$ it is easy to check that $p(x)$ must then be $p(x) = (x - a)^2$, and so both roots of $p(x)$ are in K. If $b \neq a$ then again both roots of $p(x)$ are in K. Consequently, $p(x)$ can be split by an extension of degree 2 of F. We could also get this result directly by invoking Theorem 5.3.2.

2. Let F be the field of rational numbers and let $f(x) = x^3 - 2$. In the field of complex numbers the three roots of $f(x)$ are $\sqrt[3]{2}$, $\omega\sqrt[3]{2}$, $\omega^2\sqrt[3]{2}$, where $\omega = (-1 + \sqrt{3}\,i)/2$ and where $\sqrt[3]{2}$ is a real cube root of 2. Now $F(\sqrt[3]{2})$ cannot split $x^3 - 2$, for, as a subfield of the real field, it cannot contain the complex, but not real, number $\omega\sqrt[3]{2}$. Without explicitly determining it, what can we say about E, the splitting field of $x^3 - 2$ over

F? By Theorem 5.3.2, $[E:F] \le 3! = 6$; by the above remark, since $x^3 - 2$ is irreducible over F and since $[F(\sqrt[3]{2}):F] = 3$, by the corollary to Theorem 5.1.1, $3 = [F(\sqrt[3]{2}):F] \mid [E:F]$. Finally, $[E:F] > [F(\sqrt[3]{2}):F] = 3$. The only way out is $[E:F] = 6$. We could, of course, get this result by making two extensions $F_1 = F(\sqrt[3]{2})$ and $E = F_1(\omega)$ and showing that ω satisfies an irreducible quadratic equation over F_1.

3. Let F be the field of rational numbers and let

$$f(x) = x^4 + x^2 + 1 \in F[x].$$

We claim that $E = F(\omega)$, where $\omega = (-1 + \sqrt{3}\,i)/2$, is a splitting field of $f(x)$. Thus $[E:F] = 2$, far short of the maximum possible $4! = 24$.

Problems

1. In the proof of Lemma 5.3.1, prove that the degree of $q(x)$ is one less than that of $p(x)$.
2. In the proof of Theorem 5.3.1, prove in all detail that the elements $1 + V, x + V, \ldots, x^{n-1} + V$ form a basis of E over F.
3. Prove Lemma 5.3.3 in all detail.
4. Show that τ^{**} in Lemma 5.3.4 is well defined and is an isomorphism of $F[x]/(f(x))$ onto $F[t]/(f'(t))$.
5. In Example 3 at the end of this section prove that $F(\omega)$ is the splitting field of $x^4 + x^2 + 1$.
6. Let F be the field of rational numbers. Determine the degrees of the splitting fields of the following polynomials over F.
   (a) $x^4 + 1$. (b) $x^6 + 1$.
   (c) $x^4 - 2$. (d) $x^5 - 1$.
   (e) $x^6 + x^3 + 1$.
7. If p is a prime number, prove that the splitting field over F, the field of rational numbers, of the polynomial $x^p - 1$ is of degree $p - 1$.

**8. If $n > 1$, prove that the splitting field of $x^n - 1$ over the field of rational numbers is of degree $\Phi(n)$ where Φ is the Euler Φ-function.
(This is a well-known theorem. I know of no easy solution, so don't be disappointed if you fail to get it. If you get an easy proof, I would like to see it. This problem occurs in an equivalent form as Problem 15, Section 5.6.)

*9. If F is the field of rational numbers, find necessary and sufficient conditions on a and b so that the splitting field of $x^3 + ax + b$ has degree exactly 3 over F.

10. Let p be a prime number and let $F = J_p$, the field of integers mod p.
    (a) Prove that there is an irreducible polynomial of degree 2 over F.

7. Prove that the following polynomials are irreducible over the field of rational numbers.
   (a) $8x^3 - 6x - 1$.
   (b) $x^3 - 2$.
   (c) $x^3 + x^2 - 2x - 1$.
8. Prove that $2\cos(2\pi/7)$ satisfies $x^3 + x^2 - 2x - 1$. (*Hint:* Use $2\cos(2\pi/7) = e^{2\pi i/7} + e^{-2\pi i/7}$.)
9. Prove that the regular pentagon is constructible.
10. Prove that the regular hexagon is constructible.
11. Prove that the regular 15-gon is constructible.
12. Prove that it is possible to trisect 72°.
13. Prove that a regular 9-gon is not constructible.
*14. Prove a regular 17-gon is constructible.

5.5 More about Roots

We return to the general exposition. Let F be any field and, as usual, let $F[x]$ be the ring of polynomials in x over F.

DEFINITION If $f(x) = \alpha_0 x^n + \alpha_1 x^{n-1} + \cdots + \alpha_i x^{n-i} + \cdots + \alpha_{n-1}x + \alpha_n$ in $F[x]$, then the *derivative* of $f(x)$, written as $f'(x)$, is the polynomial $f'(x) = n\alpha_0 x^{n-1} + (n-1)\alpha_1 x^{n-2} + \cdots + (n-i)\alpha_i x^{n-i-1} + \cdots + \alpha_{n-1}$ in $F[x]$.

To make this definition or to prove the basic formal properties of the derivatives, as applied to polynomials, does not require the concept of a limit. However, since the field F is arbitrary, we might expect some strange things to happen.

At the end of Section 5.2, we defined what is meant by the characteristic of a field. Let us recall it now. A field F is said to be of characteristic 0 if $ma \neq 0$ for $a \neq 0$ in F and $m > 0$, an integer. If $ma = 0$ for some $m > 0$ and some $a \neq 0 \in F$, then F is said to be of finite characteristic. In this second case, the characteristic of F is defined to be the smallest positive integer p such that $pa = 0$ for all $a \in F$. It turned out that if F is of finite characteristic then its characteristic p is a prime number.

We return to the question of the derivative. Let F be a field of characteristic $p \neq 0$. In this case, the derivative of the polynomial x^p is $px^{p-1} = 0$. Thus the usual result from the calculus that a polynomial whose derivative is 0 must be a constant no longer need hold true. However, if the characteristic of F is 0 and if $f'(x) = 0$ for $f(x) \in F[x]$, it is indeed true that $f(x) = \alpha \in F$ (see Problem 1). Even when the characteristic of F is $p \neq 0$, we can still describe the polynomials with zero derivative; if $f'(x) = 0$, then $f(x)$ is a polynomial in x^p (see Problem 2).

We now prove the analogs of the formal rules of differentiation that we know so well.

LEMMA 5.5.1 *For any* $f(x)$, $g(x) \in F[x]$ *and any* $\alpha \in F$,

1. $(f(x) + g(x))' = f'(x) + g'(x)$.
2. $(\alpha f(x))' = \alpha f'(x)$.
3. $(f(x)g(x))' = f'(x)g(x) + f(x)g'(x)$.

Proof. The proofs of parts 1 and 2 are extremely easy and are left as exercises. To prove part 3, note that from parts 1 and 2 it is enough to prove it in the highly special case $f(x) = x^i$ and $g(x) = x^j$ where both i and j are positive. But then $f(x)g(x) = x^{i+j}$, whence $(f(x)g(x))' = (i+j)x^{i+j-1}$; however, $f'(x)g(x) = ix^{i-1}x^j = ix^{i+j-1}$ and $f(x)g'(x) = jx^ix^{j-1} = jx^{i+j-1}$; consequently, $f'(x)g(x) + f(x)g'(x) = (i+j)x^{i+j-1} = (f(x)g(x))'$.

Recall that in elementary calculus the equivalence is shown between the existence of a multiple root of a function and the simultaneous vanishing of the function and its derivative at a given point. Even in our setting, where F is an arbitrary field, such an interrelation exists.

LEMMA 5.5.2 *The polynomial* $f(x) \in F[x]$ *has a multiple root if and only if* $f(x)$ *and* $f'(x)$ *have a nontrivial (that is, of positive degree) common factor.*

Proof. Before proving the lemma proper, a related remark is in order, namely, if $f(x)$ and $g(x)$ in $F[x]$ have a nontrivial common factor in $K[x]$, for K an extension of F, then they have a nontrivial common factor in $F[x]$. For, were they relatively prime as elements in $F[x]$, then we would be able to find two polynomials $a(x)$ and $b(x)$ in $F[x]$ such that $a(x)f(x) + b(x)g(x) = 1$. Since this relation also holds for those elements viewed as elements of $K[x]$, in $K[x]$ they would have to be relatively prime.

Now to the lemma itself. From the remark just made, we may assume, without loss of generality, that the roots of $f(x)$ all lie in F (otherwise extend F to K, the splitting field of $f(x)$). If $f(x)$ has a multiple root α, then $f(x) = (x-\alpha)^m q(x)$, where $m > 1$. However, as is easily computed, $((x-\alpha)^m)' = m(x-\alpha)^{m-1}$ whence, by Lemma 5.5.1, $f'(x) = (x-\alpha)^m q'(x) + m(x-\alpha)^{m-1}q(x) = (x-\alpha)r(x)$, since $m > 1$. But this says that $f(x)$ and $f'(x)$ have the common factor $x - \alpha$, thereby proving the lemma in one direction.

On the other hand, if $f(x)$ has no multiple root then $f(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$ where the α_i's are all distinct (we are supposing $f(x)$ to be monic). But then

$$f'(x) = \sum_{i=1}^{n} (x-\alpha_1)\cdots\widehat{(x-\alpha_i)}\cdots(x-\alpha_n)$$

Page No. 20

where the $\wedge$ denotes the term is omitted. We claim no root of $f(x)$ is a root of $f'(x)$, for

$$f'(\alpha_i) = \prod_{j \neq i} (\alpha_i - \alpha_j) \neq 0,$$

since the roots are all distinct. However, if $f(x)$ and $f'(x)$ have a nontrivial common factor, they have a common root, namely, any root of this common factor. The net result is that $f(x)$ and $f'(x)$ have no nontrivial common factor, and so the lemma has been proved in the other direction.

Learn the Proof

COROLLARY 1 *If $f(x) \in F[x]$ is irreducible, then*

1. *If the characteristic of F is 0, $f(x)$ has no multiple roots.*
2. *If the characteristic of F is $p \neq 0$, $f(x)$ has a multiple root only if it is of the form $f(x) = g(x^p)$.*

Proof. Since $f(x)$ is irreducible, its only factors in $F[x]$ are 1 and $f(x)$. If $f(x)$ has a multiple root, then $f(x)$ and $f'(x)$ have a nontrivial common factor by the lemma, hence $f(x) \mid f'(x)$. However, since the degree of $f'(x)$ is less than that of $f(x)$, the only possible way that this can happen is for $f'(x)$ to be 0. In characteristic 0 this implies that $f(x)$ is a constant, which has no roots; in characteristic $p \neq 0$, this forces $f(x) = g(x^p)$.

We shall return in a moment to discuss the implications of Corollary 1 more fully. But first, for later use in Chapter 7 in our treatment of finite fields, we prove the rather special

COROLLARY 2 *If F is a field of characteristic $p \neq 0$, then the polynomial $x^{p^n} - x \in F[x]$, for $n \geq 1$, has distinct roots.*

Proof. The derivative of $x^{p^n} - x$ is $p^n x^{p^n - 1} - 1 = -1$, since F is of characteristic p. Therefore, $x^{p^n} - x$ and its derivative are certainly relatively prime, which, by the lemma, implies that $x^{p^n} - x$ has no multiple roots.

Corollary 1 does not rule out the possibility that in characteristic $p \neq 0$ an irreducible polynomial might have multiple roots. To clinch matters, we exhibit an example where this actually happens. Let F_0 be a field of characteristic 2 and let $F = F_0(x)$ be the field of rational functions in x over F_0. We claim that the polynomial $t^2 - x$ in $F[t]$ is irreducible over F and that its roots are equal. To prove irreducibility we must show that there is no rational function in $F_0(x)$ whose square is x; this is the content of Problem 4. To see that $t^2 - x$ has a multiple root, notice that its derivative (the derivative is with respect to t; for x, being in F, is considered as a constant) is $2t = 0$. Of course, the analogous example works for any prime characteristic.

Now that the possibility has been seen to be an actuality, it points out a sharp difference between the case of characteristic 0 and that of characteristic p. The presence of irreducible polynomials with multiple roots in the latter case leads to many interesting, but at the same time complicating, subtleties. These require a more elaborate and sophisticated treatment which we prefer to avoid at this stage of the game. *Therefore, we make the flat assumption for the rest of this chapter that all fields occurring in the text material proper are fields of characteristic* 0.

DEFINITION The extension K of F is a *simple extension of* F if $K = F(\alpha)$ for some α in K.

In characteristic 0 (or in properly conditioned extensions in characteristic $p \neq 0$; see Problem 14) all finite extensions are realizable as simple extensions. This result is

THEOREM 5.5.1 *If F is of characteristic 0 and if a, b, are algebraic over F, then there exists an element $c \in F(a, b)$ such that $F(a, b) = F(c)$.*

Proof. Let $f(x)$ and $g(x)$, of degrees m and n, be the irreducible polynomials over F satisfied by a and b, respectively. Let K be an extension of F in which both $f(x)$ and $g(x)$ split completely. Since the characteristic of F is 0, all the roots of $f(x)$ are distinct, as are all those of $g(x)$. Let the roots of $f(x)$ be $a = a_1, a_2, \ldots, a_m$ and those of $g(x)$, $b = b_1, b_2, \ldots, b_n$.

If $j \neq 1$, then $b_j \neq b_1 = b$, hence the equation $a_i + \lambda b_j = a_1 + \lambda b_1 = a + \lambda b$ has only one solution λ in K, namely,

$$\lambda = \frac{a_i - a}{b - b_j}$$

Since F is of characteristic 0 it has an infinite number of elements, so we can find an element $\gamma \in F$ such that $a_i + \gamma b_j \neq a + \gamma b$ for all i and for all $j \neq 1$. Let $c = a + \gamma b$; our contention is that $F(c) = F(a, b)$. Since $c \in F(a, b)$, we certainly do have that $F(c) \subset F(a, b)$. We will now show that both a and b are in $F(c)$ from which it will follow that $F(a, b) \subset F(c)$.

Now b satisfies the polynomial $g(x)$ over F, hence satisfies $g(x)$ considered as a polynomial over $K = F(c)$. Moreover, if $h(x) = f(c - \gamma x)$ then $h(x) \in K[x]$ and $h(b) = f(c - \gamma b) = f(a) = 0$, since $a = c - \gamma b$. Thus in some extension of K, $h(x)$ and $g(x)$ have $x - b$ as a common factor. We assert that $x - b$ is in fact their greatest common divisor. For, if $b_j \neq b$ is another root of $g(x)$, then $h(b_j) = f(c - \gamma b_j) \neq 0$, since by our choice of γ, $c - \gamma b_j$ for $j \neq 1$ avoids all roots a_i of $f(x)$. Also, since $(x - b)^2 \nmid g(x)$, $(x - b)^2$ cannot divide the greatest common divisor of $h(x)$ and $g(x)$. Thus $x - b$ is the greatest common divisor of $h(x)$ and $g(x)$ over some extension

Page No. (22)

of K. But then they have a nontrivial greatest common divisor over K, which must be a divisor of $x - b$. Since the degree of $x - b$ is 1, we see that the greatest common divisor of $g(x)$ and $h(x)$ in $K[x]$ is exactly $x - b$. Thus $x - b \in K[x]$, whence $b \in K$; remembering that $K = F(c)$, we obtain that $b \in F(c)$. Since $a = c - \gamma b$, and since $b, c \in F(c)$, $\gamma \in F \subset F(c)$, we get that $a \in F(c)$, whence $F(a, b) \subset F(c)$. The two opposite containing relations combine to yield $F(a, b) = F(c)$.

Unit - IV is completed

A simple induction argument extends the result from 2 elements to any finite number, that is, if $\alpha_1, \ldots, \alpha_n$ are algebraic over F, then there is an element $c \in F(\alpha_1, \ldots, \alpha_n)$ such that $F(c) = F(\alpha_1, \ldots, \alpha_n)$. Thus the

COROLLARY *Any finite extension of a field of characteristic* 0 *is a simple extension.*

Problems

1. If F is of characteristic 0 and $f(x) \in F[x]$ is such that $f'(x) = 0$, prove that $f(x) = \alpha \in F$.
2. If F is of characteristic $p \neq 0$ and if $f(x) \in F[x]$ is such that $f'(x) = 0$, prove that $f(x) = g(x^p)$ for some polynomial $g(x) \in F[x]$.
3. Prove that $(f(x) + g(x))' = f'(x) + g'(x)$ and that $(\alpha f(x))' = \alpha f'(x)$ for $f(x), g(x) \in F[x]$ and $\alpha \in F$.
4. Prove that there is no rational function in $F(x)$ such that its square is x.
5. Complete the induction needed to establish the corollary to Theorem 5.5.1.

An element a in an extension K of F is called *separable over* F if it satisfies a polynomial over F having no multiple roots. An extension K of F is called *separable* over F if all its elements are separable over F. A field F is called *perfect* if all finite extensions of F are separable.

6. Show that any field of characteristic 0 is perfect.
7. (a) If F is of characteristic $p \neq 0$ show that for $a, b \in F$, $(a + b)^{p^m} = a^{p^m} + b^{p^m}$.
   (b) If F is of characteristic $p \neq 0$ and if K is an extension of F let $T = \{a \in K \mid a^{p^n} \in F \text{ for some } n\}$. Prove that T is a subfield of K.
8. If K, T, F are as in Problem 7(b) show that any automorphism of K leaving every element of F fixed also leaves every element of T fixed.
*9. Show that a field F of characteristic $p \neq 0$ is perfect if and only if for every $a \in F$ we can find a $b \in F$ such that $b^p = a$.
10. Using the result of Problem 9, prove that any finite field is perfect.