Total No. of Questions: 6 *Total No. of Printed Pages:3*

Enrollment No.....

Faculty of Science

End Sem (Even) Examination May-2022

MA5CO06 Advance Abstract Algebra -II

Programme: M.Sc. Branch/Specialisation: Mathematics

Duration: 3 Hrs. **Maximum Marks: 60**

Note: All questions are compulsory. Internal choices, if any, are indicated. Answers of Q.1 (MCQs) should be written in full instead of only a, b, c or d.

Q.1 i. If A and B be two ideals of any ring R then which is the correct. **1**

(a) A + B is an ideal (b) AB is an ideal

(c) A + B and AB both are ideal (d) None of these

ii. Which is sub direct product of integral domains **1**

(a) Nil (b) Jacobson

(c) Both (a) and (b) (d) None of these

iii. Which is the correct property for Module: **1**

(a) $r\,(m_1+m_2) = rm_1+rm_2$ (b) $(r_1r_2)\,m = r_1(r_2m)$

(c) 1.m = m (d) All of these

iv. Direct product of modules is- **1**

(a) R module (b) Not a module

(c) Direct product is not possible (d) None of these

v. An R-Module M is said to be simple if it has sub modules: **1**

(a) 0 (b) M itself

(c) 0 and M itself (d) None of these

vi. A module over a ring generated by one element is called _____module. **1**

(a) Cyclic (b) Normal (c) Free (d) None of these

vii. The characteristic of any field is- **1**

(a) 0 (b) Prime number

(c) Either 0 or prime number (d) None of these

viii. The field $F[x]$ is- **1**

(a) PID (b) UFD

(c) Both (a) & (b) (d) PID but not UFD

P.T.O.

ix. If E is a finite extension of a field F, then **1**

(a) $\left|G\left(\frac{E}{F}\right)\right| = [E:F]$ (b) $\left|G\left(\frac{E}{F}\right)\right| \geq [E:F]$

(c) $\left|G\left(\frac{E}{F}\right)\right| \leq [E:F]$ (d) None of these

x. Solvable group is- **1**

(a) Abelian (b) Not abelian

(c) Abelian but not always (d) None of these

Attempt any two:

Q.2 i. Prove that intersection of two ideals is an ideal but union of two ideals is not necessary an ideal. Give an example. **5**

ii. State and prove fundamental theorem of homomorphism. **5**

iii. Let $A_1, A_2, \ldots\ldots A_n$ be left or right ideals in a ring R, then the following are equivalent: **5**

(a) $A = \sum_{i=1}^{n} A_i$ is a direct sum

(b) If $0 = \sum_{i=1}^{n} a_i$, $a_i \in A_i$, then $a_i = 0, i = 1,2,3 \ldots . n$

(c) $A_i \cap \sum_{j=1, j\neq i}^{n} A_j = (0), i = 1,2,3 \ldots . n$

Attempt any two:

Q.3 i. Prove the sub modules of the quotient module M / N are of the form U / N, where U is a sub module of M containing N. **5**

ii. Let M be left module over ring R then following are equivalent: **5**

(a) M satisfy Ascending chain condition

(b) M satisfy MAX

(c) M and it's all sub modules are finitely generated

iii. Let f be an R homomorphism of an R module M into R module N then $M / ker\, f \cong f(M)$. **5**

Attempt any two:

Q.4 i. State and prove Schur's lemma for simple module. **5**

ii. Write and prove structure theorem for modules over PID. **5**

iii. Let M be a finitely generated free module over commutative ring R. then all bases of M have the same number of elements. **5**

Attempt any two:

Q.5 i. Let $f(x) \in Z[x]$ be primitive. Then $f(x)$ is reducible over Q if and only if $f(x)$ is reducible over Z. **5**

ii. Prove that $\emptyset_p(x) = 1 + x + x^2 + \cdots + x^{p-1}$ is irreducible over Q, where p is prime. **5**

iii. If E is a finite separable extension of a field F, then E is a simple extension of F. **5**

Attempt any two:

Q.6 i. State and prove fundamental theorem of Galois theory. **5**

ii. Prove that every polynomial $f(x) \in C[x]$ factors into linear factors in $C[x]$. **5**

iii. If $f(x) \in C[x]$ is solvable by radicals over F if and only if its splitting field E over F has solvable Galois group $G(E/F)$. **5**

******

DATE
PAGE

Medicaps University
End Sem Exam 2022
M.Sc Advance Abstract Algebra-II
Solution (MA5C006)

Q1 MCQs

1. Ans. c A+B and AB both are ideal
2. Ans c Both (a) & (b)
3. Ans d All of the above
4. Ans a R-Module
5. Ans c 0 & M itself
6. Ans a Cyclic
7. Ans c Either 0 or Prime Number
8. Ans c PID and UFD both
9. Ans c $G(E/F) \leq [E:F]$
10. Ans a Abelian

Q2

i) Let S and T be two ideal of ring $(R,+,\cdot)$ then $S \neq \phi$, $T \neq \phi$ also S & T are both additive subgroup of R Show that additive identity of R $0 \in S$ and $0 \in T \Rightarrow 0 \in S \cap T$

$\Rightarrow S \cap T \neq \phi$ (1)

Now Since S and T are additive subgroup of R then $S \cap T$ is also additive subgroup of R.

Now $r \in R, s \in S \cap T \Rightarrow r \in R, s \in S$ and $s \in T$

Since S and T are ideal of R then (1)

$r \in R, s \in S \Rightarrow rs$ and $sr \in S$

$r \in R, s \in S \Rightarrow rs$ and $sr \in T$

Now $rs, sr \in S, T \Rightarrow rs, sr \in S \cap T$ (3)

$r \in R, s \in S \cap T \Rightarrow rs, sr \in S \cap T$

$\therefore S \cap T$ is also an ideal of ring R.

ii) Fundamental Theorem of Homomorphism

Let f be a homomorphism of a ring R onto a ring S with kernel N then (2)

$$R/N \cong \text{Im } f$$

Proof: Let us define $g(a+N) = f(a)$ then g is a mapping of R/N into $\text{Im } f$ for $a+N = b+N$ $\Rightarrow a-b \in N$ or $f(a-b) = 0$ This gives $f(a) - f(b) = 0$ So g is well defined. Next g is a homomorphism. writing $\bar{a}$ for $a+N$ we have

$$g(\bar{a}+\bar{b}) = g(\overline{a+b}) = f(a+b) \quad (2)$$
$$= f(a) + f(b)$$
$$= g(\bar{a}) + g(\bar{b})$$

Similarly $g(\bar{a}\bar{b}) = g(\bar{a})g(\bar{b})$

Clearly g is an onto mapping. (1)

we show g is 1-1. Let $f(a) = f(b)$ then $f(a-b) = 0$ So $a-b \in N$ but then $\bar{a} = \bar{b}$ this shows g is 1-1 Hence $R/N \cong \text{Im } f$

iii)

Proof: (i) $\Rightarrow$ (ii) follows from definition. (1)
of direct sum

(ii) $\Rightarrow$ (iii) Let $x \in A_i \cap \sum_{j=1, j\neq i}^{n} A_j$ then

$$x = a_1 + \cdots + a_{i-1} + a_{i+1} + \cdots + a_n \in A_i \quad (1)$$

Thus $0 = a_1 + \cdots + a_{i-1} + (-x) + a_{i+1} + \cdots + a_n$

then by (ii) we get $x = 0$

(iii) $\Rightarrow$ (i) let $a = a_1 + a_2 + \cdots + a_n$ and

$a = b_1 + b_2 + \cdots + b_n$ where $a_i, b_i \in A_i$ $i = 1, 2, \ldots n$ then (1)

$$0 = (a_1 - b_1) + (a_2 - b_2) + \cdots + (a_n - b_n)$$

this gives

$$a_1 - b_1 \in A_1 \cap \sum_{i=2}^{n} A_i = (0) \quad (2)$$

Hence $a_1 = b_1$ Similarly $a_2 = b_2 = \cdots a_n = b_n$

Hence $A = \sum_{i=1}^{n} A_i$ is a direct sum

Q3

1) Proof: Let $f : M \to M/N$ be a canonical (2)
Mapping that is $f(x) = x + N$, $x \in M$
Let X be an R Module of M/N. Consider
$U = \{ x \in M \mid f(x) \in X \}$ we claim that
U is an R Submodule of M.

For if $x, y \in U$ and $r \in R$ then (1)

$$f(x - y) = f(x) - f(y) \in X$$

and $f(rx) = r f(x) \in X$

which shows that U is an R submodule of M.

Also $N \subset U$ because for all $x \in N$ (2)
$f(x) = \bar{0} \in X$ Thus N is an R Submodule of U Also if $x \in X$ then there exists $y \in M$ such that $f(y) = x$ because f is onto Mapping so by def. of U $y \in U$ Hence $x \in f(U)$. clearly $f(U) \subset X$ thus $X = f(U)$ but $f(U) = U/N$ thus

$$X = U/N$$

DATE
PAGE

(ii) Proof: (i) ⇒ (ii)

Assume M satisfies Acc. let S be a non empty set of submodules of M Suppose S does not have a maximal number. Choose $N_1 \in S$. Since N_1 is not a maximal member of S, we can choose $N_2 \in S$ such that $N_1 \subset N_2$. Continuing in this way we can construct an ascending chain

$$N_1 \subset N_2 \subset N_3 \subset \cdots$$

(2)

(ii) ⇒ (iii) Assume that M satisfies MAX and N be a submodule of M. let S be the set of all finitely generated submodule of N where S is not empty since 0 is necessary a finite generated submodule of N. So S has a maximal element say

$L = \sum_{i=1}^{n} Ra_i$. if $L = N$ we are done. $a_{n+1} \in N \setminus L$ but $L \subsetneq L + Ra_{n+1}$

$= \sum_{i=1}^{n+1} Ra_i \in N$ Contradicting the maximality of L.

(2)

(iii) ⇒ (i)

(1)

Assume all submodules of M are f.g. let

$N_1 \subseteq N_2 \subseteq N_3 \subseteq \cdots$ be ascending chains of submodule of M

let $N = \bigcup_{k=1}^{\infty} N_k$ then N is a submodule of M and so N is f.g

$N = Ra_1 + Ra_2 + \cdots + Ra_n$

where $x_1, x_2, \cdots x_n \in N$ for each $i = 1, 2, \cdots n$

Hence $N = Rx_1 + Rx_2 + \cdots + Rx_m \subseteq N_M \subseteq N$

Therefore $N_M = N$ and so $N_k = N$ where $k \geq m$ hence M has ACC

iii) Proof :- Consider the Mapping

$$g : M/\ker f \to f(M) \quad \text{---(1)}$$

$$g(m + \ker f) = f(m)$$

g is well defined

$$m + \ker f = n + \ker f \quad (1)$$

$$g(m + \ker f) = g(n + \ker f)$$

$$f(m) = f(n)$$

$$\boxed{m = n}$$

∴ g is well defined

Now we show that g is 1-1 Mapping

Let $g(m + \ker f) = g(n + \ker f)$ (1)

$$f(m) = f(n)$$

$$f(m) - f(n) = 0'$$

$$f(m - n) = 0'$$

$$m - n = 0$$

$$\boxed{m = n}$$

g is 1-1 Mapping

g is onto Mapping →

obviously $f(m) = g(m + \ker f)$ (2)

by def.

let $m + \ker f, n + \ker f \in M/\ker f$

$\forall\ m, n \in M$ let

$$g[a(m + \ker f) + b(n + \ker f)]$$

$$= g[(am + bn) + \ker f]$$

$$= g\, f(am + bn) = af(m) + bf(n)$$

$$= a\, g(m + \ker f) + b\, g(n + \ker f)$$

$\therefore \frac{M}{\ker f} \cong f(M)$

→

Q4 ii) Schur's Lemma - Let M be a simple R module then $\text{Hom}_R(M, M)$ is a division ring (2)

If $f: M \to N$ is a Hom. of simple Module then either $f = 0$ or f is an isomorphism in particular ring $\text{End}_R(M)$ is a division ring for a simple module M.

Proof: Let $0 \neq \phi \in \text{Hom}_R(M, M)$ (1)

Consider the R-submodules $\ker\phi$ and $\text{Im}\,\phi$ of M. if $\ker\phi = M$ then $\phi = 0$ a contradiction

Thus $\ker\phi = (0)$ so ϕ is injective further if

$\text{Im}\,\phi = (0)$ then $\phi = 0$ (2)

a contradiction therefore $\text{Im}\,\phi = M$ which implies ϕ is surjective. Hence ϕ is bijective which proves that ϕ is invertible

iii) Proof:- Theorem States that if (1)

$R^m = R^n$ then $m = n$

Let $m < n$ let $\phi: R^m \to R^n$ be an R homomorphism and $\psi = \phi^{-1}$ let $(e_1 \dots e_m)$ and $(f_1 \dots f_n)$ be ordered bases of R^m and R^n resp let us

(17) Proof:

If F is a finite field then each finite extension E of F is simple. So suppose now that F is infinite Because E is a finite extension of F.

$E = F(a_1 - - a_n)$ where $a_i \in E$ (3)
$1 \le i \le n$ are algebraic over F we first show that if $E = F(\alpha, \beta)$ then there exist one element $\theta \in E$ such that $E = F(\theta)$ then the result will follow by induction.
Let $p(x)$ and $q(x)$ be the minimal Poly. nomial for α and β resp over F. Let the roots of $p(x)$ be $\alpha = \alpha_1 - - \alpha_n$ and let those of $q(x)$ be $\beta = \beta_1 - - \beta_m$ because E is a seperable extension of F, all α_i $1 \le i \le n$ and all β_j, $1 \le j \le m$ are distinct because F is infinite there exist $a \in F$ such that $a \ne (\alpha_i - \alpha)(\beta - \beta_j)$ for $1 \le i \le n$ $2 \le j \le m$ then
$a(\beta - \beta_j) \ne \alpha_i - \alpha$ so $a\beta + \alpha \ne \alpha_i + a\beta_j$ for $j \ne 1$ Set $\theta = a\beta + \alpha$ then $\theta - a\beta_j \ne \alpha_i$ for all $i = 1 - - n$ and $j = 2 - - m$
define $h(x) = p(\theta - ax) \in F(\theta)[x]$ then $h(\beta) = p(\alpha) = 0$ $h(\beta_j) = p(\theta - a\beta_j) \ne 0$ for $j \ne 1$ So β is a root of $h(x)$ but no β_j $(j \ne 1)$ is a root of $h(x)$ Also β is a root of $q(x)$, $q(x) \in F(\theta)[x]$ Let $A(x) \in F(\theta)[x]$ be a Minimal Poly. of β over $F(\theta)$ then $A(x) \mid h(x)$ and $A(x) \mid q(x)$ then any root of $A(x)$ is a root of $q(x)$ as well as root of $h(x)$

but only common root of β therefore (2)
$h(x) = x - \beta \Rightarrow \beta \in F(\theta)$ then
Since $\theta = a\beta + \alpha$, $\alpha \in F(\theta)$ hence
$F(\alpha, \beta) = F(\theta)$

96

1) Fundamental Theorem of Galois Theory
Let E be a Galois extension of F.
Let K be any subfield of E containing F
then the mapping $K \to G(E/K)$ sets up
a one to one corresponding the set of (2)
subfields of E containing F to the
subgroups of $G(E/F)$ such that

1) $K = E_{G(E/K)}$

2) for any subgroup H of $G(E/F)$
$H = G(E/E_H)$

3) $[E:K] = |G(E/K)|$, $[K:F] =$ index of
$G(E/K)$ in $G(E/F)$

4) K is a normal extension of F if
and only if $G(E/K)$ is a normal
subgroup of $G(E/F)$

5) If K is a normal extension of F
then $G(K/F) \simeq G(E/F)/G(E/K)$

Proof: By def of normality, E is a (1)
normal extension of K Thus K is the
fixed field of $G(E/K)$ Proves (1)
for Proof (2) needs only the fact that

E is a finite seperable extension of F. Because E is a normal extension of F and also of K we have

$$[E:K] = |G(E/K)| \quad (1)$$

$$[E:K] = |G(E/K)|$$

Thus $[E:F] = [E:K][K:F]$

gives $|G(E/F)| = |G(E/K)|[K:F]$

This proves $[K:F]$ = index of $G(E/K)$ in $G(E/F)$

$$\frac{G(E/F)}{G(E/K)} = T_1, T \in G(K/F) \quad (1)$$

$$\left|\frac{G(E/F)}{G(E/K)}\right| = [K:F]$$

Also because K is normal over F

$$|G(K/F)| = [K:F]$$

Hence

$$\left|\frac{G(E/F)}{G(E/K)}\right| = G(K/F)$$

Proof ii) let $f(x) = a_0 + a_1x + \cdots + a_nx^n \in C[x]$

let

$$g(x) = (x^2+1)(a_0 + a_1x + \cdots + a_nx^n)(\bar{a}_0 + \bar{a}_1x + \cdots + \bar{a}_nx^n) \quad (2)$$

$g(x) \in R[x]$

let F be the splitting field of $g(x)$ over R then $R \subset C \subset E$ we prove $E = C$

First we assert that there does not exist a subfield K of E containing C

such that $[K:C]=2$ Suppose that (3)
such subfield exists Because K is
finite seperable extension of C
$K = C(\alpha)$ for some $\alpha \in K$ if $p(x) \in C[x]$
is the minimal Polynomial of α over C
then deg $p(x) = 2$

Suppose

$$p(x) = x^2 + 2ax + b$$

$$p(x) = (x+a)^2 - (a^2 - b)$$

$$= (x+a-\sqrt{a^2-b})(x+a+\sqrt{a^2-b})$$

which is a contradiction because
$p(x)$ is irreducible over C which
Proves our assertion.

(2)

Proof (iii) First suppose that $G(E/F)$ is solvable
because Charact $F = 0$ E is normal
seperable extension so $[E:F] = |G(E/F)|$
$= n$. Assume that F contains a
Primitive nth root of unity then F
Contains Primitive mth roots of unity
for all Positive integers m that divide
n. let $G = G(E/F)$ Because G is
Solvable and finite there is a chain
$G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_r = (e)$
of subgroups of G such that
$G_i \lhd G_{i-1}$ and G_{i-1}/G_i is cyclic let
$F = F_0 \subset F_1 \subset \cdots \subset F_r = E$ be the
Corresponding subfields of E given by the
fundamental theorem then $E_{G_i} = F_i$ and

$$\varphi(e_i) = a_{1i} f_1 + \cdots + a_{ni} f_n \quad 1 \le i \le m \qquad (1)$$

$$\psi(f_j) = b_{1j} e_1 + \cdots + b_{mj} e_m \quad 1 \le j \le n$$

Let $A = (a_{ji})$ and $B = (b_{kj})$ be $n \times m$ and $m \times n$ matrices then

$$\psi\varphi(e_i) = \sum_{k=1}^{m} \sum_{j=1}^{n} b_{kj} a_{ji} e_k \quad 1 \le i \le m$$

Thus by linear independence of the e_i's and by $\psi = \varphi^{-1}$ we have

$$\sum_{j=1}^{n} b_{kj} a_{ji} = \delta_{ki} \qquad (3)$$

This yields

$$BA = \begin{bmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & & \vdots \\ b_{m1} & \cdots & b_{mn} \end{bmatrix} \begin{bmatrix} a_{11} & \cdots & a_{m1} \\ \vdots & & \\ a_{n1} & \cdots & a_{nm} \end{bmatrix} = I_m$$

where I_m is the $m \times m$ identity matrix

Similarly $AB = I_n$ Let

$$A' = [A \; 0] \quad B' = \begin{bmatrix} B \\ 0 \end{bmatrix}$$ be $n \times n$ augmented matrix then

$$A'B' = I_n \qquad B'A' = \begin{bmatrix} I_m & \vdots \\ 0 & 0 \end{bmatrix}$$

$\Rightarrow \det(A'B') = 1$ and $\det(B'A') = 0$

but A', B' are $n \times n$ matrices over commutative rings so $\det(A'B') = \det(B'A')$ which yields contradiction hence $m \ge n$ by symmetry $n \ge m \Rightarrow \boxed{m = n}$

Q.5 i) Gauss Lemma

Proof:- If $f(x)$ is reducible over $\mathbb{Z}$ then trivially $f(x)$ is reducible over $\mathbb{Q}$ (1)

Conversely

Suppose $f(x)$ is reducible over $\mathbb{Q}$.

Let $f(x) = u(x)v(x)$ with $u(x), v(x) \in \mathbb{Q}[x]$ and $u(x) \notin \mathbb{Q}$, $v(x) \notin \mathbb{Q}$ (4)

then $f(x) = (a/b)u'(x)v'(x)$ where

$u'(x), v'(x)$ are Primitive Polynomials in $\mathbb{Z}[x]$ then $bf(x) = a(u'(x)v'(x))$

The g.c.d of Coeff of $bf(x)$ is b and g.c.d of Coeff $a(u'(x)v'(x))$ is a by Lemma of Primitive Polynomial

$b = \pm a$ so $f(x) = \pm u'(x)v'(x)$

therefore $f(x)$ is reducible over $\mathbb{Z}$.

⟶

ii) Write $\phi_p(x) = (x^p - 1)/(x-1)$ (1)

$g(x) = \phi_p(x+1) = ((x+1)^p - 1)/((x+1)-1)$ (1)

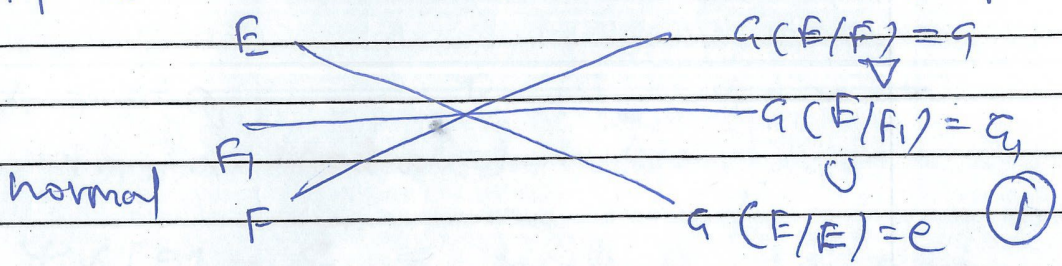
$= \frac{1}{x}\left(x^p + \binom{p}{1}x^{p-1} + \cdots + \binom{p}{p-1}x\right)$ (1)

$= x^{p-1} + \binom{p}{1}x^{p-2} + \cdots + \binom{p}{p-1}$ (1)

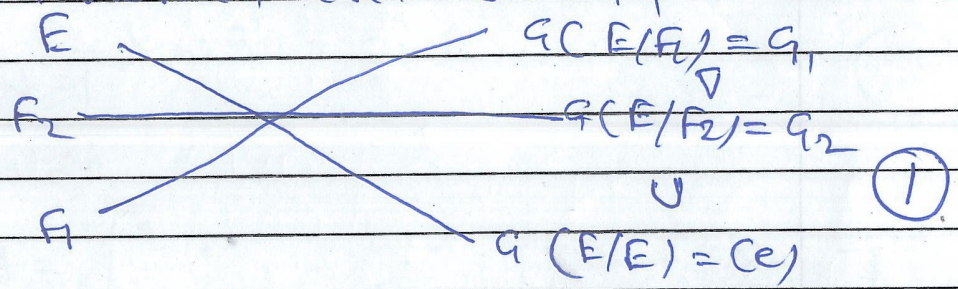
Clearly p divides all the Coefficients except that of x^{p-1} and p^2 does not divide Constant term. Thus $g(x)$ is irreducible over $\mathbb{Q}$. Hence $\phi_p(x)$ is also irreducible over $\mathbb{Q}$ (1)

$G(E/F_i) = G_i$ Also by fundamental theorem $G_i = G(E/F_i) \lhd G(E/F) = G$

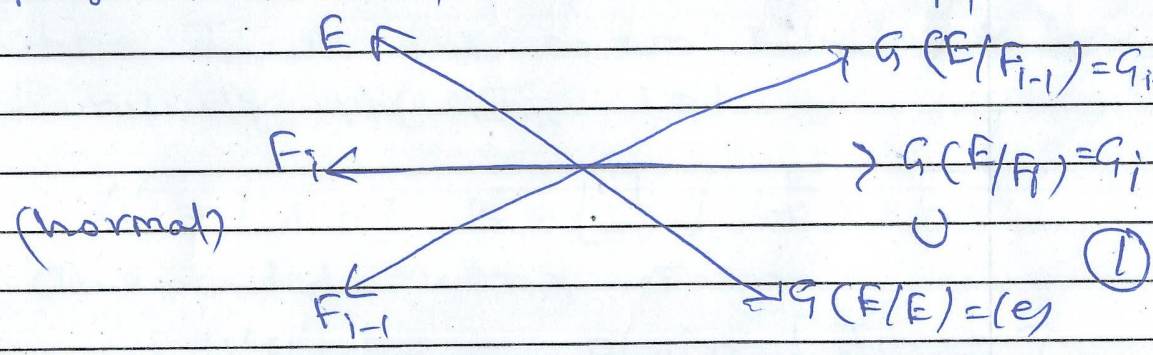
$\Rightarrow F_i$ is a normal extension of F



Now E can be regarded as the splitting field of $f(x)$ over F_i. So F is a finite normal extension of F_i then $G_2 \lhd G_1$ implies F_2 is a normal extension F_1



Continue in this way to show that F_i is a normal extension of F_{i-1}



Furthermore $G(F_i/F_{i-1}) = G(E/F_{i-1}) / G(E/F_i)$

$= G_{i-1}/G_i$ by the fundamental theorem