UNIT 12 : FACTORIZATION IN INTEGRAL DOMAIN AND FIELD EXTENSION

UNIT STRUCTURE

12.1 Learning Objectives

12.2 Introduction

12.3 Associates, Irreducible and Prime Elements of Integral Domain: Definitions and Examples

12.4 Properties of Associates, Irreducible and Prime Elements of Integral Domains

12.5 Principal Ideal Domains : Definitions and Examples

12.6 Properties of PID

12.7 Unique Factorization Domains : Definitions and Examples

12.8 Properties of UFD

12.9 Euclidean Domains : Definitions and Examples

12.10 Properties of ED

12.11 Field Extensions : Definitions and Examples

12.12 Propertes of Field Extensions

12.13 Let Us Sum Up

12.14 Further Readings

12.15 Answers To Check Your Progress

12.16 Model Questions

12.1 LEARNING OBJECTIVES

After going through this unit, you will able to-

- know about associates, irreducible and prime elements of a commutative ring with unity
- learn about PID, UFD and ED
- appreciate the significance of unique factorization in rings and integral domain
- know about the significance of field extensions
- provide important results on algebraic extension, transcendental extension, Minimal polynomials, degree of extension and splitting fields.

12.2 INTRODUCTION

In number theory one comes across the Fundamental Theorem of Arithmetic which states that any integer n>1 is expressible as a product of powers of distinct primes and this expression is unique to within order. In this unit we intend to generalize this result to the elements of certain special domains whose definitions are motivated by the properties of ring of integers. In this unit we shall be mainly concerned with commutative ning with unity

The concept of field has a central place in algebra. It has wide applications in Linear Algebra and in the theory of equations, which deal with the study of roots of polynomials. In this unit we shall also concerned with the development of that part of the theory of fields which has direct applications to the theory of Equations.

12.3 ASSOCIATES, IRREDUCIBLE AND PRIME ELEMENTS OF INTEGRAL DOMAIN: DEFINITIONS AND EXAMPLES

Definition: (Associates) Elements a and b of an integral domain D are called associates if a = ub, where u is a unit of D.

Example 1. In z, –3 and 3 are associates as –1 is a unit. In fact the only units in Z are 1 and –1; so every nonzero integer $\sqrt{n}$ has two associates namely –n and n.

Example 2. In $Z/\langle 8\rangle$ only units are $\bar{1}$, $\bar{3}$, $\bar{5}$ and $\bar{7}$. The associates of $\bar{2}$ are therefore $\bar{2}$ and $\bar{6}$.

Example 3. In Z [i] = {a+bi |a, b∈Z, i = $\sqrt{-1}$} the units are 1, –1, i, –i. So the associates of 2+3i are 2+3i, –2 –3i, 2i–3 and 3–2i.

Definition: (Prime element) A nonzero element p of an integral domain D is called prime if

(i) p is not a unit and

(ii) p|ab implies p|a or p|b

Example 1. In Z, every prime number is a prime element.

Example 2. In $Z[\sqrt{5}] = \{a+b\sqrt{-5} : a,b \in z\}, \sqrt{5}$ is prime element since if

$\sqrt{-5} \mid (a+b\sqrt{-5})(c+d\sqrt{-5})$ for some a, b, c, d $\in Z$

$\Rightarrow (a+b\sqrt{-5})(c+d\sqrt{-5}) = \sqrt{-5}(x+y\sqrt{-5})$ for some x, y $\in Z$

$\Rightarrow (a^2+5b^2)(c^2+5d^2) = 5(x^2+5y^2)$

$\Rightarrow 5 \mid (a^2+5b^2)(c^2+5d^2)$

$\Rightarrow 5 \mid a^2c^2+5a^2d^2+5b^2c^2+25b^2d^2$

$\Rightarrow 5 \mid a^2c^2$

$\Rightarrow 5 \mid a^2$ or $5 \mid c^2$

$\Rightarrow 5 \mid a$ or $5 \mid c$

Let 5|a. Then $\sqrt{-5} \mid a$ as $5 = (\sqrt{-5})(-\sqrt{-5})$

Therefore $\sqrt{-5} \mid a+b\sqrt{-5}$.

Similarly in case 5|c we get $\sqrt{-5} \mid c+d\sqrt{-5}$

Definition: (Irreducible element) A nonzero element a of an integral domain D is called irreducible if

(i) a is not a unit and

(ii) whenever b, c $\in$ D with a = bc, then b or c is a unit.

Example 1. In Z, the prime numbers are irreducible elements.

Example 2. In $Z[\sqrt{-5}]$, the units are 1 and –1. We claim that 3 is irreducible in $Z[\sqrt{-5}]$.

Let $3 = (a+b\sqrt{-5})(c+d\sqrt{-5})$ for some a, b, c, d $\in$ z, where both $a+b\sqrt{-5}$ and $c+d\sqrt{-5}$ are non units units. Then $9 = (a^2+5b^2)(c^2+5d^2)$

$\Rightarrow a^2+5b^2 = 1$, $c^2+bd^2 = 9$ or $a^2+5b^2=3$, $c^2+5d^2 = 3$ or $a^2+5b^2 = 9$, $c^2+5d^2=1$.

If $a^2+5b^2 = 1$, then the only integral solutions are $a = \pm 1$, b = 0 since 5>1.

If $a^2+5b^2 = 3$, then there is no integral solutions.

If $c^2+5d^2 = 1$, then c = 1, d = 0.

Thus $3 = (a+b\sqrt{-5})(c+d\sqrt{-5})$

$\Rightarrow a+b\sqrt{-5} = \pm 1$ or $c+d\sqrt{-5} = \pm 1$

So 3 is an irreducible element of $z[\sqrt{-5}]$.

Note that 3 is not prime since

$$3 \mid 9 = (2+\sqrt{-5})(2-\sqrt{-5})$$

but $3 \nmid 2+\sqrt{-5}$ and $3 \nmid 2-\sqrt{-5}$.

Remark : The distinction between primes and irreducibles is best illustrated by integral domain of the form $z[\sqrt{d}] = \{a+b\sqrt{d} : a, b \in z\}$, where d is not 1 and is not divisible by the square of a prime. To analyze these rings, we need a convenient method of determining their units, irreducibles and primes. To do this, we define a function $N : Z[\sqrt{d}] \to N$ by

$N(a+b\sqrt{d}) = |a^2 - db^2|$

Then (i) $N(x) = 0 \Leftrightarrow x = 0$

(ii) $N(x.y) = N(x)\, N(y)$ for all x and y

(iii) x is a unit $\Leftrightarrow N(x) = 1$

(iv) N(x) is prime $\Rightarrow$ x is irreclucible in $Z[\sqrt{d}]$

Example 1. Consider the integral domain

$Z[\sqrt{-3}] = \{a+b\sqrt{-3} : a, b \in Z\}$

Here $N(a+b\sqrt{-3}) = |a^2-(-3)b^2|$

$= |a^2+3b^2|$

$= a^2+3b^2$ $[\because a^2+3b^2 > 0)$

Consider $1+\sqrt{-3}$. Suppose

$1+\sqrt{-3} = xy$, where neither x nor y is unit.

$N(x)\, N(y) = N(xy)$

$= N(1+\sqrt{-3})$

$= 1^2+3.1^2$

$= 4$

$\Rightarrow N(x) = 2$

But there no integers a and b that satisfy $a^2+3b^2 = 2$. Thus x or y is a unit and hence $1+\sqrt{-3}$ is an irreducible element in $Z[\sqrt{-3}]$.

Again $(1+\sqrt{-3})(1-\sqrt{-3}) = 4\ 4 = 2.2$

$\Rightarrow 1+\sqrt{-3} \mid 2.2$

But $1+\sqrt{-3} \nmid 2$. Thus $1+\sqrt{-3}$ is not a prime.

12.4 PROPERTIES OF ASSOCIATES, IRREDUCIBLE AND PRIME ELEMENTS OF INTEGRAL DOMAINS

Theorem 12.4.1. Let D be an integral domain. Then the following holds.

(i) The relation of being associates is an equivalance relation in D.

(ii) If a, b are two non-zero elements of D, then a is an associate of b $\Leftrightarrow$ a/b and b/a.

(iii) If a, b are nonzero elements of D, then a/b and b/a $\Leftrightarrow \langle a \rangle = \langle b \rangle$.

Proof : (i) Let D be an integral domain and define a relation ~ : $D \to D$ by a ~ b $\Leftrightarrow$ a associates b

Reflexivity : For any $a \in D$, a = 1a

i.e. a associates a. i.e. a ~ a

Symmetricity : Let a, $b \in D$ such that

a~b $\Rightarrow$ a associates b

$\Rightarrow$ a = ub, where u is an unit in D

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

$\Rightarrow$ b~a as u^{-1} is again a unit in D.

Transitivity : Let a, b, $c \in D$ such that

a~b, b~c

$\Rightarrow$ a = ub, b = vc for some unit u, $v \in D$

$\Rightarrow$ a = uvc

$\Rightarrow$ a~c as u, v are units in D $\Rightarrow$ uv is also an unit in D.

Thus ~ is an equivalence relation in D.

(ii) Let a is an associate of b. Then a = ub for some unit u in D.

$\Rightarrow$ b|a

Again a is an associate of b

$\Rightarrow$ b is an associate of a

$\Rightarrow$ b = va for some unit in D

$\Rightarrow$ a|b

Conversely, let a, $b \in D$ and

a|b and b|a

$\Rightarrow$ b = ua and a = vb for some u, $v \in D$.

$\Rightarrow$ ab = uv(ab)

$\Rightarrow$ ab (a–uv) = 0

$\Rightarrow$ 1–uv = 0 [$\because a \neq 0, b \neq 0$ and D is an integral domain]

$\Rightarrow$ uv = 1

$\Rightarrow$ u is an unit in D.

$\therefore$ b = ua, where a is an unit in D.

$\Rightarrow$ a is an associate of b.

(iii) Let a, b two nonzero element of D such that a|b and b|a.

$\Rightarrow$ b = ua and a = vb for some u, v $\in$ D.

$\Rightarrow b \in \langle a \rangle$ and $a \in \langle b \rangle$

$\Rightarrow b \in \langle b \rangle \subseteq \langle a \rangle$ and $a \in \langle a \rangle \subseteq \langle b \rangle$

$\Rightarrow \langle a \rangle = \langle b \rangle$.

Conversely, let $\langle a \rangle = \langle b \rangle$. Then

$a \in \langle b \rangle$

$\Rightarrow$ a = ub for some uD

$\Rightarrow$ b|a

In the same way <b>=<a> gives a|b.

Theorem 12.4.2. In an integral domain, every prime is an irreducible.

Proof : Suppose that p is a prime in an integral domain and p = ab. We must show that a or b is a unit. By the definition of prime, we know that p|a or p|b. Let p|a. Then a = pt

and 1a = a = pt = abt = a (bt)

$\Rightarrow$ bt = 1

$\Rightarrow$ b is a unit.

Thus p is irreducible.



CHECK YOUR PROGRESS

Q 1: Find all the units in Z [i].

Q 2: Find all the units in Z [$\sqrt{-5}$].

Q 3: Show that 1+i is an irreducible element in Z [i].

Q 4: Show that in Z_6, $\bar{2}$ is a prime element but not irreducible.

12.5 PRINCIPAL IDEAL DOMAINS : DEFINITIONS AND EXAMPLES

Definition: (Principal Ideal) : Let R be a ring. Then the ideal generated by a singleton subset of R is called a principal ideal.

Let {a} $\subseteq$ R. Then the ideal generated by {a} is called a principal ideal and it is denoted by $\langle a \rangle$.

Definition: (Principal Ideal domain) Let D be an integral domain with unity. Then D is called a PID if every ideal of D is a principal ideal.

Example 1. Consider the integral domain Z. Let A be a nonzero ideal of Z. We have to show A is principal ideal.

Since $A \neq (0)$. therefore there exist $a(\neq 0) \in A$. We may assume a as positive integer (for if $a < 0$, then we can consider $-a$ as a).

Let A_+ be the subset of A containing positive integers. By well ordering principle, there exists a least positive integer in A_+.

Claim : $A = \langle n \rangle$ i.e. $A = nZ$.

Let $x \in \langle b \rangle$. Then $x = nz$ for some $z \in Z$

$\Rightarrow x \in A$ [$n \in A_+ \subseteq A$ and A is an ideal of Z]

$\therefore \langle n \rangle \subseteq A$

Next, let $y \in A$. Then by division algorithm, there exists $q, r \in z$ such that

$y = nq + r$ where $0 \leq r < n$

We consider $r \neq 0$. Then $0 < r < n$. Now

$y = nq + r$

$\Rightarrow r = y - nq \in A$ [$\because y \in A, n \in A \Rightarrow y \in A, nq \in A \Rightarrow y - nq \in A$]

$\Rightarrow$ r is a positive integer less than n such that $r \in A$.

$\Rightarrow r \in A_+$ and $r < n$

Which contradicts the fact that n is the least positive integer in A_+.

Hence $r = 0 \Rightarrow y = nq \in nZ = \langle n \rangle$

$\therefore A \subseteq \langle n \rangle$

Thus $A = \langle n \rangle$ and hence A is a principal ideal.

If $A = (0)$, then $A = \langle a \rangle$

Thus every ideal of Z is a principal ideal. Hence Z is a PID.

Example 2. Let F be a field. Then F[x] is an integral domain with unity.

Let A be a nonzero ideal of F[x]. Then there exists a nonzero polynomial f(x) in A.

Let g(x) be the polynomial of least degree in A.

Claim : $A = \langle g(x) \rangle$

Let $y \in \langle g(x) \rangle$

$\Rightarrow y = h(x)\, g(x)$ where $h(x) \in F[x]$.

$\Rightarrow y \in A$ [$\because$ A is an ideal of F[x]]

$\therefore \langle g(x) \rangle \subseteq A$ (1)

Next, let $f(x) \in A$. Then by division algorithm, there exists $q(x), r(x) \in F[x]$ such that $f(x) = g(x)\, q(x) + r(x)$

Where either $r(x) = 0$ or $\deg r(x) < \deg g(x)$.

Let $r(x) \neq 0$. Then $f(x) = g(x)\, q(x) + r(x)$

$\Rightarrow r(x) = f(x) - g(x)\, q(x) \in A$ [$\because f(x), g(x) \in A$ and A is an ideal of F[x]]

This contradicts the fact that g(x) is the polynomial of least degree. Thus $r(x) = 0$ and

$f(x) = g(x)\, q(x) \in \langle g(x) \rangle$

$\therefore A \subseteq \langle g(x) \rangle$ (2)

From (1) and (2), we get $A = \langle g(x) \rangle$.

Thus every ideal of F[x] is a principal ideal and hence F[x] is a PID.

Example 3. Every field is a PID. The only ideals of a field F are (0) and F itself. Since for each $x \in F$, $x = x.1$ yields $x \in \langle 1 \rangle$, so $F = \langle 1 \rangle$. Hence every ideal of F is principal and which implies F is a PID.

12.6 PROPERTIES OF PID

Theorem 12.6.1. In a PID, an element is an irreducible if and only if it is a prime.

Proof : Theorem 12.4.2 shows that primes are irreducible. To prove the converse, let a be an irreducible element of a PID D and suppose that a|bc. We must show that a|b or a|c.

Consider the ideal

$I = \{ax + by | x, y \in D\}$

and let $\langle d \rangle = I$. Since $a \in I$, we can write $a = dr$

and because a is irreducible, d is a unit or r is a unit.

If d is a unit, then I = D and we may unit

$I = ax + by$

$\Rightarrow c = acx + bcy$ and

$a | acx + bcy$

$\Rightarrow a | c$

On the other hand, if r is a unit, then $\langle a \rangle = \langle d \rangle = I$, and, because $b \in I$, there is an element t in D such that

$$at = b$$

$$\Rightarrow a|b$$

Theorem 12.6.2. Let R be a PID which is not a field. Then any proper ideal A of R is a maximal ideal if and only if it is generated by an irreducible element of R.

Proof : Since R is a PID but not a field, therefore there exists an element $a(\neq 0) \in R$ such that a is not a unit in R. Then

$\langle 0 \rangle \subset \langle a \rangle \subseteq R$

$\Rightarrow \langle 0 \rangle$ is not a maximal ideal.

Let A be a maximal ideal of R. Then $A \neq \langle 0 \rangle$. Since R is a PID, so there exists $p(\neq 0) \in R$ such that

$A = \langle p \rangle$

We have to show that p is an irreducible element.

Since A is maximal, so $A \neq R$ and

$1 \notin A$

$\Rightarrow 1 \notin \langle p \rangle$

$\Rightarrow$ p is not a unit.

Next, let p = ab, where $a, b \in R$. Then

$\langle p \rangle \subseteq \langle a \rangle$ $\quad [\because t \in \langle p \rangle \Rightarrow t = pt' = abt' = a(bt') \in \langle a \rangle]$

$\Rightarrow \langle p \rangle \subseteq \langle a \rangle \subseteq R$

Since $\langle p \rangle$ is maximal, so either $\langle p \rangle = \langle a \rangle$ or $\langle a \rangle = R$

If $\langle p \rangle = \langle a \rangle$, then $a = 1.a \in \langle a \rangle$

$\Rightarrow a \in \langle p \rangle$

$\Rightarrow a = pr, r \in R$

$\Rightarrow ab = prb$

$\Rightarrow p = prb$

$\Rightarrow rb = 1$

$\Rightarrow$ b is a unit.

If $\langle a \rangle = R$, then $1 = as, s \in R$

$\Rightarrow$ a is a unit.

Thus p = ab $\Rightarrow$ either a is a unit or b is a unit

$\Rightarrow$ p is an irreducible element.

Conversely, let p be an irreducible element and let $A = \langle p \rangle$. We have to prove A is a maximal ideal of R.

Since p is not a unit, so $A \neq R$. Let J be an ideal of R such that

$A \subseteq J \subseteq R$.

Since R is a PID, so

J is a principal ideal.

$\Rightarrow \exists\ x(\neq 0) \in R$ such that $J = \langle x \rangle$ and so

$\langle p \rangle \subseteq \langle x \rangle \subseteq R$

$\Rightarrow x \notin \langle p \rangle = A$

If $x \in A$, then $r\,x \in A$ for all $x \in R$

$\Rightarrow \langle x \rangle \subseteq A$

Which is a contradition to the fact that $A \subseteq \langle x \rangle$.

Since $\langle p \rangle \subseteq \langle x \rangle$ so $p = 1.p \in \langle p \rangle \subseteq \langle x \rangle$

$\Rightarrow p = xy$ for some $y \in R$

As p is irreducible, one of x and y must be unit

If y is a unit, then $x = py^{-1} \in \langle p \rangle = A$

$\Rightarrow x \in A$

Which is a contradiction.

Hence x must be a unit.

$\Rightarrow \exists\ x' \in R$ such that $xx^{-1} = \in \langle x \rangle$

$\Rightarrow 1 \in J$

$\Rightarrow J = R$

Thus A is a maximal ideal of R.

Theorem 12.6.3. In a PID, any strictly increasing chain of ideals $I_1 \subset I_2 \subset \ldots$ must be finite in length.

Proof : Let $I_1 \subset I_2 \subset \ldots$ be a chain of strictly increasing ideals in a PID D and let $I = UI_k$. Then I is an ideal of D.

Since D is a PID, there is an element a in D such that $I = \langle a \rangle$. Because $a \in I$ and $I = UI_k$, a belongs to some member of the chain, say $a \in I_n$. Then clearly, for any member I_i of the chain, we have

$I_i \subseteq I = \langle a \rangle \subseteq I_n$

Therefore I_n must be the last member of the chain.



CHECK YOUR PROGRESS

Q 5: Show that Z [x] is not a PID.

Q 6: Show that an ideal $\langle p \rangle$ in Z is maximal if and only if p is a prime number.

Q 7: Show that the ideal $\langle x+2 \rangle$ is maximal in Q[x].

Q 8: Let R be a PID. Show that every pair of nonzero elements have ged and LCM. If gcd(a, b) = d, then show that d = ax+by for some x, $y \in R$.

12.7 UNIQUE FACTORIZATION DOMAINS : DEFINITIONS AND EXAMPLES

Definition: (Unique Factorization Domain (UFD)) An integral domain D is a unique factorization domain if

(i) every nonzero element of D that is not a unit can be written as a product of irreducible of D; and (ii) If $a = p_1^{n_1}.p_2^{n_2}.\ldots.p_k^{n_k}$ and $a = q_1^{m_1}.q_2^{m_2}.\ldots.q_r^{m_r}$ are two expression as product of irreducible elements, where no two of the p_i'.s are associates and no two of the a_j's are associates, then k = r, each p_i is an associate of one and only one q_j and $n_i = m_j$.

Example 1. Ring Z is a UFD, since in Z every integer different from –1, 0 and 1 is expessible as a product of finite number of prime numbers and this expression is unique except for order and sign. Notice that in Z, the prime numbers all nothing but irreducible elements and their negatives are also irreducible elements, i.e. –3 and 3 both are irreducible elements.

Example 2. Every field F is a UFD, since if it were not, we would have found a nonzero non-unit in F which is not expressible as a product of irreducible elements. But in a field there is no nonzero non-unit.

Example 3. $Z[\sqrt{-5}]$ is an integral domain which is not a UFD, since $46 \in Z[\sqrt{-5}]$ is a nonzero non-unit element and we can express it as product of irreducibles in two ways

$46 = 2 \cdot 23$

$46 = (1+3\sqrt{-5})\,(1-3\sqrt{-5})$

but 2 is not associate of $1+3\sqrt{-5}$ or $1-3\sqrt{-5}$.

12.8 PROPERTIES OF UFD

Theorem 12.8.1. In a UFD every irreducible element is prime.

Proof : Let D be UFD and p be an irreducible element in D. Then $p \neq 0$ and p is not a unit. We have to prove p is a prime.

Let $a, b \in D$ such that p|ab. We have to prove p|a or p|b.

Now $p|ab \Rightarrow ab = pc$ for some $c \in D$.

As p is not a unit both a and b cannot be unit (for if both a and b are units, then ϕ is also a unit).

Case (I). If a is a unit, then ab = pc

$\Rightarrow b = pca^{-1}$

$\Rightarrow p|b$

Case (II). If b is a unit, then ab = pc

$\Rightarrow a = pcb^{-1}$

$\Rightarrow p|a$

Case (III). If a and b both are not units, then ab = pc implies c is not a unit. If c is a unit, then ab and p are associates. But p is irreducible, so ab are also irreducible. Then one of a and b must be a unit. This is a contradiction.

Thus a, b, c are not units.

Since D is a UFD, a, b and c can be expressed as product of finite number of irreducible elements.

Let $a = p_1 p_2 p_3 \ldots . p_k$

$b = q_1 q_2 q_3 \ldots . q_l$

$c = r_1 r_2 r_3 \ldots . r_m$

Where p_i's. q_j's and r_t's are irreducible elements.

Now ab = pc

$\Rightarrow p_1 p_2 p_3 \ldots . p_k \; q_1 q_2 q_3 \ldots . q_l = pr_1 r_2 r_3 \ldots . r_{n1}$

$\Rightarrow$ p is an associate of some p_i or some q_j where $i \in \{1, 2, 3, \ldots, k\}$ and $j \in \{1, 2, 3, \ldots ., l\}$.

If p is an associate of p_i, then

$p_i = px$ where x is a unit

$\Rightarrow p|p_i$

$\Rightarrow p|p_1\, p_2\, p_3 \ldots . p_k$

$\Rightarrow p|a$

If p is an associate of q_j, then p|b.

Thus $p|ab \Rightarrow p|1|$ or p|b

Hence p is a prime

Theorem 12.8.2. Every PID is a UFD.

Proof : Let D be a PID. We have to prove D is a UFD. Let $a(\neq 0) \in D$ be a non-unit element. Then there exists an irreducible element p_1 such that $p_1|a$ and which implies $a = p_1a_1$ for some $a_1 \in D$.

If a_1 is a unit, then a and p_1 are associates. Also p_1 is irreducible and so a is irreducible and hence there is nothing to prove.

If a_1 is not a unit, then $\langle a_1 \rangle \neq D$ and

$a = p_1a_1 \Rightarrow \langle a \rangle \subseteq \langle a_1 \rangle$ [$\because x \in \langle a \rangle \Rightarrow x = ar = p_1a_1r = a_1(p_1r) \in \langle a \rangle$]

If $\langle a \rangle = \langle a_1 \rangle$, then

$a_1 \in \langle a_1 \rangle = \langle a \rangle$

$\Rightarrow a_1 = ax$ for some $x \in D$

$\Rightarrow a_1 = p_1a_1x$

$\Rightarrow p_1x = 1$

$\Rightarrow p_1$ is a unit.

Which is a contradiction. Thus $\langle a \rangle \neq \langle a_1 \rangle$ and so $\langle a \rangle \subset \langle a_1 \rangle$

Since a_1 is a non-unit, so we get an irreducible element p_2 such that $p_2|a_1$

$\Rightarrow a_1 = p_2a_2$ for some $a_2 \in D$.

If a_2 is a unit, then a_1 and p_2 are associates and p_2 being irreducible we get a_1 is also irreducible. Thus we get $a = p_1a_1$, product of two irreducible elements.

If a_2 is not a unit, then $\langle a_2 \rangle \neq D$ and

$a_1 = p_2a_2 \Rightarrow \langle a_1 \rangle \subseteq \langle a_2 \rangle$.

If $\langle a_1 \rangle = \langle a_2 \rangle$, then we get p_2 is a unit, which is not possible.

So $\langle a_1 \rangle \subset \langle a_2 \rangle$.

Continue this process, we get an ascending chain of ideals of D.

$\langle a \rangle \subset \langle a_1 \rangle \subset \langle a_2 \rangle \subset \ldots .$

Such a chain of ideals must be finite. Thus for some n, a_{n+1} must be

a unit and

$a_n = p_{n+1}a_{n+1}$

$\Rightarrow a_n$ and p_{n+1} are associates and p_{n+1} being irreducible, we find a_n is irreducible. Thus

$a = p_1a_1 = p_1(p_2a_2)$

$= p_1p_2(p_3a_3)$

- - - - - - - -

- - - - - - - -

$= p_1p_2$ - - - - (p_na_n)

$= p_1p_2$ - - - - p_na_n

$= p_1p_2$ - - - - p_np_{n+1} taking a_n as p_{n+1}

$\Rightarrow a$ can be expressed as finite product of irreducible elements.

Let $a = q_1q_2$ - - - q_m be another representation of a as product of irreducible elements. We have to prove n+1 = m and each p_1 is an associate of some q_j and each q_j is an associate of some p_1, $I \leq i \leq n+1$, $I \leq j \leq m$.

$a = p_1p_2p_3$ - - - $p_{n+1} = q_1q_2q_3$ - - - q_m

We apply induction on n+1. If n = 0, the result is trivial.

We assume that the result holds for all those nonzero non-units which are expressible as product of less than n+1 elements.

p_1p_2 - - - $p_{n+1} = q_1q_2$ - - - q_m

$\Rightarrow q_1 | p_1p_2$ - - - p_{n+1}

$\Rightarrow q_1 | p_i$ for some i (as each irreducible element in a PID is a prime element)

$\Rightarrow p_i = q_1x_i$ where x_i must be a unit for p_i is irreducible.

$\Rightarrow q_1 = p_i\, x^{-1}_i = p_iu_i$ where $u_i = x^{-1}_i$

By renumbering the p_i's, we can take i = 1. Then

p_1p_2 - - - $p_{n+1} = p_1u_1q_2q_3$ - - - q_m

$\Rightarrow p_2p_3$ - - - $p_{n+1} = u_1q_2q_3$ - - - q_m

$\Rightarrow p_2p_3$ - - - $p_{n+1} = q'_2q_3$ - - - q_m where $q'_2 = u_1q_2$

If we put $b = p_2p_3$ - - - p_{n+1}, then

$b = q'_2q_3$ - - - q_m

We have two expressions of b product of n irreducible elements. Since n < n+1, by induction hypothesis $n = m-1 \Rightarrow m = n+1$ and each p_i is

an associate of some q_j's $\forall$ i, $2 \le i \le n+1$ and $\forall$ j, $2 \le j \le m$.

Also $q_1 = p_1 u_1 \Rightarrow p_1$ and q_1 are associates.

Thus each p_i is an associate of some q_j for all i, $1 \le i \le n+1$ and for all j, $1 \le j \le m$ and vice versa.

Hence D is a UFD.

Lemma 12.8.3. If D is a UFD, then every nonzero polynomial in D[x] is a product of a primitive polynomial over D and an element of D.

Proof : Let $f(x) = a_0+a_1x+a_2x^2+- - -+a_nx^n$ be a non zero polynomial in D[x], where d is a UFD. Let d be the HCF of $a_0, a_1, a_2, - - -, a_n$ in D. Then

$a_i = db_i$ for some $b_i \in D$ $\forall$ i = 0, 1, 2, - - -, n.

Since HCF $(a_0, a_1, a_2, - - -, a_n) = d$, so HCF$(b_0, b_1, - - -, b_n) = 1$

This proves that

$f(x) = d(b_0+b_1x+b_2x^2+ - - -+b_nx^n)$

$= dg(x)$, where $g(x) = b_0+b_1x+b_2x^2+ - - -+b_nx^n \in D[x]$ and HCF$(b_0, b_1, b_2, - - -, b_n) = 1$, i.e. g(x) is primitive.

Theorem 12.8.4. The product of two primitive polynomials over a UFD is a primitive polynomial.

Proof : Let D be a UFD and

$f(x) = a_0+a_1x+a_2x^2+ - - - +a_nx^n$

$g(x) = b_0+b_1x+b_2x^2+ - - - +b_nx^n$

be two primitive polynomials over D. Then

$f(x)\, g(x) = c_0+c_1x+c_2x^2+ - - - + c_{m+n}x^{m+n}$

Where $c_k = \sum_{i+j=k} a_i b_j$ for $0 \le k \le m+n$.

We have to prive HCF$(c_0, c_1, c_2, - - -, c_{m+n}) = 1$. If possible, let HCF $(c_0, c_1, c_2, - - -, c_{m+n}) = d$ be a non-unit. Then there exists an irreducible element p such that $p|d$. Clearly $p|c_k$ for all k. Since HCF $(a_0, a_1\, a_2, - - - a_n) = 1$ as f is primitive, so p cannot divides all a_i's.

Let t be the smallest suffix such that $p \nmid a_t$.

Similarly u be the smallest suffix such that $p \nmid b$.

Consider $C_{t+u} = (a_0b_{t+u}+a_1b_{t+u-1}+ - - - + a_{t-1}b_{u+1}) + q_tb_u +$

$(a_{t+1}b_{u-1}+a_{t+2}b_{u-2}+ - - - + a_{t+u}b_0)$

By our choice $p|a_0$, $p|a_1$, - - - $p|a_{t-1}$. This yields $p|a_0b_{t+u}+a_1b_{t+u-1}$+ - - - + $a_{t-1}b_{u+1}$. Similarly $p|a_{t+1}b_{u-1}+a_{t+2}b_{u-2}$+ - - - + $a_{t+u}b_0$.

Also $p|c_{t+u}$ $\Rightarrow p|a_tb_u$

$\Rightarrow p|a_t$ or $p|b_u$ as p is prime.

This is a contradiction. Hence HCF (c_0, c_1, c_2, - - -, c_{m+n}) = 1, i.e.

f(x) g(x) is primitive.

Theorem 12.8.5. If D is a UFD, then D[x] is also UFD.

Proof : Let D be a UFD. Then D is an integral domain with unity. Which implies D[x] is an integral domain with unity.

First we have to show every nonzero non-unit in D[x] can be expressed as a finite product of irreducible elements of D[x].

Let $f(x) \in D[x]$ be a nonzero non-unit.

Case (I): If $f(x) \in D$, then f(x) can be expressed as product of irreducible elements of D. Since every irreducible element of D is an irreducible element or D[x], f(x) can be expressed as product of irreducible element of D[x].

Case (II): Let $f(x) \notin D$ and f(x) be a primitive polynomial in D[x]. We have prove by induction on degree of f(x).

If deg f(x) = 1, then f(x) is an irreducible polynomial.

$\Rightarrow$ f(x) is an irreducible primitive polynomial in D[x].

$\Rightarrow$ f(x) is an irreducible element in D[x].

The result holds for f(x) if deg f(x) = 1.

Let deg f(x) = n > 1 and let our assertion holds for all primitive polynomials of degree < n.

If f(x) itself is irreducible polynomial, then there is nothing to prive. Let f(x) be a reducible pilynomial in D[x]. Then there exists g(x), $h(x) \in D[x]$ such that f(x) = g(x).h(x), where deg g(x) < n, deg h(x) < n.

Since f(x) is primitive, therefore g(x) and h(x) are both primitive polynomials. Also, we have deg g(x) < n and deg h(x) < n, so by induction hypothesis, g(x) and h(x) both can be expressed as products of irreducible elements in D[x]. Thus f(x) can be expressed as a product of irreducible element in D[x].

Case (III) : Let $f(x) \notin D$ and f(x) be a primitive polynomial. Then f(x) can be expressed as

$f(x) = d.\ g(x)$

Where $d \in D$ is nonzero non-unit and g(x) is a primitive polynomial in D[x].

D being a UFD, d can be expressed as product of irreducible element in D[x].

Also g(x) is a primitive polynomial, so by case (II) g(x) can be expressed as product of irreducible polynomial in D[x]. Hence f(x) can be expressed as product of irreducible polynomial in D[x].

Let $f(x) \in D[x]$ be a nonzero non-unit and $f(x) = g_1(x)\ g_2(x) \ldots g_k(x)$ where $g_i(x) \in D[x]$ for all i = 1, 2, . . ., k and each $g_i(x)$ is an irreducible elements in D[x].

Also $f(x) = h_1(x)\ h_2(x) \ldots h_m(x)$ be another representation of f(x) as a product of irreducible elements in D[x]. We have show k = m and each g_i is associate of some h_j and vice versa for i = 1, 2, 3, . . ., k; j = 1, 2, 3, . . ., m.

We apply induction on k. If k = m, the result is obvious. We assume the result holds for all those non zero non-units in D[x] which are expressible as product of less than k irreducible elements in D[x].

Now $g_1(x)\ g_2(x) \ldots g_k(x) = h_1(x)\ h_2(x) \ldots h_m(x)$

$\Rightarrow g_1(x) | h_1(x)\ h_2(x) \ldots h_m(x)$

$\Rightarrow g_1(x) | h_j(x)$ for some j [$\because$ each irreducible element in D[x] is a prime element in D[x]]

$\Rightarrow h_j(x) = g_1(x).r(x)$ where $r(x) \in D[x]$.

Since $h_j(x)$ is irreducible, so r(x) must be unit in D[x].

Since r(x) is a unit in D[x], so $r(x) \in D$, i.e.

$r(x) = u$ for some $u \in D$.

Thus $h_j(x) = g_1(x).u$. By renumbering the h_j's, we can assume j = 1 and then $h_1(x) = g_1(x).u$ and

$g_1(x)\ g_2(x) \ldots g_k(x) = g_1(x).u\ h_2(x) \ldots h_m(x)$

$\Rightarrow g_2(x)\ g_3(x) \ldots g_k(x) = u\ gh_2(x)\ h_3(x) \ldots h_m(x)$

$\Rightarrow g_2(x)\ g_3(x) \ldots g_k(x) = h'_2(x)\ h_3(x) \ldots h_m(x)$ where $h'_2(x) = u\ h_2(x)$

If we put $p(x) = g_2(x)\ g_3(x) \ldots g_k(x)$

and $p(x) = h'_2(x)\, h_3(x) \ldots g_m(x)$, then by induction hypothesis, k–1= m–1 $\Rightarrow$ k = m and each $g_i(x)$ is an associate of some $h_j(x)$ and vice verse for all i = 2, 3, . . ., k and j = 2, 3, . . ., m.

Also $h_1(x) = g_1(x).u$

$\Rightarrow h_1(x)$ and $g_1(x)$ are associates.

Hence k = m and each $g_i(x)$ is an associate of some hj(x) and vice versa for all i = 1, 2, . . . k and for all j = 1, 2, . . ., m. Thus D[x] is a UFD.



CHECK YOUR PROGRESS

Q 9: Prove that any two nonzero elements in a UFD have a gcd.

Q 10: Prove that any two nonzero in a UFD have an LCM.

Q 11: For any two nonzero polynomials f and g over a UFD, C(fg) = C(f).C(g), where C(f) = content of f.

Q 12: Show that Z[x] is UFD but not PID.

Q 13: Show that $Z_5[x]$ is a UFD. Is x^2+2x+3 reducible over $Z_5[x]$?

12.9 EUCLIDEAN DOMAINS : DEFINITIONS AND EXAMPLES

Definition: (Euclidean Domain) An integral domain D is called a Euclidean domain (ED) if there exists a function

$\delta : D - \{0\} \to Z$

such that (i) $\delta(a) \geq 0$ for all $a \in D - \{0\}$,

(ii) $\delta(ab) \geq \delta(a)$ for all $a, b \in D - \{0\}$,

and (iii) for $a \in D$, $b \in D - \{0\}$ there exist $q, r \in D$

such that a = bq + r where r = 0 or $\delta(r) < \delta(b)$.

Example 1. We have Z is an integral domain. We define $\delta : Z - \{0\} \to Z$ by $\delta(a) = |a|$.

(i) $|a| \geq 0$ for all $a \in Z - \{0\}$

$\Rightarrow \delta(a) \geq 0$ for all $a \in Z - \{0\}$

(ii) For $a, b \in Z - \{0\}$, $\delta(ab) = |ab| \geq |a|$

$\Rightarrow \delta(ab) \geq \delta(a)$.

(iii) If $a \in Z$ and $b \in Z - \{0\}$, there exist unique $q, r \in Z$ such that $a = bq+r$ where $0 \leq r < |b|$

$\Rightarrow a = bq + r$ where $r = 0$ or $0 < r < |b|$

where $r = 0$ or $|r| < |b|$

where $r = 0$ or $\delta(r) < \delta(b)$

Hence Z is a Euclidean domain.

Example 2. Let F be a field. Then F is an integral domain. We define a map $\delta : F - \{0\} \to Z$ by

$\delta(a) = 1$

Then (i) $\delta(a) = 1 > 0$ for all $a \in F - \{0\}$

(ii) For $a, b \in F - \{0\}$, $\delta(ab) = 1 = \delta(a)$.

(iii) Let $a \in F$, $b \in F - \{0\}$. Then

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

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

$= b(ab^{-1})$

$= bq + r$ where $q = ab^{-1} \in F$, $r = 0$

Hence F is a Euclidean domain. i.e. any field is a Euclidean domain.

Example 3. Let F be a field. Then F is an integral domain.

$\Rightarrow F[x]$ is an integral domain.

We define $\delta : F[x] - \{0\} \to Z$ by

$\delta(f(x)) = \deg f(x)$.

(i) $\deg f(x) \geq 0$ for all $f(x) \in F[x]$

$\Rightarrow S(f(x)) \geq 0$ for all $f(x) \in F[x]$.

(ii) For $f(x), g(x) \in F[x] - \{0\}$,

$\delta[f(x).g(x)] = \deg (f(x).g(x))$

$= \deg f(x) + \deg g(x)$ [$\because$ F[x] is an integral domain]

$\geq \deg f(x)$

$\therefore \delta(f(x).g(x)) \geq \delta(f(x))$

(iii) For any $f(x) \in F[x]$, $g(x) \in F[x] - \{0\}$, by division algorithm, there exist $q(x), r(x) \in F[x]$ such that

$f(x) = g(x)\, q(x) + r(x)$ where $r(x) = 0$ or $\deg r(x) < \deg g(x)$

i.e. $f(x) = g(x)\, q(x) + r(x)$ where $r(x) = 0$ or $\delta(r(x)) < \delta(g(x))$.

Hence F[x] is a Euclidean domain.

12.10 PROPERTIES OF ED

Theorem 12.10.1. Every ED is a PID.

Proof: Let D be a ED. Then D is an integral domain. Let δ be the Euclidean valuation on D and let A be a nonzero ideal of D. Then there exists a $(\neq 0) \in$ A. Consider the set M=$\{\delta(x)|x(\neq 0) \in A\}$. Clearly M$\in \phi$ as δ (a)$\in$M.

$\Rightarrow$ M is a nonempty set of non-negative integers.

By well ordering principle. M has a least element.

Let δ (b) be the least element of M, where b$(\neq 0) \in$A.

Claim : A = $\langle b \rangle$.

Let y$\in \langle b \rangle$. Then y = rb for some r$\in$D

$\Rightarrow$y$\in$A [$\because$ b$\in$A and A is an ideal of D]

$\therefore \langle b \rangle \subseteq$A (I)

Next, let z$\in$A. Then by the Euclidean algorithm. there exist q, r$\in$D such that

z = bq + r where r = 0 or $\delta(r) < \delta(b)$

Let r$\neq$ 0. Then δ (r)(b). Also r = z – bq()A

$\therefore$ r$(\neq 0) \in$A, δ (r)$\in$M and $\delta(r) < \delta(b)$. Which contradicts to the fact that δ (b) is the least element in M. Thus r = 0 and hence

Z = bq $\in \langle b \rangle$

A $\subseteq \langle b \rangle$ (II)

From (I) and (II), A = $\langle b \rangle$.

Since D itself is a ideal, $\exists$ d$(\neq 0)$ D such that

D = $\langle b \rangle$

This implies that there exists e$\in$D such that d = ed. Now we want to show e is the unity in D. Let s$\in$D.

Then s = td for some t$\in$D. Now

se = (td)e = t(de) = t(ed) = td = s

$\Rightarrow$ se = es = s

$\Rightarrow$e is the unity in D.

Therefore D is an integral domain with unity and every ideal of D is principal. Hence D is a PID.

Corollary 12.10.2. Every ED is a UFD.

Proof: Since every ED is PID and every PID is UFD, therefore every ED is a UFD.

Remark : ED $\Rightarrow$ PID $\Rightarrow$ UFD

UFD $\not\Rightarrow$ PID $\not\Rightarrow$ ED



CHECK YOUR PROGRESS

Q 14: Let D be an ED. Then show that $a(\neq 0) \in D$ is a unit if and only if $\delta(a) = \delta(1)$.

Q 15: Show that Z[i] is a ED.

Q 16: Let D be a ED. Then

(i) If a and b are associates, then show that $\delta(a) = \delta(b)$; $a, b \in D$.

(ii) a|b and $\delta(a) = \delta(b) \Rightarrow$ a and b are associates.

(iii) $\delta(ab) > \delta(b) \Leftrightarrow$ a is not a unit, $a, b \in D$.

(iv) Give an example of two elements a and b such that $\delta(a) = \delta(b)$ but a and b are not associates.

Q 17: Show that $Z\left[\sqrt{2}\right]$ is a ED.

12.11 FIELD EXTENSIONS : DEFINITIONS AND EXAMPLES

Definition: (Extension of a field). Let K and F be any two fields and $\sigma : F \to K$ be a monomorphism. Then $F \cong \sigma(F) \subseteq K$. and (K, σ) is called an extension of field F. Since $F \cong \delta(F)$ and $\sigma(F)$ is a subfield of K, so we may regard F as a subfield of K. So, if K and F are two fields such that F is a subfield of K, then K is called an extension of F and we denote it by K\F or K|F or I^k_F.

Example 1. Every field is an extension of itself.

Example 2. Every field is an extension of its every subfield, for example, R is a field extension of Q and C is a field extension of R.

Remark : Let K|F be any extension. Then F is a subfield of K. We define a mapping $\phi : FXK \to K$ by

$\phi(\lambda k) = k$ for all $\lambda \in F, k \in K$.

We observe that K becomes a vector space over F under this scalar multiplication. Thus, K must have a basis and dimension over F.

Definition: (Degree of an extension) The dimension K as a vector space over F is called degree of K|F, i.e. degree of K|F = [K : F].

If [K : F] = n < ∞, then we say K is a finite extension of F of degree n and if [K : F] = ∞, then we say that K is an infinite extension of F.

Example 1. [F : F] = 1, [K : F] > 1 if K $\neq$ F.

Example 2. [C : R] = 2, because basis of vector space C over the field R is {1, i}.

Definition: (Transcendental Number) : A number (real or complex) is said to be transcendental if it does not satisfy any polynomial over Q.

Example. π, e are transcendental numbers.

Remark. Every transcendental number is an irrational number but converse is not true. For example, $\sqrt{2}$ is an irrational number but it is not transcentental because it satisfies the polynomial x^2-2.

Definition: (Algebraic Number). Let R|F be any extension. If $\alpha \in$ K and α satisfies a polynomial over F, i.e. f(α) = 0, where f(x) = $\lambda_0 + \lambda_1 x + \lambda_2 x^2 + \ldots + \lambda_n x^n$; $\lambda_i \in$ F for all i = 0, 1, 2, . . ., n. Then α is called algebraic over F.

If α does not satisfy any polynomial over F, then α is called transcendental over F. For example, π is transcendental over Q but π is not transcendental over R.

Note : Every element of F is always algebraic over F.

Definition: (Algebraic Extension) The extension K|F is called algebraic extension if every element of K is algebraic over F. Otherwise, K|F is said to be transcendental extension if at least one element is not algebraic over F.

Definition: (Minimal Polynomial) If p(x) is a polynomial over F of smallest degree satisfied by α, then p(x) is called minimal polynomial of α. Without loss of generallity, we can assume that leading coefficient in p(x) is 1, i.e., p(x) is a monic polynomial.

Definition: (Subfield generated by a subset of a field) Let S be a subset of a field K, then the subfield K$'$ of K is said to be generated by

S if (i) $S \subseteq K'$ and

(ii) for any subfield L of K, $S \subseteq L$ implies $K' \subseteq L$.

We denote the subfield generated by S by $\langle S \rangle$. Essentially the subfield generated by S is the intersection of all subfields of K which contains S.

Definition: (Subfield generated by a subset S of K over F) Let K be a field extension of F and S be any subset of K, then the subfield of K generated by FUS is said to be the subfield of K generated by S over F and this subfield is denoted by F(S). However, if S is a finite set and its members are $a_1, a_2, \ldots, a_n$, then we write $F(S) = F(a_1, a_2, \ldots, a_n)$. Sometimes $F(a_1, a_2, \ldots, a_n)$ is also called adjunction of $a_1, a_2, \ldots, a_n$ over F.

Definition: A field K is said to be finitely generated over F if there exists a finite number of elements $a_1, a_2, \ldots, a_n$ in K such that

$K = F(a_1, a_2, \ldots, a_n)$.

In particular, if K is generated by a single element 'a' over F, i.e. K = F(a), then K is called a simple extension of F.

Definition: Let K|F be any field extension and let F[x] be the pilynomial ring over F. We define $F[a] = \{f(a) : f(x) \in F[x]\}$

Remarks : (I) Let $f(a) \in F[a]$ where $f(x) = \lambda_0 + \lambda_1 x + \lambda_2 + \ldots + \lambda_n x^n \in F[x]$. Clearly $f(a) = \lambda_0 + \lambda_1 a + \lambda_2 a^2 + \ldots + \lambda_n a^n \in F[a]$.

Thus $F[a] \subseteq F(a)$.

(II) $a_1 \in F \Leftrightarrow F(a_1) = F$.

12.12 PROPERTES OF FIELD EXTENSIONS

Theorem 12.12.1. Every finite extension is an algebraic extension.

Proof : Let K|F be an extension and let [K: F] = n, i.e. dim K|F = n. Every element of F is obviously algebraic. Let $\alpha \in K$ be any arbitrary element consider the elements 1, $\alpha, \alpha^2, \ldots, \alpha^n$ in K. If all these elements are not distinct, then

$\alpha^i = \alpha^j$ for some $i \neq j$

$\Rightarrow \alpha^i - \alpha^j = 0$

Consider the polynomial $f(x) = x^i - x^j \in F[x]$

and $f(\alpha) = \alpha^i - \alpha^j = 0$

Thus, α satisfies f(x)$\in$F[x] and hence α is algebraic over F.

If 1, α, α^2 . . ., α^n are all distinct, then these must be linearly dependent over F as dim K|F = n. So there exists $\lambda_0, \lambda_1, \lambda_2, \ldots, \lambda_n \in F$ (not all zero) such that

$\lambda_0 + \lambda_1\alpha + \lambda_2\alpha^2 + \ldots + \lambda_n\alpha^n = 0$

Thus α satisfies the polynomial

$f(x) = \lambda_0 + \lambda_1 x + \lambda_2 x^2 + \ldots + \lambda_n x^n$

Which implies α is algebraic over F. Hence every finite extension is an algebraic extension.

Remark : Converse of above theorem is not true, i.e. every algebraic extension is not a finite extension. For example, $Q\left(\sqrt{2}, \sqrt{3}, \sqrt{4}, \ldots, \sqrt{n}, \ldots\right)$ is a algebraic extension of Q but it is not finite.

Lemma 12.12.2. If p(x)$\in$F[x] be a minimal polynomial of α and f(x)$\in$F[x] be any other polynomial such that f(α) = 0, then p(x)|f(x).

Proof : Since F is a field so F[x] must be a unique factorization domain (UFD) and so division algorithm hold in F[x]. Therefore, there exists polynomials q(x) and r(x) such that

f(x) = p(x) q(x) + r(x) where r(x) = 0 or deg r(x) < deg p(x)

Now f(α) = 0 $\Rightarrow$ p(α) q(α) + r(α) = 0

$\Rightarrow$ r(α) = 0 [$\because$ p(α) = 0]

If r(x)$\in$F[x] is a non-zero polynomial, then it is a contradiction to minimality of p(x), since deg r(x) < deg p(x). So, we must have r(x) = 0. Thus

f(x) = p(x) q(x)

$\Rightarrow$ p(x) | f(x)

Theorem 12.12.3. Minimal polynomial of an element is unique.

Proof : Let p(x) and q(x) be two minimal polynomials of α. Since p(x) is a minimal polynomial of α, so

p(x) | q(x)

and deg p(x)$\leq$deg q(x) (I)

Also q(x) is a minimal polynomial of α, so

q(x) | p(x)

and deg q(x) $\leq$ deg p(x) (II)

From (I) and (II), deg p(x) = deg q(x).

Let p(x) = λ q(x) for some $\lambda \in F$.

Since p(x) and q(x) are both monic polynomials, so comparing the coefficients of leading terms on both sides, we get λ = 1. Therefore p(x) = q(x).

Theorem 12.12.4. Minimal polynomial of any element is irreducible over F.

Proof : If possible, let minimal polynomial p(x) of $\alpha \in F$ is reducible over F. Then we have

p(x) = q(x) t(x) for some q(x), t(x) $\in$ F[x].

Then p(α) = 0 implies q(α) t(α) = 0

$\Rightarrow q(\alpha) = 0$ or $t(\alpha) = 0$

Which is not possible because deg q(x) < deg p(x) and deg t(α) < deg p(x). Thus p(x) is a irreducible plynomial over F.

Theorem 12.12.5. Let K|F be any field extension. Then a $\in$ K is algebraic over F if and only if [F(a) : F] is finite, i.e., F(a) is a finite extension over F. Moreover [F(a) : F] = n, where n is the degree of minimal polynomial of a over F.

Proof : Let [F(a) : F] = n. Then $\dim_F F(a) = n$.

Now, consider the elements 1, a, a^2, . . . , a^n of F(a).

Since $\dim_F F(a) = n$, so these n+1 elements in F(a) are linearly dependent. Thus there exists $\lambda_0, \lambda_1, \lambda_2 ..., \lambda_n \in F$ (not all zero)

Such that, $\lambda_0 + \lambda_1 a + \lambda_2 a^2 + \ldots + \lambda_n a^n = 0$

Thus a satisties the polynomial f(x) = $\lambda_0 + \lambda_1 x + \lambda_2 x^2 + \ldots + \lambda_n x^n$. So a is algebraic over F.

Conversely, let a $\in$ K be algebraic over F and p(x) $\in$ F[x] be a minimal polynomial of a over F such that deg p(x) = n $\geq$ 1. We have to prove [F(a) : F] = n.

Let p(x) = $\lambda_0 + \lambda_1 x + \lambda_2 x^2 + \ldots + \lambda_n x^n$, $\lambda_n \neq 0$.

Since p(x) is minimal polynomial of a, so p(a) = 0.

If g(x) $\in$ F[x] is any plynomial such that g(a) = 0, then p(x)|g(x).

Consider t $\in$ F[a]. Then t = f(a) for some f(x) $\in$ F[x]

If t $\neq$ 0, then f(a) $\neq$ 0, i.e. f(x) does not satisfy by a. So, p(x) $\nmid$ f(x).

As F[x] is an Euclidean domain, so we get gcd [p(x), f(x)] = 1. Therefore there exists polynomials h(x), k(x) $\in$ F[x] such that

f(x) h(x) + p(x) k(x) = 1

Put x = a, f($\because$ a) h(a) +p(a) k(a) = 1

$\Rightarrow$ f(a) h(a) = 1 [p(a) = 1]

$\Rightarrow$ f(a) is invertible.

We know that an integral domain in which every nonzero element is invertible is a field. Hence F[a] is a field.

Since F[a] $\subseteq$ F(a) and F(a) is the field of quotients of F[a], therefore F[a] = F(a).

Now applying division algorithm to p(x), f(x) $\in$ F[x], we can write

f(x) = p(x) q(x) +r(x) where r(x) = 0 or deg r(x) < deg p(x).

Let r(x) = $\lambda_0 + \lambda_1 x + \lambda_2 x^2 + \ldots + \lambda_{n-1} x^{n-1} \in F[x]$.

Then t = f(a) = p(a) q(a) + r(a)

= r(a) [$\because$ p(a) = 0]

= $\lambda_0 + \lambda_1 a + \lambda_2 a^2 + \ldots + \lambda_{n-1} a^{n-1}$

Thus t is a linear combination of 1, a, a^2, . . ., a^{n-1} over F, i.e. the set {1, a, a^2, . . ., a^{n-1}} generates F(a). If possible, let the set {1, a, a^2, . . . a^{n-1}} is linearly dependent. Then there exists scalars $v_0, v_1, \ldots, v_{n-1} \in F$ (not all zero) such that

$v_0 + v_1 a + v_2 a^2 + \ldots + v_{n-1} a^{n-1} = 0$

i.e. a satisfies a polynomial of n–1 degree, which is a contradiction to minimality of p(x). Hence {1, a, a^2, . . ., a^{n-1}} is linearly independent and so it is a basis for F(a) over F. Therefore [F(a) : F] = n < ∞.

Theorem 12.12.6. Let K|F be a finite extension of degree n and L|K be a finite extension of degree m, then L|F is a finite extension of degree mn, i.e.,

[L : F] = [L : K] [K : F]

Proof : Given that L|K be a finite extension such that [L : K] = m, i.e. $\dim_K L = m$. Let $\{x_1, x_2, \ldots, x_m\}$ be a basis of L over K.

Also, given that K|F is finite extension such that [K : F] = n, i.e., $\dim_F K = n$. Let $\{y_1, y_2, \ldots, y_n\}$ be a basis of K over F.

Let $\alpha \in$ L. Then

$\alpha = \alpha_1 x_1 + \alpha_2 x_2 + \ldots + \alpha_m x_m$

$= \sum_{i=1}^{m} \alpha_i x_i$, $\alpha_i \in K$

Now, $\alpha_i \in K$ and $\{y_1, y_2, \ldots, y_n\}$ be a basis of K over F, so

$\alpha_i = \alpha_{i1} y_1 + \alpha_{i2} y_2 + \ldots + \alpha_{in} y_n = \sum_{j=1}^{n} \alpha_{ij} y_j$, $\alpha_{ij} \in F$

Thus $\alpha = \sum_{i=1}^{m} \left(\sum_{j=1}^{n} \alpha_{ij} y_j \right) x_i$

$= \sum_{i,j} \alpha_{i1} x_i y_j$ where $\alpha_{i1} \in F$ and $x_i, y_j \in L$

Therefore $\{x_1 y_1, x_1 y_2, \ldots, x_1 y_n, x_2 y_1, x_2 y_2, \ldots, x_2 y_n, \ldots, x_m y_1, x_m y_2, \ldots, x_m y_n\}$ spans L over F and have mn elements in number.

If $\alpha = 0$, then

$$0 = \sum_{i,j} \alpha_{ij} x_i y_j = \sum_{i=1}^{m} \left(\sum_{j=1}^{n} \alpha_{ij} y_j \right) x_i$$

$$= \sum_{i=1}^{m} \alpha_i x_i$$

Since $\alpha_i \in K$ and $\{x_1, x_2, \ldots, x_m\}$ are L.I. over K. Thus

$\alpha_i = 0$ for all i = 1, 2, . . ., n.

Again since $\{y_1, y_2, \ldots y_n\}$ are L.I. over F. Thus $\alpha_{ij} = 0$ for all j=1,2,...,n.

Thus $\alpha_{ij} = 0$ for all i = 1, 2, 3, . . ., m; j = 1, 2, . . .,n.

So $\{x_1, y_1, x_1 y_2, \ldots, x_1 y_n, x_2 y_1, x_2 y_2, \ldots, x_2 y_n, \ldots, x_m y_1, x_m y_2, \ldots, x_m y_n\}$ is L.I, and hence it is basis for L over F. Therefore.

[L : F] = mn = [L : K] [K : F].

Theorem 12.12.7. If $F \subseteq E \subseteq K$ and $a \in K$ is algebraic over F, then $[E(a) : E] \leq [F(a) : F]$.

Proof : Let $F \subseteq E \subseteq K$ and $a \in K$ is algebraic over F. Then there exists a polynomial

$f(x) = \lambda_0 + \lambda_1 x + \lambda_2 x^2 + \ldots + \lambda_n x^n \in F[x]$ such that f(a) = 0

Since $f(x) \in F[x]$ and $F \subseteq E$, therefore

$F[x] \subseteq E[x]$

$\Rightarrow f(x) \in E[x]$ such that f(a) = 0

So, if p(x) is the minimal polynomial of a over F and $p_1(x)$ is the minimal polynomial of a over E, then as $p(x) \in E[x]$, we get $p_1(x) | p(x)$ in E[x].

This gives deg $p_1(x) \leq$ deg p(x). However we know that [F(a) : F] = deg p(x) and [E(a) : E] = deg $p_1(x)$.

Hence $[E(a) : E] \leq [F(a) : F]$

Remark : Let K|F be any field extension. Then

$F(a_1, a_2, \ldots, a_n) = F(a_1, a_2, \ldots, a_{n-1})(a_n)$

$= F(a_1, a_2, \ldots, a_{n-2})(a_{n-1}, a_n)$

$= F(a_1, a_2, \ldots, a_{n-3})(a_{n-2}, a_{n-1}, a_n)$

$= F(a_1)(a_2, a_3, \ldots, a_{n-1}, a_n)$

Theorem 12.12.8. Let K|F be an algebraic extension and L|K be also algebraic extension. Then L|F is also an algebraic extension.

or

Algebraic extension of an algebraic extension is also an algebraic extension.

Proof : Let K|F and L|K be two algebraic extensions. We have to prove L|F is also an algebraic extension.

To prove L|F is an algebraic extension, it is sufficient to show that every element of L is algebraic over F. Equivalently, we have to prove that if $a \in L$, then $[F(a) : F] < \infty$.

Since L|K is an algebraic extension, so for $a \in L$, a satisfies some polynomial f(x) over K, say

$f(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \ldots + \alpha_n x^n \in K[x]$

Since $\alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_n \in K$ and K|F is an algebraic extension, therefore α_i's are algebraic over F. Consider the element α_0. Since α_0 is algebraic over F, so

$[F(\alpha_0) : F] < \infty \Rightarrow [F_0 : F] < \infty$, where $F_0 = F(\alpha_0)$ and we have $F \subseteq F_0 \subseteq K$.

Now $\alpha_1 \in K$ is algebraic over F, so by theorem 12.12.7,

We have $[F_0(\alpha_1) : F_0] \leq [F(\alpha_1) : F] < \infty$.

Put $F_0(\alpha_1) = F_1$, $[F_1 : F_0] < \infty$ and

$F \subseteq F_0 \subseteq F_1 \subseteq K$.

Also considering $F_1(\alpha_2) = F_2$ and as above, we get

$[F_2 : F_1] < \infty$

Continue the process, lastly, we get

$F_{n-1}(\alpha_n) = F_n$ and $[F_n : F_{n-1}] < \infty$

By construction, we get

$F_n = F_{n-1}(\alpha_n)$

$= F_{n-2}(\alpha_{n-1}, \alpha_n)$

$= F_0(\alpha_1, \alpha_2, \ldots, \alpha_n)$

$= F(\alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_n)$

and by theorem 12.12.6, we have

$[F_n : F] = [F_n : F_{n-1}] [F_{n-1}, F_{n-2}] \ldots [F_1 : F_0] [F_0 : F]$

Thus $[F_n : F]$ is finite since all the numbers on RHS are finite.

Now, as $\alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_n \in F_n$, $f(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \ldots + \alpha_n x^n \in F_n$ [x].

Since f(a) = 0, so a is algebraic over F_n. Thus

$[F_n(a) : F_n]$ = degree of minimal polynomial of a over $F_n < \infty$

and $[F_n(a) : F] = [F_n(a) : F_n] [F_n : F] < \infty$

Thus $F_n(a)|F$ is a finite extension.

$\Rightarrow F_n(a)$ is algebraic extension over F.

$\Rightarrow$ a is algebraic over F.

Hence L is algebraic extension of F.

Theorem 12.12.9. Let K|F be any extension and $S = \{x \in K : x$ is algebraic over F$\}$. Then, S is a subfield of K containing F and S is the largest algebraic extension of F contained in K.

Proof : Let $\alpha \in F \subseteq K$. Since α satisfies a polynomial $f(x) = x - \alpha$ in F[x]. So, α is algebraic over F. Thus $\alpha \in S$ and so $F \subseteq S$. So, S is nonempty.

Let $a, b \in S$. We claim that $a - b \in S$ and if $b \neq 0$, then $ab^{-1} \in S$. Since K is a field, therefore, trivially $a - b \in K$ and if $b \neq 0$, then $ab^{-1} \in K$. To prove $a - b \in S$ and if $b \neq 0$, then $ab^{-1} \in S$ it is sufficient to show that a–b and ab^{-1} are algebraic over F.

Since $a \in S$, i.e., a is algebraic over F, so

$[F(a) : F] < \infty$

Put $F(a) = F_1$. Then $[F_1 : F] < \infty$

Also $b \in S$, i.e. b is algebraic over F, so

$[F(b) : F] < \infty$

Since b is algebraic over F and $F \subseteq F_1 \subseteq K$, so be is algebraic over F_1 and

$[F_1(b) : F_1] < [F(b) : F] < \infty$

Thus $[F_1(b) : F] = [F_1(b) : F_1]\,[F_1 : F] < \infty$, i.e. $F_1(b)$ is finite extension of F, i.e. F(a, b) is an algebraic extension of F as $F_1(b) = F(a, b)$.

Hence every element of F(a, b) is algebraic over F. Since $a, b \in F(a, b) \Rightarrow a-b \in F(a, b)$ and $ab^{-1} \in F(a, b)$, therefore a–b and ab^{-1} are algebraic over F.

$\Rightarrow a-b, ab^{-1} \in S$

$\Rightarrow$ S is a subfield of K containing F.

Thus S is an algebraic extension of F.

Let E be any other algebraic extension such that $F \subseteq E \subseteq K$. Let $\alpha \in E \subseteq K$. Therefore, α is algebraic over F. Thus $\alpha \in S$ and hence $E \subseteq S$.

Hence S is the largest algebraic extension of F contained in K.

Corollary 12.12.10. If K|F is algebraic extension. Then K = S.

Proof : In the above theorem, S is a subfield of K. Therefore $S \subseteq K$.

Since S is the largest algebraic extension of F and K is an algebraic extension of F, therefore $K \subseteq S$.

Hence S = K

Corollary 12.12.11. If K|F be any extension and $a, b \in K$ be algebraic over F. Then a+b, a–b, ab and ab^{-1} $(b \neq 0)$ are also algebraic.

Proof : If a, b are algebraic over F, then F(a, b) is algebraic extension of F. Since a+b, a–b, ab and $ab^{-1} \in F(a, b)$ and every element of F(a, b) is algebraic over F, so a+b, a–b, ab and ab^{-1} $(b \neq 0)$ are algebraic over F.

Theorem 12.12.12 (Factor theorem) Let K|F be any extension and $f(x) \in F[x]$. Then the element $a \in K$ is a root of polynomial f(x) iff x–a|f(x) in K[x], i.e. iff there exists some g(x) in K[x] such that f(x) = (x–a) g(x).

Proof : Let (x–a)|f(x) in K[x]. Then, we have f(x) = (x–a) g(x) for some g(x) in K[x]. Therefore f(a) = (a–a) g(a) = 0

Thus a is a root of f(x).

Conversely, let a be a root of f(x) where $a \in K$. Consider the polynomial x–a in K[x].

We have $f(x) \in F[x] \subseteq K[x]$. Therefore by division algorithm in K[x], there exists unique polynomial q(x) and r(x) in K[x] such that

f(x) = (x–a) q(x) +r(x)

Where r(x) = 0 or deg r(x) < deg (x–a) = 1

i.e. r(x) = 0 or r(x) = constant

But f(a) = 0 $\Rightarrow$ r(a) = 0

Thus r(x) = 0

Hence f(x) = (x–a) q(x)

$\Rightarrow$ x–a|f(x) in K[x]

Theorem 12.12.13. Let K|F be any extension and a $\in$ K is algebraic over F. Let p(x) $\in$ F[x] be the minimal polynomial of a. Then

$$F[x]/\langle p(x)\rangle \cong F[a] = F(a)$$

Proof : Consider the ring F[x] and F[a].

We define the mapping η : F[x] $\rightarrow$ F[a] by η(f(x)) = f(a).

We claim that η in an onto ring homomorphism

Let f(x), g(x) $\in$ F[x]. Then

η(f(x) + g(x)) = f(a) + g(a) = η(f(x))+ η(g(x))

and η(f(x) g(x)) = f(a) g(a) = η(f(x)) η(g(x))

Thus η is ring homomorphism.

Let $\alpha \in$ F[a]. Then α = h(a) for some h(x) $\in$ F[x]. Now η[h(x)] = h(a) = α.

Thus η is onto.

By fundamental theorem of ring homomorphism.

$$F[x]/\text{Ker}\,\eta \cong F[a]$$

Now we claim that ker η = $\langle$ p(x) $\rangle$ where p(x is minimal polynomial of a over F.

Let f(x) $\in$ Ker η $\Rightarrow$ η(f(x)) = 0

$\Rightarrow$ f(a) = 0

$\Rightarrow$ a satisfies f(x)

$\Rightarrow$ p(x)|f(x), since p(x) is minimal polynomial.

$\Rightarrow$ f(x) = p(x) q(x) for some q(x) $\in$ F[x].

$\Rightarrow$ f(x) $\in$ $\langle$ p(x) $\rangle$

$\therefore$ Ker η $\subseteq$ $\langle$ p(x) $\rangle$ (I)

Again, let f(x) $\in$ $\langle$ p(x) $\rangle$

$\Rightarrow$ f(x) = p(x) q(x) for some q(x) $\in$ F[x].

$\Rightarrow$ f(a) = p(a) q(a)

$\Rightarrow f(a) = 0 \qquad [\because p(a) = 0]$

$\Rightarrow \eta(f(x)) = 0$

$\Rightarrow f(x) \in \ker \eta$

$\therefore \langle p(x) \subseteq \ker \eta \qquad$ (II)

From (I) and (II), we get $\ker \eta = \langle p(x) \rangle$ and so

$$F[x]/\langle p(x) \rangle \cong F[a]$$

Since a is algebraic over F, therefore F[a] = F(a) and hence

$$F[x]/\langle p(x) \rangle \cong F(a)$$

Definition: (Conjugates) Let K|F be any extension. Two algebraic elements a, $b \in K$ are said to be conjugates over the field F if they have same minimal polynomials, i.e., we can say that all the roots of minimal polynomial polynomial are conjugate of each other.

Corollary 12.12.14. If a and b are two conjugate elements of K over F, where K|F is an extension. Then $F[a] \cong F[b]$.

Proof : Let p(x) be the minimal polynomial of a and b both. Then by theorem 12.12.12

$$F[x]/\langle p(x) \rangle \cong F[a] \text{ and } F[x]/\langle p(x) \rangle \cong F[b]$$

$\Rightarrow F[a] \cong F[b]$

Definition: Let K|F be any extension and $f(x) \in F[x]$ be a nonzero polynomial. Then a is said to be a root of f(x) of multiplicity $m \geq 1$ if $(x-a)^m | f(x)$ but $(x-1)^{m+1} \nmid f(x)$.

Theorem 12.12.16. Let $p(x) \in F[x]$ be an irreducible polynomial o0ver F. Then there exists an estension E of F which contains at least one root of p(x) and [E:F]=n=dge g(x). Let I = <p(x)> be an ideal of F[x]. We know that polynomial ring over a field is a Euclidean domain and any ideal of Euclidean domain is maximal iff it is genearated by some irreducible element. Therefore F[x] is a Euclidean domain and $I = \langle p(x) \rangle$ is a maximal ideal as p(x) is irreducible.

Since every Euclidean domain possess unity, therefore F[x] is a commutative ring with unity. Since $\langle p(x) \rangle$ is maximal, so $F[x]/\langle p(x) \rangle$ is a field.

Consider E = $F[x]/\langle p(x) \rangle$

We claim that E is an extension of F. We define a mapping $\sigma : F \to E$ by $\sigma(\lambda) = \lambda + I$ for all $\lambda \in F$.

Then, for $\lambda_1, \lambda_2 \in F$, we have

$$\sigma(\lambda_1 + \lambda_2) = (\lambda_1 + \lambda_2) + 1$$
$$= (\lambda_1 + I) + (\lambda_2 + I)$$
$$= \sigma(\lambda_1) + \sigma(\lambda_2)$$

and $\sigma(\lambda_1 \lambda_2) = \lambda_1 \lambda_2 + 1$

$$= (\lambda_1 + I) + (\lambda_2 + I)$$
$$= \sigma(\lambda_1)\ \sigma(\lambda_2)$$

Therefore σ is a ring homomorphism.

Also, if $(\lambda_1) = \sigma(\lambda_2)$, we have

$$\Rightarrow \lambda_1 + I = \lambda_2 + I$$
$$\Rightarrow \lambda_1 - \lambda_2 \in I = \langle p(x) \rangle$$
$$\Rightarrow p(x) | \lambda_1 - \lambda_2$$
$$\Rightarrow \lambda_1 - \lambda_2 = 0$$
$$\Rightarrow \lambda_1 = \lambda_2$$

Therefore σ is monomorphism. Thus (E, σ) is an extension of F.

Let $p(x) = \lambda_0 + \lambda_1 x + \lambda_2 x^2 + \ldots + \lambda_n x^n \in I = \langle p(x) \rangle$.

Consider the element $\bar{x} = x + I \in E$. Then

$$p(\bar{x}) = \lambda_0 + \lambda_1 \bar{x} + \lambda_2 \bar{x}^2 + \ldots + \lambda_n \bar{x}^n$$
$$= \lambda_0 + \lambda (x+I) + \lambda_2 (x+I)^2 + \ldots + \lambda_n (x+I)^n$$
$$= (\lambda_0 + \lambda_1 x + \lambda_2 x^2 + \ldots + \lambda_n x^n) + I$$
$$= p(x) + I$$
$$= I \qquad [\because p(x) \in I]$$

Thus p(x) has a root $\bar{x}$ in E.

We claim that $1, \bar{x}, \bar{x}^2, \ldots, \bar{x}^{n-1}$ form a basis of E over F. Let us consider a representation.

$\lambda_0 1 + \lambda_1 \bar{x} + \lambda_2 \bar{x}^2 + \ldots + \lambda_{n-1} \bar{x}^{n-1} = \bar{0}$, identity of E.

$\Rightarrow \lambda_0 + \lambda_1 x + \lambda_2 x^2 + \ldots + \lambda_{n-1} x^{x-1} + I = I$

$\Rightarrow \lambda_0 + \lambda_1 x + \lambda_2 x^2 + \ldots + \lambda_{n-1} x^{x-1} \in I = \langle p(x) \rangle$

$\Rightarrow p(x) | \lambda_0 + \lambda_1 x + \lambda_2 x^2 + \ldots + \lambda_{n-1} x^{x-1}$

$\Rightarrow \lambda_0 = \lambda_1 = \lambda_3 = \ldots + \lambda_{n-1} = 0$ [$\because$ deg p(x) = n]