Def: Every non-zero polynomial in the polynomial domain F[x] over the field F, which has its multiplicative inverse in F[x] is called a unit in F[x].

Ex: $f(x) = 7$, $f(x) \in \mathbb{R}[x] \Rightarrow f(x)$ is unit since $\frac{1}{7} \in R[x]$ s.t. $7 \cdot \frac{1}{7} = 1$

Def: A non-zero polynomial f(x) in the polynomial domain F[x] of a field F is said to be an irreducible or a prime polynomial, if f(x) has no proper divisors, otherwise it is reducible
i.e. A non-zero polynomial $f(x) \in F[x]$ is irreducible over F (or irreducible in F[x]) if f(x) cannot expressed as a product $g(x) \cdot h(x)$ of two polys. g(x) and h(x) both of lower degree, ~~than the~~ of the degree of f(x). The poly which is not irreducible is said to be reducible.

Ex-: Let $f(x) = x^2 - 2$, $f(x) \in \mathbb{Q}[x]$
$\therefore f(x)$ is irreducible over $\mathbb{Q}$ since
$x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$, $\sqrt{2} \notin \mathbb{Q}$
But f(x) is reducible over $\mathbb{R}$, $\sqrt{2} \in \mathbb{R}$
i.e. $f(x) \in \mathbb{R}[x]$ then f(x) is reducible.

Scanned by TapScanner

Def.: An irreducible Polynomial $f(x)$ is a non-constant Polynomial such that in any factorization $f(x) = g(x)h(x)$ in $F[x]$ either $g(x)$ or $h(x)$ is a unit.

Ex. $6x+3 = 3(2x+1)$, $6x+3 \in Q[x]$
unite in Q

Ex: Show that $f(x) = x^3+3x+2$, $f(x) \in Z_5[x]$ is irreducible in $Z_5[x]$.

sol.: If $f(x)$ is reducible $\Rightarrow$ $f(x)$ has factored in $Z_5[x]$ into Poly. of lower degree $\Rightarrow \exists$ a lineal factor of $f(x)$ of the form $x-a$, for some $a \in Z_5$
$\Rightarrow f(a) = 0$

But $f(1)=1$, $f(2)=1$, $f(3)=3$, $f(4)=3$, $f(0)=2$
$\therefore f(x)$ has no root in Z_5
$\therefore f(x)$ is irreducible in $Z_5[x]$.

Theorem 4-7: let $f(x) \in F[x]$, and $f(x)$ is of degree 2 or 3 then $f(x)$ is reducible in F iff it has a root in F.

proof: ($\Rightarrow$) suppose that $f(x)$ is reducible in F
$\Rightarrow f(x) = g(x)\cdot h(x)$, $\deg g(x)$, $\deg h(x) < \deg f(x)$
$\because f(x)$ is either quadratic or cubic then either $\deg g(x)$ or $\deg h(x)$ is one.

Scanned by TapScanner

If $\deg g(x) = 1 \Rightarrow g(x) = x - a \Rightarrow g(a) = 0 \Rightarrow f(a) = 0$

$\Rightarrow f(x)$ ~~has~~ has a root in F.

($\Leftarrow$) suppose that $f(x)$ has a root in F, say a

$\Rightarrow x - a$ is a factor of $f(x)$ [$\deg f(x) = 2$ or 3]

$\Rightarrow f(x)$ is reducible

[لانها امتلكت جذر اي عامل

[$f(x) = (x-a)(\ )$

Theorem 4-8: Let $p \in \mathbb{Z}$ be a prime number. Suppose that $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ is in $\mathbb{Z}[x]$, and $a_n \not\equiv 0 \pmod p$, but $a_i \equiv 0 \pmod p$ for $i < n$, with $a_0 \not\equiv 0 \pmod{p^2}$. Then $f(x)$ is irreducible over $\mathbb{Q}$.

بدون برهان

Ex- Show that $f(x) \in \mathbb{Z}[x]$ s.t. ~~f(x)~~

$f(x) = 25x^5 - 9x^4 + 3x^2 - 12$ is irreducible ~~on~~ over $\mathbb{Q}$.

Sol: $a_0 = -12$, $a_1 = 0$, $a_2 = 3$, $a_3 = 0$, $a_4 = -9$, $a_5 = 25$

Take $p = 3$.

$a_0 = -12 \equiv 0 \pmod 3 \Rightarrow -12 - 0 = 3k \Rightarrow -12 = 3(-4)$

$a_1 = 0 \equiv 0 \pmod 3 \Rightarrow 0 = 3(0)$

$a_2 = 3 \equiv 0 \pmod 3 \Rightarrow 3 = 3(1)$

$a_3 = 0 \equiv 0 \pmod 3 \Rightarrow 0 = 3(0)$

$a_4 = -9 \equiv 0 \pmod 3 \Rightarrow -9 = 3(-3)$

$a_5 = 25 \not\equiv 0 \pmod 3 \Rightarrow 25 \neq 3k$, $k \in \mathbb{Z}$.

$a_0 = -12 \not\equiv 0 \pmod{3^2} \Rightarrow -12 \neq 9k$, $k \in \mathbb{Z}$

by theorem 4-8 $\Rightarrow f(x)$ is irreducible over $\mathbb{Q}$.

Scanned by TapScanner

نون برهان

the poly domain

Theorem 4-9: An ideal $(p(x)) \neq \{0\}$ of $F[x]$ is maximal iff $p(x)$ is irreducible over F.

proof: suppose that $(p(x))$ is maximal in $F[x]$

then $(p(x)) \neq F[x] \Rightarrow p(x) \in F[x]$

let $p(x) = f(x) \cdot g(x)$ in $F[x]$

$\because (p(x))$ is maximal $\Rightarrow (p(x))$ is prime [theorem 2-18]

$\therefore f(x) g(x) \in (p(x))$

$\Rightarrow$ either $f(x) \in (p(x))$ or $g(x) \in (p(x))$

$\Rightarrow f(x) = q(x)\, p(x)$

or $g(x) = r(x)\, p(x)$ c!

since the degree of both $f(x)$ and $g(x)$ can not be less than degree of $p(x)$.

$\therefore p(x)$ is irreducible over F

$(\Leftarrow)$ suppose that $p(x)$ is irreducible over F

T.P. $(p(x))$ is maximal in $F[x]$.

let N be an ideal of $F[x]$ s.t. $(p(x)) \subseteq N \subseteq F[x]$

By theorem 4-6 $\Rightarrow N$ is principal $\Rightarrow \exists\, g(x) \in F[x]$

s.t. $N = (g(x))$

$\because p(x) \in N \Rightarrow p(x) = \underset{\text{unit}}{\overset{\text{ثابت}}{q(x)}} \cdot g(x)$, $q(x) \in F[x]$

But $p(x)$ is irreducible, then either $q(x)$ or $g(x)$ is of degree zero.

If $g(x)$ is of degree $0 \Rightarrow g(x)$ is a unit in $F[x]$.

$(g(x)) = F[x]$

$\therefore N = F[x]$

Scanned by TapScanner

If $g(x)$ is of degree 0, then $g(x) = c \in F[x]$

and $g(x) = \frac{1}{c} P(x)$

$\Rightarrow g(x) \in (P(x)) \Rightarrow (g(x)) \subseteq (P(x))$

$\Rightarrow N \subseteq (P(x)) \Rightarrow N = (P(x))$

$\therefore (P(x))$ is maximal ideal in $F[x]$.

Chapter Five
The chain

Def-: Let $(R,+,\cdot)$ be a comm. ring then R is said to satisfy the Ascending chain condition (A.C.C) on ideal if $I_1 \subseteq I_2 \subseteq \cdots$ then there exist $n \in \mathbb{Z}_+$ such that $I_n = I_{n+1} = \cdots$

i.e. Every Ascending chain of ideals in a ring $(R,+,\cdot)$ must be stationary تتوقف

Ex- $(\mathbb{Z},+,\cdot)$ satisfies Ascending chain condition

$(8) \subseteq (4) \subseteq (2)$

Ex: $\mathbb{Z}_n$ satisfies A.C.C.

Theorem 5.1: For any ring $(R,+,\cdot)$, the following conditions are equivalent:

① R satisfies the A.C.C. on ideals

② Every non-empty collection of ideals has a maximal element.

Scanned by TapScanner

③ Every ideal of R is finitely generated.

proof: $1 \Rightarrow 2$ suppose that R satisfies the A.c.c.
let C be a non-empty collection of ideals in R.
$\because C \neq \phi \Rightarrow \exists I_1 \in C \Rightarrow I_1$ is not maximal ideal.
$\Rightarrow \exists I_2 \in C$ s.t. $I_1 \subseteq I_2$ and I_2 is not maximal.
$\Rightarrow \exists I_3 \in C$ s.t. $I_2 \subseteq I_3$ and I_3 is not maximal
and so on. Then we have $I_1 \subset I_2 \subset I_3 \subset \cdots$ C!
since R satisfies A.c.c.
$\therefore$ C has maximal element.

$2 \Rightarrow 3$ let I be an ideal of R and I is not finite generated.
$\because I \neq \phi \Rightarrow \exists a_1 \in I \Rightarrow$ s.t. $I_1 = (a_1) \subset I$
$\Rightarrow \exists a_2 \in I$, $a_2 \notin I_1 \Rightarrow I_1 \subset I_2 = (a_1, a_2)$
Thus we get $I_1 \subset I_2 \subset I$
and so on we have $a_n \in I$, $a_n \notin I_{n-1}$ s.t.
$I_1 \subset I_2 \subset \cdots \subset I_{n-1} \subset I \subset \cdots$
let $C = \{I_n : n \in Z\} \Rightarrow C \neq \phi$.
By ② C has maximal element
let I_K be a maximal element of C which is contradiction since $I_K \subset I_{K+1} \in C$
$\Rightarrow$ I must be finite generated.

$3 \Rightarrow 1$ Let $I_1 \subseteq I_2 \subseteq \cdots$ be the A.c.c. of ideals in R

put $I = \bigcup_n I_n$, I is an ideal of R

By hypotheses I is finite generated

$\Rightarrow \exists\, a_1, a_2, \ldots, a_m \in R$ s.t.

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

Assume that $a_1 \in I_{K_1}$, $a_2 \in I_{K_2}, \ldots, a_m \in I_{K_m}$

Let $r = \max\{K_1, \ldots, K_m\}$

$\Rightarrow a_1, a_2, \ldots, a_m \in I_r$

But $I_{r+1} \subseteq I$

$\Rightarrow I_{r+1} \subseteq I_r$ $[I \subseteq I_r]$

But $I_r \subseteq I_{r+1} \Rightarrow I_r = I_{r+1}$

$\therefore$ R satisfies the A.c.c.

Def: A ring $(R, +, \cdot)$ with identity is called Noetherian if R satisfies the A.c.c.

Scanned by TapScanner