E-Learning Materials for Sem - 6(T)

Unit - 1, CC - 14

Topic - Ring theory and Linear Algebra - II

Date - 16.04.2020.

Prepaired by - Dr. Alauddin Dafadar.

Eisenstein Criterion :⇒

Let p be a prime integer.

Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0 \in \mathbb{Z}[x]$

and $a_n \not\equiv 0 \pmod p$, $a_i \equiv 0 \pmod p$ for $i = 0, 1, \dots, n-1$

with $a_0 \not\equiv 0 \pmod{p^2}$.

Then $f(x)$ is irreducible over $\mathbb{Q}$.

or,

Let $(U, +, \cdot)$ be a UFD and $(\mathbb{Q}, +, \cdot)$ be a field of quotient.

Let $f(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n$ in $U[x]$

If there is a prime $p \in U$ s.t. $p \mid a_0, p \mid a_1, \dots, p \mid a_{n-1}$

but $p \nmid a_n$ and $p^2 \nmid a_0$

Then $f(x)$ is irreducible in $\mathbb{Q}[x]$.

Theorem 13 :⇒

If F be a field, then $F[x]$ is a principal ideal domain.

⇒ Let U be an ideal in $F[x]$. If $U = \{0\}$ then $U = \langle 0 \rangle$, a principal ideal.

Let $U \neq \{0\}$ and let $g(x)$ be a non-zero polynomial in U of minimal degree.

If the degree of $g(x)$ be zero, then $g(x) \in F[x]$. and it is a unit

so $U = \langle 1 \rangle = F[x]$ and it is a principal.

If $\deg(g(x)) \geq 1$, let $f(x)$ be any polynomial in U.

Then $f(x) = g(x) q(x) + r(x)$, where $q(x), r(x) \in F[x]$.

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

Since U is an ideal $g(x) \in U$, $q(x) \in F[x]$

$\Rightarrow g(x)q(x) \in U$

and $f(x) \in U$, $g(x)q(x) \in U$,

$\Rightarrow r(x) \in U$.

Since $g(x)$ is a polynomial of minimal degree in $F[x]$, it follows that $r(x) = 0$, consequently $f(x) = g(x)q(x)$ and therefore $U = \langle g(x) \rangle$, a principal ideal.

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

Theorem 14 :⇒ P – 300

If F be a field, then $F[x]$ is a Euclidean domain.

⇒ Since F is a field, F is an integral domain and therefore $F[x]$ is an integral domain.

Let us define a map v from the set of non-zero elements of $F[x]$ to the set of non-negative integer by $v(f(x)) = \deg(f(x))$ for all non-zero polynomial $f(x) \in F[x]$.

i) If $f(x), g(x)$ be non-zero polynomial in $F[x]$, then

$$v[f(x)g(x)] = \deg(f(x)g(x))$$
$$= \deg(f(x)) + \deg(g(x)), \text{ since } F[x] \text{ is an integral domain}$$
$$\geq \deg(f(x)) = v(f(x))$$

ii) If $f(x), g(x)$ be non-zero polynomial in $F[x]$, then by divison algorithom $\exists$ unique polynomial $r(x)$ and $q(x)$ in $F[x]$ such that $f(x) = g(x)q(x) + r(x)$, where either $r(x) = 0$ or, $\deg(r(x)) < \deg(g(x))$ i.e; $v(r(x)) < v(g(x))$.

Thus both the conditions for a Euclidean valuation are satisfied by v and, hence F[x] is a Euclidean domain.

Ex-20 Show that the polynomial $f(x) = x^2 + x + 1$ is irreducible over the field $(F, +_{11}, \odot_{11})$ of integers modulo 11.

⇒ The elements of F are $0, 1, 2, \ldots, 10$

If $f(x)$ is irreducible then it must have a linear factor $x - a$ where a is zero of $f(x)$.

we have $f(0) = 0 +_{11} 0 +_{11} 1$

$= 1$

$f(1) = 1^2 +_{11} 1 +_{11} 1 = 3$

$f(2) = 2^2 +_{11} 2 +_{11} 1 = 7$, $f(3) = 3^2 +_{11} 3 +_{11} 1 = 0$

$f(4) = 4^2 +_{11} 4 +_{11} 1 = 10$, $f(5) = 5^2 +_{11} 5 +_{11} 1 = 8$

$f(6) = 6^2 +_{11} 6 +_{11} 1 = 7$, $f(7) = 7^2 +_{11} 7 +_{11} 1 = 10$

$f(8) = 8^2 +_{11} 8 +_{11} 1 = 8$, $f(9) = 9^2 +_{11} 9 +_{11} 1 = 3$, $f(10) = 10^2 +_{11} 10 +_{11} 1 = 1$.

This shows that $f(x)$ has no zero in F

$\therefore f(x)$ is irreducible.

Ex.21: Examine if the polynomial $x^3 + x^2 + x + 1$ is irreducible over $\mathbb{Z}_2$.

⇒ If $x^3 + x^2 + x + 1$ be reducible then $x^3 + x^2 + x + 1 = g(x)\,h(x)$ where both $g(x)$ and $h(x)$ are polynomial of lower degree.

Then one of the $g(x)$ must be of degree 1.

$\therefore g(x) = x - a$, for some $a \in \mathbb{Z}_2$

$\therefore f(a) = 0$ where $f(x) = x^3 + x^2 + x + 1$ but

$f(0) = 0+0+0+1 = 1$, $f(1) = 1+1+1+1 = 0$.

This shows that $f(x)$ has a zero in $\mathbb{Z}_2$ hence $f(x)$ is reducible over $\mathbb{Z}_2$.

Ex. 22 Examine if the polynomial $2x^3 + 3x^2 + 2x + 3$ is irreducible over $\mathbb{Z}_7$.

⇒ If $2x^3 + 3x^2 + 2x + 3$ be reducible then

$f(x) = g(x) \cdot h(x)$, where $f(x) = 2x^3 + 3x^2 + 2x + 3$ and $g(x), h(x)$ are polynomial.

One of, say $g(x) = x - a$, for some $a \in \mathbb{Z}_7$

$\therefore f(a) = 0$, where $f(x) = 2x^3 + 3x^2 + 2x + 3$

but $f(0) = 3$, $f(1) = 10$, $f(2) = 0$, $f(3) = 6$.

This shows that $f(x)$ has a zero in $\mathbb{Z}_2$ hence $f(x)$ is reducible over $\mathbb{Z}_7$.

Note: ⇒ $3x^2 + 6$ is reducible over $\mathbb{Z}$ because $3x^2 + 6 = 3(x^2 + 2)$ where 3 is not a unit in $\mathbb{Z}$ and 3 is a proper division of $3x^2 + 6$

But $3x^2 + 6$ is irreducible over $\mathbb{Q}$ because 3 is a unit in $\mathbb{Q}$ and no 3 is not a proper division of $3x^2 + 6$

Ex. 23: Show that $5x^4 + 4x^3 - 6x^2 - 11x + 2$ is irreducible over $\mathbb{Z}$.

⇒ Let $f(x) = 5x^4 + 4x^3 - 6x^2 - 11x + 2$ here

2×5, $2 \mid 4$, $2 \mid (-6)$, $2 \mid (-11)$, $2 \mid 2$, but $2^2 \nmid 2$.

$\therefore f(x)$ is irreducible polynomial over $\mathbb{Z}$ by Eisenstein criterion

Ex. 24 : show that $2x^4 + 6x^3 - 9x^2 + 15$ is irreducible over $\mathbb{Z}$.

⇒ Let $f(x) = 2x^4 + 6x^3 - 9x^2 + 15$

$15 = 3 \cdot 5$

3 is a prime in $\mathbb{Z}$ and $3 \nmid 2$, $3 \mid 6$, $3 \mid (-9)$, $3 \mid 15$.

but $3^2 \nmid 15$

By 'Eisenstein criterian' $f(x)$ is irreducible over $\mathbb{Q}$

More over $\gcd\{2, 6, -9, 15\} = 1$

$\therefore$ $f(x)$ is primitive and hence $f(x)$ is irreducible over $\mathbb{Z}$.

Ex. 25 show that $x^3 + 2x^2 + 3$ is irreducible over $\mathbb{Q}$.

⇒ Let $f(x) = x^3 + 2x^2 + 3$

Since $\deg(f(x)) = 3$,

we have : if $f(x)$ is not irreducible over $\mathbb{Q}$ then $f(x)$ must have a linear factor i.e., $f(x)$ has a root over $\mathbb{Q}$.

The possible root of $f(x)$ $\frac{p}{q}$, $p, q \in \mathbb{Z}$, $q \neq 0$.

$\frac{p}{3}$, $\frac{q}{1}$.

The only possibility are ± 3, but $f(3) = 48 \neq 0$.

and $f(-3) = -6 \neq 0$.

$\therefore$ $f(x)$ has no linear factor and hence $f(x)$ is irreducible over $\mathbb{Q}$.

Ex.26 show that $x^3 + x^2 + \bar{1}$ is irreducible over $\mathbb{Z}_2$.

⇒ let $f(x) = x^3 + x^2 + \bar{1}$.

if $f(x) = g(x)\,h(x)$, $g(x)$, $h(x)$ both polynomial of lower degree.

then one of them say $g(x)$ must be of degree 1.

and then $g(x) = x - a$ for some $a \in \mathbb{Z}_2$.

$\therefore f(a) = 0$ but $f(\bar{0}) = \bar{1}$, $f(\bar{1}) = \bar{3} = \bar{1}$.

This shows that $f(x)$ has no zero in $\mathbb{Z}_2$ so $f(x)$ is irreducible in $\mathbb{Z}_2$.

Ex.27 show that $x^3 + \bar{9}$ is irreducible over $\mathbb{Z}_3$.

⇒ Let $f(x) = x^3 + \bar{9}$.

if $f(x) = g(x)\,h(x)$, where $g(x)$, $h(x)$ both polynomial of lower degree.

Then one of them say $g(x)$ must have be of degree 1.

and then $g(x) = x - a$ for some $a \in \mathbb{Z}_3$.

$\therefore f(a) = 0$. but $f(\bar{0}) = \bar{9} = \bar{0}$. $f(\bar{1}) = \bar{10} = \bar{1}$.

This show that $f(x)$ has a zero in $\mathbb{Z}_2$.

so $f(x)$ is reducible over $\mathbb{Z}_2$.

Ex.28 Let F be a field. show that every polynomial of degree one is an irreducible polynomial in $F[x]$.

⇒ Since $\deg(f(x)) = 1$ then $f(x)$ is non zero non unit.

Suppose $f(x) = g(x)\,h(x)$, $g(x)$, $h(x) \in F[x]$.

$g(x)$, $h(x)$ are non-zero polynomials.

Here $1 = \deg(f(x)) = \deg(g(x)) + \deg(h(x))$

either $\deg(g(x)) = 1$ $\quad$ $\deg(h(x)) = 0$

or, $\deg(g(x)) = 0$ $\quad$ or, $\deg(h(x)) = 0, 1$.

$\Rightarrow$ $g(x) \in F - \{0\}$ or, $h(x) \in F - \{0\}$.

$\Rightarrow$ Either $g(x)$ is unit or $h(x)$ is unit.

$\Rightarrow$ $f(x)$ is irreducible.

Ex. 29 show that $x^3 + [2]x + [4]$ is irreducible in $\mathbb{Z}_5[x]$

$\Rightarrow$ Let $f(x) = x^3 + [2]x + [4]$. ~~is irreducible in $\mathbb{Z}_5[x]$~~

$f([0]) = [4]$, $f([1]) = [7] = [2]$, $f([2]) = [16] = [1]$.

$f([3]) = [37] = [2]$. $f([4]) = [76] = [1]$.

This shows that $f(x)$ has no root in $\mathbb{Z}_5[x]$.

$\Rightarrow$ $f(x)$ is irreducible in $\mathbb{Z}_5[x]$.

Ex. 30 Find all irreducible polynomial of degree 2 of $\mathbb{Z}_2[x]$.

$\Rightarrow$ Any polynomial of degree 2 in $\mathbb{Z}_2[x]$ each of the form $ax^2 + bx + c$ where $a, b, c \in \mathbb{Z}_2$, $a \neq \bar{0}$.

$\therefore a = \bar{1}$.

Then the only polynomial of degree 2 in $\mathbb{Z}_2[x]$ are x^2, $x^2 + x$, $x^2 + \bar{1}$ and $x^2 + x + \bar{1}$.

Now $x^2 = x \cdot x$, $x^2 + x = x(x+1)$, $x^2 + \bar{1} = (x+i)(x-i)$

This shows that the above three polynomial are reducible

Let $f(x) = x^2 + x + \bar{1}$

$f(\bar{0}) = \bar{1} \neq \bar{0}$

$f(\bar{1}) = \bar{3} = \bar{1} \neq \bar{0}$.

$\therefore f(x)$ has no root in $\mathbb{Z}_2$.

$\therefore x^2+x+\bar{1}$ is irreducible over $\mathbb{Z}_2$.

Ex.31 Show that the number of irreducible polynomial of degree 2 in $\mathbb{Z}_p[x]$ $\frac{p(p-1)}{2}$, p is prime

⇒ Let $f(x) = x^2 + ax + b \in \mathbb{Z}_p[x]$ where $a, b \in \mathbb{Z}_p$

since $|\mathbb{Z}_p| = p$.

$\therefore$ There are p^2 such polynomial in $\mathbb{Z}_p[x]$

If $f(x)$ is not irreducible then

$f(x) = (x-\alpha)(x-\beta)$, for some $\alpha, \beta \in \mathbb{Z}_p$.

Now we have to find how many such distinct product of factors occurs

If α, β distinct then the number is ${}^pC_2$ or $\binom{p}{2}$

$= \frac{p(p-1)}{2}$

If $\alpha = \beta$ then the no. is p. [In this case we assume $(x-\alpha)(x-\beta)$ and $(x-\beta)(x-\alpha)$ are the same product of factor]

$\therefore$ Total no of distinct product $p + \frac{p(p-1)}{2} = \frac{p(p+1)}{2}$.

$\therefore$ The required no. of irreducible polynomial over $\mathbb{Z}_p$ of degree 2 is $p^2 - \frac{p(p+1)}{2} = \frac{p(p-1)}{2}$.

Ex.32 Let $f(x) = x^5 + \bar{2}x^4 + \bar{2}x^3 + \bar{3}x^2 + \bar{4}x + \bar{3}$

$g(x) = x^3 - \bar{2}x^2 + \bar{3}x - \bar{1}$.

in $\mathbb{Z}_6[x]$ find the polynomial $q(x)$ and $r(x) \in \mathbb{Z}_6[x]$ show that $f(x) = q(x)g(x) + r(x)$ where either $r(x) = 0$, or $\deg(r(x)) < \deg(g(x))$

References - Higher Algebra - ⑧
S.K. Mapa.