Lecture 31

Oct 25, 2022

Note Title 10/26/2022

__Nilpotent element:__ Let R be a ring. An element $a \in R$ is called nilpotent if $\exists\, n \geq 1$ such that $a^n = 0$.

- 0 is always a nilpotent element in any ring R.
- In $\mathbb{Z}_4$, 0 and 2 are both nilpotent elements.
- In an integral domain D, 0 is the only nilpotent element.

__Theorem__ Let R be a commutative ring with identity. Then, $f(x) = a_0 + a_1 x + \dots + a_n x^n \in R[x]$ is a unit if and only if $a_0 \in U(R)$ and $a_1, \dots, a_n$ are nilpotent elements in R.

(1) Let R be an integral domain.

Then, $U(R[x]) = U(R)$ (Since in an integral domain, 0 is the only nilpotent element).

$\therefore$ $U(\mathbb{Z}[x]) = U(\mathbb{Z}) = \{1, -1\}$.

That is, 1 and -1 are the only polynomials in $\mathbb{Z}[x]$ which are units.

(2) Let $R = \mathbb{Z}_4$. Then, $1 + 2x^3 \in U(\mathbb{Z}_4[x])$ since 2 is a nilpotent element of $\mathbb{Z}_4$.

Clearly, inverse of $1 + 2x^3$ is $1 + 2x^3$.

- $(1+2x^3) \cdot (1+2x^3) = 1 + 4x^3 + 4x^6 = 1$ in $\mathbb{Z}_4[x]$.

(3) Let F be a field. Then $U(F[x]) = U(F) = F \setminus \{0\}$.

Thus, the units in $F[x]$ are nonzero constant polynomials.

§ <u>Factorization in Polynomial rings</u>:

Let R be commutative with identity.

Let $f(x) \in R[x]$. We say that $a \in R$ is a zero of f if $f(a) = 0$.

(1) Let F be a field, $\alpha \in F$ and $f(x) \in F[x]$.

Applying division algorithm, we find that α is a zero of $f(x)$ if and only if $x - \alpha$ is a factor of $f(x)$, that is, $f(x) = (x-\alpha)\, g(x)$ for some $g(x) \in F[x]$

(2) A polynomial of degree n over a field has at most n zeros, counting multiplicity.

<u>Proof</u>: Follows from division algorithm.

In general, the statement (2) is not true.

For example, let $f(x) = 2x \in \mathbb{Z}_4[x]$. Then, $\deg f = 1$ but f has two zeros, namely, 0 and 2.

<u>Definition (irreducible polynomial)</u>: Let R be a commutative ring with identity. A polynomial $f(x) \in R[x]$ is called irreducible if

(1) f is non-zero and non-unit ($f \neq 0$ and $f \notin U(R[x])$).

(2) whenever $f(x) = h(x) \cdot g(x)$, then either $h(x)$ is unit or $g(x)$ is unit.

A reducible polynomial is a polynomial which is not irreducible.

__Ex:__ Let $f(x) = 4+2x^2$. Clearly, $f \neq 0$ and $f \notin U(\mathbb{Z}[x])$.
we have $f(x) = 2(2+x^2)$ and both 2 and $2+x^2$ are non-units.
$\therefore$ $4+2x^2$ is __not__ irreducible over $\mathbb{Z}$.
However, $4+2x^2$ is irreducible in $\mathbb{Q}[x]$.

__Ex:__ The polynomial x^2-5 is irreducible over $\mathbb{Q}$ but reducible over $\mathbb{R}$.

__Ex:__ Let F be a field. Then, every degree 1 polynomial in $F[x]$ is irreducible.

Theorem (Root test): Let F be a field. If $f(x) \in F[x]$ and $\deg f$ is 2 or 3, then f is reducible if and only if $f(x)$ has a zero in F.

Proof: Let $\deg f \geq 2$ and $\alpha \in F$ is a zero of f.

Then, $f(x) = (x-\alpha) \cdot h(x)$. Since $\deg f \geq 2$, so $\deg h = \deg f - 1 \geq 1$.

$\therefore$ Both $x - \alpha$ and $h(x)$ are non-units.

$\Rightarrow f$ is reducible.

Conversely, suppose that $\deg f = 2$ or 3 and f is reducible.

Let $f(x) = h(x) g(x)$, where both $h(x)$ and $g(x)$ are non-units.

$\therefore \deg h \geq 1$ and $\deg g \geq 1$.

If $\deg f = 2$, then $\deg h = \deg g = 1$

$\therefore$ $h(x) = ax + b$ with $a \neq 0$. Then, $\alpha = -a^{-1}b$ is a root of $f(x)$.

If $\deg f = 3$, then $\deg h + \deg g = 3$

$\Rightarrow$ either $\deg h = 1$ or $\deg g = 1$

In any case, $f(x)$ has a root. #

—— x ——

<u>Ex</u>: Let $f(x) = x^2 + 1 \in \mathbb{Z}_3[x]$. Note that $\mathbb{Z}_3$ is a field.

$f(0) = 1$, $f(1) = 2$, $f(2) = 5 = 2$.

$\therefore$ $f(x)$ does not have any root in $\mathbb{Z}_3$.

Since $\deg f = 2$, so f is irreducible in $\mathbb{Z}_3[x]$.

But x^2+1 is reducible in $\mathbb{Z}_5[x]$ since 2 is a zero of x^2+1 in $\mathbb{Z}_5$.

<u>Ex:</u> In $\mathbb{Z}_2[x]$, degree 1 irreducible polynomials are x and $1+x$.
In $\mathbb{Z}_2[x]$, degree 2 irreducible polynomial is $1+x+x^2$.
In $\mathbb{Z}_2[x]$, degree 3 irreducible polynomials are

$$x^3+x^2+1 \quad \text{and} \quad x^3+x+1.$$

#

<u>Thm:</u> (Rational Root test) Let $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x]$. Then, if $\alpha = \frac{m}{k}$, $\gcd(m,k)=1$, is a rational root of $f(x)=0$, then $m \mid a_0$ and $k \mid a_n$.

<u>Proof.</u> If $f(\alpha)=0$, then $a_0 + a_1 \frac{m}{k} + a_2 \frac{m^2}{k^2} + \cdots + a_n \frac{m^n}{k^n} = 0$

$\Rightarrow a_0 k^n + a_1 m k^{n-1} + \cdots + a_{n-1} m^{n-1} k + a_n m^n = 0$

$\therefore\ m \mid a_0 k^n$ and $k \mid a_n m^n$.

Since $\gcd(m, k) = 1$, so $m \mid a_0$ and $k \mid a_n$. #

<u>Ex:</u> Let $f(x) = 1 + 2x + 3x^3 \in \mathbb{Z}[x]$.

By Rational root test, if $\alpha = \frac{m}{k}$, $\gcd(m,k) = 1$, is a root of $f(x) = 0$, then $m \mid 1$ and $k \mid 3$

$\Rightarrow m = \pm 1$ and $k = \pm 1, \pm 3$

$\therefore\ \alpha = \pm 1, \pm \frac{1}{3}$. But for these values of α, $f(\alpha) \neq 0$.

$\therefore\ 1 + 2x + 3x^3$ is irreducible in <u>$\mathbb{Q}[x]$</u>.

__Mod p irreducibility test:__ Let p be a prime and suppose that $f(x) \in \mathbb{Z}[x]$ with $\deg f \geq 1$. Let $\overline{f(x)} \in \mathbb{Z}_p[x]$ be the polynomial obtained by reducing all the co-efficients of $f(x)$ modulo p. If $\overline{f(x)}$ is irreducible over $\mathbb{Z}_p$ and $\deg f(x) = \deg \overline{f(x)}$, then $f(x)$ is also irreducible over $\mathbb{Q}$.

__Ex:__ $f(x) = 1 + 5x + 7x^2 \in \mathbb{Z}[x]$. Take $p = 5$.

Then, $\overline{f(x)} = 1 + 2x^2 \in \mathbb{Z}_5[x]$.

Now, $\overline{f(0)} = 1$, $\overline{f(1)} = 3$, $\overline{f(2)} = 9 = 4$, $\overline{f(3)} = 4$, $\overline{f(4)} = 3$.

$\therefore$ $\overline{f(x)}$ has no zero in $\mathbb{Z}_5$. Since $\deg \overline{f(x)} = 2$, so $\overline{f(x)}$ is irreducible in $\mathbb{Z}_5[x]$. Also, $\deg f = \deg \overline{f}$, hence f is irreducible over $\mathbb{Q}$.

Ex: $f(x) = 21x^3 - 3x^2 + 2x + 9$.

Then, over $\mathbb{Z}_2$, $\overline{f(x)} = x^3 + x^2 + 1$ which is irreducible over $\mathbb{Z}_2$.

Since $\deg f = \deg \overline{f}$, so f is irreducible over $\mathbb{Q}$.

—— x ——