Lecture 32 — 28th Oct, 2022

Note Title — 10/28/2022

Let $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x]$ be a non-zero polynomial.
The content of $f(x)$ is defined to be the gcd of $a_0, a_1, \ldots, a_n$ and is denoted by $\text{cont}(f)$.

Thus, $\text{cont}(f) = \gcd(a_0, a_1, a_2, \ldots, a_n)$.

If $\text{cont}(f) = 1$, then f is called a primitive polynomial.

<u>Gauss Lemma</u>: The product of two primitive polynomials is primitive.

<u>Proof</u>: Let $f(x), g(x) \in \mathbb{Z}[x]$ be two primitive polynomials

<u>Claim</u>: $f(x) \cdot g(x)$ is primitive.

Suppose that $f(x) \cdot g(x)$ is <u>not</u> primitive.

Then, content of fg is greater than 1.

Let p be a prime which divides $\text{cont}(fg)$.

Let $\overline{f(x)}$, $\overline{g(x)}$, $\overline{f(x)g(x)}$ be the polynomials obtained from $f(x)$, $g(x)$ and $f(x)g(x)$ respectively, by reducing the coefficients modulo p. Then, $\overline{f(x)}, \overline{g(x)}, \overline{f(x)g(x)} \in \mathbb{Z}_p[x]$.

Since p divides the content of $f(x).g(x)$, so p divides all the coefficients of $f(x)g(x)$.

$\therefore \overline{f(x)g(x)} = 0$ in $\mathbb{Z}_p[x] \Rightarrow \overline{f(x)} \cdot \overline{g(x)} = 0$ in $\mathbb{Z}_p[x]$

Since $\mathbb{Z}_p$ is an integral domain, so $\mathbb{Z}_p[x]$ is an integral domain

$\therefore$ Either $\overline{f(x)} = 0$ in $\mathbb{Z}_p[x]$ or $\overline{g(x)} = 0$ in $\mathbb{Z}_p[x]$.

$\Rightarrow$ either p divides all the coefficients of $f(x)$
OR p divides all the coefficients of $g(x)$.

$\Rightarrow$ either p divides $\mathrm{cont}(f)$ OR p divides $\mathrm{cont}(g)$.

This is a contradiction, since both $f(x)$ and $g(x)$ are primitive polynomials.

This proves that $f(x)\,g(x)$ must be a primitive polynomial.

———— x ————

Theorem 1: Let $f(x) \in \mathbb{Z}[x]$.
If $f(x)$ is irreducible over $\mathbb{Z}$, then $f(x)$ is irreducible over $\mathbb{Q}$.
Equivalently, if $f(x)$ is reducible over $\mathbb{Q}$, then it is reducible over $\mathbb{Z}$.

__Proof:__ Let $f(x) \in \mathbb{Z}[x]$. Suppose that $f(x)$ is reducible over $\mathbb{Q}$.

Let $f(x) = g(x)\,h(x)$, where $g(x), h(x) \in \mathbb{Q}[x]$.

Let $\mathrm{cont}(f) = k$. Then, $f_1(x) = \dfrac{f(x)}{k} \in \mathbb{Z}[x]$ and $\mathrm{cont}(f_1) = 1$

Let $g_1(x) = \dfrac{g(x)}{k}$.

Then, $f_1(x) = g_1(x)\,h(x)$.

Let 'a' be the least common multiple of the denominators of the coefficients of $g_1(x)$, and let 'b' be the least common multiple of the denominators of the coefficients of $h(x)$.

Then, $\boxed{ab\, f_1(x) = a g_1(x) \cdot b\, h(x).}$ ① Clearly, $a g_1(x) \in \mathbb{Z}[x]$ $b \cdot h(x) \in \mathbb{Z}[x]$.

Since $a \cdot g_1(x) \in \mathbb{Z}[x]$, so $a \cdot g_1(x) = c_1\, g_2(x)$, where $c_1 = \text{cont}(a \cdot g_1(x))$ and $g_2(x)$ is primitive.

Similarly, since $bh(x) \in \mathbb{Z}[x]$, so $b \cdot h(x) = c_2\, h_1(x)$, where $c_2 = \text{cont}(b \cdot h(x))$ and $h_1(x)$ is primitive.

Since $f_1(x)$ is primitive, so $\text{cont}(ab \cdot f_1(x)) = ab$.

Now, $a\, g_1(x) \cdot b\, h(x) = c_1\, g_2(x)\, c_2 h_1(x) = c_1 c_2\, g_2(x) h_1(x)$.

Since $g_2(x)$ and $h_1(x)$ are primitive, so $g_2(x)\, h_1(x)$ is primitive.

$\therefore \text{cont}(a \cdot g_1(x)\, b\, h(x)) = c_1 c_2$

From (1), we have $ab = c_1 c_2$

Thus, $ab\, f_1(x) = c_1 c_2\, g_2(x)\, h_1(x)$

$\Rightarrow f_1(x) = g_2(x)\, h_1(x)$, where $f_1(x), g_2(x), h_1(x) \in \mathbb{Z}[x]$.

Now, $f(x) = k f_1(x) = k\, g_2(x) h_1(x)$ over $\mathbb{Z}$.

Clearly, $\deg g_2 = \deg g_1 = \deg g$

$\deg h_1 = \deg h$

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

This completes the proof.

———— x ————

We now give a proof of "mod p irreducibility test" where we will use Theorem 1.

<u>Mod p irreducibility test:</u> Let $f(x) \in \mathbb{Z}[x]$ and $\deg f \geq 1$. Suppose that, for a prime p, $\overline{f(x)} \in \mathbb{Z}_p[x]$ is irreducible over $\mathbb{Z}_p$ and $\deg f(x) = \deg \overline{f(x)}$. Then, $f(x)$ is irreducible over $\mathbb{Q}$.

<u>Proof:</u> Suppose that $f(x)$ is reducible over $\mathbb{Q}$.

Then, by Theorem 1, $f(x)$ is reducible over $\mathbb{Z}$.

Hence, $f(x) = g(x)\, h(x)$ for some $g(x)\, h(x) \in \mathbb{Z}[x]$, and both have degree less than that of $f(x)$.

Now, $\overline{f(x)} = \overline{g(x)} \cdot \overline{h(x)}$

Since, $\deg f(x) = \deg \overline{f(x)}$, so $\deg \overline{g(x)} \leq \deg g(x) < \deg f(x) = \deg \overline{f(x)}$

and $\deg \overline{h(x)} \leq \deg h(x) < \deg f(x) = \deg \overline{f(x)}$.

Thus, $\overline{f(x)} = \overline{g(x)} \cdot \overline{h(x)}$ with $\deg \overline{g(x)} < \deg \overline{f(x)}$

and $\deg \overline{h(x)} < \deg \overline{f(x)}$.

$\Rightarrow$ $\overline{f(x)}$ is reducible over $\mathbb{Z}_p$, which is a contradiction.

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

—— x ——

Theorem 2 (Eisenstein criterion): Let $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x]$. If there is a prime p such that $p \nmid a_n$, $p \mid a_{n-1}, \ldots, p \mid a_0$ but $p^2 \nmid a_0$, then $f(x)$ is irreducible over $\mathbb{Q}$.

Ex: $f(x) = 3x^5 + 15x^4 - 20x^3 + 10x + 20 \in \mathbb{Z}[x]$.

Clearly, $p = 5$ satisfies Eisenstein criterion, and hence $f(x)$ is irreducible over $\mathbb{Q}$.

Theorem 3: Let F be a field. Let $f(x) \in F[x]$.
Then, $f(x)$ is irreducible over $F \Leftrightarrow (f(x))$ is a maximal ideal in $F[x]$.

Proof: Let $f(x)$ be irreducible. Hence, $f(x) \notin U(F[x]) \Rightarrow (f(x)) \neq F[x]$.

Let $(f(x)) \subseteq I \subseteq F[x]$. Since $F[x]$ is PID, so $I = (g(x))$ for some $g(x) \in F[x]$.

Now, $(f(x)) \subseteq (g(x))$

$\Rightarrow f(x) = g(x) \cdot h(x)$.

Since f is irreducible, so either $g(x)$ is unit or $h(x)$ is unit.

If $g(x)$ is a unit, then $(g(x)) = F[x]$.

If $h(x)$ is a unit, then $h(x) = a$, $a \neq 0$, $a \in F$.

$\therefore g(x) = a^{-1} \cdot f(x) \in (f(x)) \Rightarrow (g(x)) \subseteq (f(x))$.

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

This proves that $(f(x))$ is a maximal ideal in $F[x]$.

Conversely, suppose that $(f(x))$ is a maximal in $F[x]$.

Then, $(f(x)) \neq F[x]$ and $(f(x)) \neq (0)$.

$\therefore$ $f(x)$ is nonzero and non-unit.

Now, let $\boxed{f(x) = h(x)\, g(x)}$ * over F.

Then, $(f(x)) \subseteq (h(x))$ and $(f(x)) \subseteq (g(x))$.

$\Rightarrow (h(x)) = (f(x))$ or $(h(x)) = F[x]$ ($\because (f(x))$ is maximal)

$\Rightarrow h(x) = f(x)\, k(x)$ or $h(x)$ is a unit

$\Rightarrow g(x)\, k(x) = 1$ (using *)

$\Rightarrow g(x)$ is a unit

This also implies that either $h(x)$ is a unit or $g(x)$ is a unit.

Hence, $f(x)$ is irreducible,

This completes the proof. #

Let F be a field. Let $f(x) \in F[x]$ and $\deg(f) = n$.

Then, $F/(f(x)) = \{a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} + (f(x)) \mid a_i \in F\}$

by applying the division algorithm applied to $F[x]$.

Let $f(x) = 1 + x + x^3 \in \mathbb{Z}_2[x]$.

Since $1+x+x^3$ is irreducible over $\mathbb{Z}_2$, so $\mathbb{Z}_2[x]/(1+x+x^3)$ is a field. Now, $\mathbb{Z}_2[x]/(1+x+x^3) = \{a + bx + cx^2 + (1+x+x^3) \mid a, b, c \in \mathbb{Z}_2\}$

is a field which contains $2^3 = 8$ elements.

$\therefore$ $\mathbb{Z}_2[x]/(1+x+x^3)$ is a finite field with 8 elements.

In general we have the following theorem.

<u>Theorem 4:</u> Let p be a prime, and let $f(x)$ be an irreducible polynomial of degree n over $\mathbb{Z}_p$.

Then, $\mathbb{Z}_p[x]/(f(x))$ is a field of order p^n.

<u>Proof:</u> Since $f(x)$ in irreducible over $\mathbb{Z}_p$, so $\mathbb{Z}_p[x]/(f(x))$ is a field.

By division algorithm,

$$\mathbb{Z}_p[x]/(f(x)) = \{a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} + (f(x)) \mid a_i \in \mathbb{Z}_p\}$$

clearly, $\mathbb{Z}_p[x]/(f(x))$ has p^n elements.

#