Lecture 38

17 Factorization of polynomials

17.1 Reducibility Tests

Definition 17.1 (Irreducible/Reducible Polynomial)**.** Let D be an integral domain. A polynomial $f(x) \in D[x]$ that is neither 0 nor a unit in $D[x]$ is said to be irreducible over D if whenever $f(x) = g(x)h(x)$, then $g(x)$ or $h(x)$ is a unit in $D[x]$. A nonzero, nonunit element of $D[x]$ that is *not* irreducible is said to be reducible.

Example 17.1.

$$\begin{aligned} f(x) &= 2x^2 + 4 \\ &= 2 \cdot (x^2 + 2) \\ &= 2(x + \sqrt{-2})(x - \sqrt{-2}) \end{aligned}$$

Reducible over $\mathbb{Z}$, $\mathbb{C}$. Irreducible over $\mathbb{Q}$, $\mathbb{R}$.

Example 17.2. $x^2 - 2 = (x + \sqrt{2})(x - \sqrt{2})$ is irreducible over $\mathbb{Q}$ but reducible over $\mathbb{R}$.

Theorem 17.1 (Reducibility Test for Degrees 2 and 3)**.** Let F be a field and $f(x) \in F[x]$ such that $\deg f = 2$ or 3. Then $f(x)$ is reducible over $F \Longleftrightarrow f(x)$ has a zero in F.

Pf sketch. If $f(x) = g(x)h(x)$ then $\deg g(x) + \deg h(x) = \deg f(x) = 2$ or 3. So $g(x)$ or $h(x)$ has a degree of 1 (if $\deg g(x) = 0$ or $\deg h(x) = 0$ then $g(x)$ or $h(x)$ is a unit).

$$\begin{aligned} \deg 1 &\implies ax + b, \quad a, b \in F \\ &\implies a(x + \frac{b}{a}) \\ &\implies -\frac{b}{a} \text{ is a zero of } f(x) \end{aligned}$$

□

Example 17.3. $x^2 + 1$ is irreducible over $\mathbb{Z}_3 \quad \Longleftarrow \quad (0^2 + 1 = 1,\ 1^2 + 1 = 2,\ 2^2 + 1 = 5 = 2 \text{ in } \mathbb{Z}_3)$

$x^2 + 1$ is reducible over $\mathbb{Z}_5 \quad \Longleftarrow \quad (x^2 + 1 = (x - 2)(x - 3) \text{ in } \mathbb{Z}_5[x])$

Exercise. Prove Example 17.3

Example 17.4. $x^4 + 2x^2 + 1 = (x^2 + 1)^2$ is reducible over $\mathbb{Q}$ (or $\mathbb{R}$) in $\mathbb{Q}[x]$ (or $\mathbb{R}[x]$) but $x^4 + 2x^2 + 1$ has no zeros in $\mathbb{Q}$ (or in $\mathbb{R}$)

Definition 17.2 (Content of a Polynomial, Primitive Polynomial)**.** The content of a nonzero polynomial

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$$

is the greatest common divisor of $a_n, a_{n-1}, \ldots, a_0$. A primitive polynomials is an element in $\mathbb{Z}[x]$ with content 1.

Lemma 17.1 (Gauss's Lemma)**.** The product of two primitive polynomials in $\mathbb{Z}[x]$ is primitive.

Proof. Assume $f(x), g(x)$ are primitive, and suppose $f(x)g(x)$ is not primitive. Let p be a prime divisor of the content of $f(x)g(x)$. Consider the ring homomorphism from $\phi : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$. Let $\overline{f(x)g(x)}$ be the image of $f(x)g(x)$ in $\mathbb{Z}_p[x] \implies \overline{f(x)g(x)} = \overline{f(x)g(x)}$

Note. In other words, $\overline{f(x)}$ is the polynomial in $\mathbb{Z}[x]$ obtained by reducing the coefficients of $f(x)$ modulo p.

Since $p \,\big|\,$ content of $f(x)g(x) \implies \overline{f(x)g(x)} = 0$ in $\mathbb{Z}_p[x]$
$\implies \overline{f(x)} = 0$ or $\overline{g(x)} = 0$ because $\mathbb{Z}_p[x]$ is an integral domain.
$\implies f(x)$ or $g(x)$ is not primitive. ($\Rightarrow\!\Leftarrow$) $\square$

Theorem 17.2. Let $f(x) \in \mathbb{Z}[x]$. If $f(x)$ is reducible over $\mathbb{Q}$, it is reducible over $\mathbb{Z}$.

Proof. Assume $f(x) = g(x)h(x)$ with $g(x), h(x) \in \mathbb{Q}[x]$. Let a and b be the LCM of denominators of coefficients of $g(x)$ and $h(x)$ respectively. Then $(ab)f(x) = abg(x)h(x) = (ag(x))(bh(x))$. Let c_1 and c_2 be the content of $ag(x)$ and $bh(x)$ respectively. Then $ag(x) = c_1\hat{g}(x)$ and $bh(x) = c_2\hat{h}(x)$ where $\hat{g}(x)$ and $\hat{h}(x)$ are primitive in $\mathbb{Z}[x]$. Let d be the content of f (i.e. $f(x) = d\hat{f}(x)$ where $\hat{f}(x) \in \mathbb{Z}[x]$ is primitive.) Then $(abd)\hat{f}(x) = (c_1c_2)\hat{g}(x)\hat{h}(x) \in \mathbb{Z}[x]$. By Gauss' lemma, $\hat{g}(x)\hat{h}(x)$ is primitive in $\mathbb{Z}[x]$
$\implies abd = c_1c_2 \implies \hat{f}(x) = \hat{g}(x)\hat{h}(x)$
$\implies f(x) = d\hat{f}(x) = (d\hat{g}(x)) \cdot \hat{h}(x)$
$\implies f(x)$ is reducible over $\mathbb{Z}$ (since $d\hat{g}(x), \hat{h}(x) \in \mathbb{Z}[x]$). $\square$

Example 17.5. $f(x) = 6x^2 + x - 2 = \underbrace{(3x - \frac{3}{2})}_{g(x)}\underbrace{(2x + \frac{4}{3})}_{h(x)}$

$d = 1,\ a = 2,\ b = 3,\ c_1 = 3,\ c_2 = 2 \implies f(x) = (2x - 1)(3x + 2)$

FINISH EXAMPLE (NOTES-38)

Theorem 17.3. Let p be prime and $f(x) \in \mathbb{Z}[x]$ such that $\deg f \geq 1$. $\overline{f(x)}$ reducing coeff of $f(x)$ modulo p.

If $\overline{f(x)}$ is irreducible over $\mathbb{Z}_p$ and $\deg \overline{f(x)} = \deg f(x)$, then $f(x)$ is irreducible over $\mathbb{Q}$.

Remark. $f(x) = 21x^3 - 3x^2 + 2x + 9$ work over $\mathbb{Z}_2$

$\overline{f(x)} = x^3 + x^2 + 1$ has no zero in $\mathbb{Z}_2 \implies$ irriducible