date: thursday, march 7, 2024

Irreducible Polynomials

Theme: (Last two classes) $\mathbb{Z}$ and $F[x]$ are similar.

In $\mathbb{Z}$, have a notion of a prime number. Want something similar in $F[x]$.

Note: Any polynomial $p(x) \in F[x]$ can be factored.
$p(x) = x^2 + x + 1 = \frac{1}{c}(cx^2 + cx + c)$, $c \neq 0$

Def$^{\underline{n}}$: A nonconstant polynomial $f(x)$ is irreducible if you cannot write $f(x)$ as $f(x) = g(x)h(x)$ with $0 < \deg g(x) < \deg f(x)$ and $0 < \deg h(x) < \deg f(x)$. Otherwise, $f(x)$ is reducible.

IMPORTANT: Irreducibility depends upon field F.
- $x^2 - 2$ is irreducible in $\mathbb{Q}[x]$
- $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$ is reducible in $\mathbb{R}[x]$

Fact: If $f(x)$ has degree >1 and $f(x)$ has a root $\alpha \in F$, then $f(x)$ is reducible.

Proof: Since $f(\alpha) = 0 \Rightarrow f(x) = (x - \alpha)g(x)$. Since $\deg f(x) > 1$, this means $\deg g(x) \geq 1$.

eg. Show $p(x) = x^3 + x^2 + 2$ is irreducible in $\mathbb{Z}_3[x]$.
If $p(x)$ was reducible, then $p(x) = q(x)r(x)$ and one of $q(x)$ has degree 1 and the other degree 2.
Say $\deg q(x) = 1 + r(x)$, then $q(x) = ax + b$, $a, b \in \mathbb{Z}_3$.
So $p(x)$ has a root in $\mathbb{Z}_3$.
But, $p(0) = 2 \neq 0$
$p(1) = 4 = 1 \neq 0$
$p(2) = 14 = 2 \neq 0$
So $p(x)$ has no root, so irreducible.

Theorem: ① $f(x) \in \mathbb{C}[x]$ is irreducible iff $f(x) = (x-\alpha)$ (Fundamental Theorem of Algebra)

② $f(x) \in \mathbb{R}[x]$ is irreducible iff $f(x) = (x-\alpha)$ and $f(x) = ax^2 + bx + c$ with $b^2 - 4ac < 0$.

Factorization of $\mathbb{Q}[x]$

Reduction to polynomials over $\mathbb{Z}[x]$.

Lemma: Consider $p(x) \in \mathbb{Q}[x]$. There exists $r, s, a_0, \dots, a_n \in \mathbb{Z}$ with $\gcd(r,s) = 1$ and $\gcd(a_0, \dots, a_n) = 1$ such that

$$p(x) = \frac{r}{s}(a_n x^n + \cdots + a_1 x + a_0)$$

eg. $p(x) = \frac{3}{5} + \frac{2}{3}x + \frac{3}{10}x^2$

$$= \frac{1}{5 \cdot 3 \cdot 10}\left[3 \cdot 10 \cdot 3 + 5 \cdot 10 \cdot 2x + 5 \cdot 3 \cdot 3x^2\right]$$

$$= \frac{5}{5 \cdot 3 \cdot 10}\left[3 \cdot 2 \cdot 3 + 10 \cdot 2x + 3 \cdot 3x^2\right]$$

$$= \frac{1}{30}\left[18 + 20x + 9x^2\right]$$

(Gauss' Lemma) Let $p(x)$ be a polynomial of $\mathbb{Z}[x]$ such that $p(x) = \alpha(x)\beta(x)$ with $\alpha(x), \beta(x) \in \mathbb{C}[x]$. Then $p(x) = a(x)b(x)$ with $a(x), b(x) \in \mathbb{Z}[x]$ with $\deg \alpha(x) = \deg a(x)$ and $\deg \beta(x) = \deg b(x)$.

Note: The text requires $p(x)$ monic but you don't need this.

Corollary: Let $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ with $a_i \in \mathbb{Z}$ and $a_0 \neq 0$. If $p(x)$ has a root $\frac{r}{s} \in \mathbb{Q}$, then it has a root $\alpha \in \mathbb{Z}$ and $\alpha \mid a_0$.

<u>Proof</u>

Suppose $p(\frac{r}{s}) = 0$. So $p(x) = (x - \frac{r}{s})q(x)$ with $(x - \frac{r}{s}), q(x) \in \mathbb{Q}[x]$. By Gauss' Lemma, exists $(x-\alpha), q'(x) \in \mathbb{Z}[x]$ such that $p(x) = (x-\alpha)(q'(x))$. Thus, α is a root of $p(x)$ and $\alpha \in \mathbb{Z}$. If we

Write

$$q(x) = b_{n-1}x^{n-1} + \cdots + b_1 x + b_0$$

we have

$$p(x) = x^n + \cdots + a_1 x + a_0 = (x-\alpha)(b_{n-1}x^{n-1} + \cdots + b_0) = \cdots + \alpha b_0.$$

So $a_0 = \alpha b_0 \Rightarrow \alpha \mid a_0$.

$\square$

eg. Show $x^3 - 7x^2 + 5$ has no roots in $\mathbb{Q}$.
If it did have a root, it would have an integer root α.
Then $\alpha \mid 5$. So $\alpha = \pm 1$ or ± 5.
But $(1)^3 - 7(1) + 5 \neq 0$ $\quad 5^3 - 7(5)^2 + 5 \neq 0$
$(-1)^3 - 7(-1) + 5 \neq 0$ $\quad (-5)^3 - 7(-5)^2 + 5 \neq 0$.

(Eisenstein's Criterion) Let $p(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$. Suppose there is a prime p such that

- $p \mid a_0, a_1, \ldots, a_{n-1}$
- $p \nmid a_n$
- $p^2 \nmid a_0$

Then $p(x)$ is irreducible.

<u>Proof</u>

By Gauss' Lemma, if $p(x)$ was reducible,

$$p(x) = (b_r x^r + \cdots + b_0)(c_s x^s + \cdots + c_0) \in \mathbb{Z}[x].$$

Since $p^2 \nmid a_0 = b_0 c_0$ but $p \mid a_0$, p does not divide one of them. Say $p \nmid b_0$ but $p \mid c_0$. Since $a_n = b_r c_s$ and $p \nmid a_n$, $p \nmid b_r$ and $p \nmid c_s$. Let k be the smallest integer such that $p \nmid c_k$. (Note we have $c_0, c_1, \ldots, c_s$ where $p \mid c_0$ and $p \nmid c_s$).
Then,

$$a_k = b_0 c_k + b_1 c_{k-1} + \cdots + b_k c_0 \iff b_0 c_k = a_k - b_1 c_{k-1} - \cdots - b_k c_0.$$

If $k < n$, then p divides right hand side but not left. So $k = n$. This implies $\deg(c_s x + \cdots + c_0) \geq n$, a contradiction. Thus, $p(x)$ is irreducible.

$\square$

eg. $x^n - 2024$ is irreducible over $\mathbb{Q}[x]$ for all $n \geq 2$.
Let $p = 23$. Then $p \mid 2024$, $p^2 \nmid 2024$, $p \nmid 1$.
So by Eisenstein's Criterion, $x^n - 2024$ is irreducible.