Factorization Techniques

<u>Goal</u>: Factor (or check for factors) of polynomials

e.g. $x^7 - 7x^2 - 2x + 1$

$x^4 + 3x^3 - 27x^2 + 9x + 6$

<u>Prop</u>: Let F be a field, $p(X) \in F[X]$

Then $p(X)$ has a factor of degree one in $F[X]$

iff $p(X)$ has a <u>root</u> in F, i.e. $\exists\, \alpha \in F$ s.t. $p(\alpha) = 0$

<u>Pf</u>: If $p(X)$ has a factor of degree one in $F[X]$

i.e. $p(X) = (\alpha X - \beta) \cdot q(X)$, $\alpha, \beta \in F$, $\alpha \neq 0$

$$\Longrightarrow \quad p\left(\frac{\beta}{\alpha}\right) = \left(\alpha \cdot \left(\frac{\beta}{\alpha}\right) - \beta\right) \cdot q\left(\frac{\beta}{\alpha}\right)$$

$$= 0 \cdot q\left(\frac{\beta}{\alpha}\right) = 0$$

Conversely, if $p(X)$ has a root $\alpha \in F$

Then we can write $p(X) = q(X) \cdot (X - \alpha) + r(X)$

where $r(X) = 0$ or $\deg r(X) < \deg(X - \alpha) = 1$

(i.e. $r(X) \equiv r$ is a constant)

$$p(\alpha) = q(\alpha) \cdot (\alpha - \alpha) + r$$
$$0 = 0 + r$$

$$\Longrightarrow \quad r = 0 \quad \text{and} \quad p(X) = q(X) \cdot \underbrace{(X - \alpha)}_{\text{degree one factor}}$$

$\square$

<u>Cor</u>: If $p(X) \in F[X]$ has roots $\alpha_1, \alpha_2, \dots, \alpha_k$

(not necessarily distinct roots)

Then $p(X)$ has $(X-\alpha_1)\cdot(X-\alpha_2)\cdot\dots\cdot(X-\alpha_k)$

as a factor

<u>Defn</u>: If $p(X) \in F[X]$ is divisible by $(X-\alpha)^k$

Then we say that the root α has <u>multiplicity</u> k.

<u>Cor</u>: If $\deg(p(x)) = n$

Then it has at most n roots in F

(even counting with multiplicity).

<u>Cor</u>: If $p(X) \in F[X]$ and $\deg p = 2$ or 3

Then $p(X)$ is reducible iff p has a root in F

<u>Prop</u>: Let $p(X) = a_0 + a_1 X + a_2 X^2 + \_\_\_ + a_n X^n \in \mathbb{Z}[X]$

If $\frac{r}{s} \in \mathbb{Q}$ is in lowest terms (i.e. $\gcd(r,s)=1$)

and $p(\frac{r}{s}) = 0$

Then $r \mid a_0$, $s \mid a_n$

In particular, if $a_n = 1$ (i.e. p is monic)

and $p(d) \neq 0$ $\forall d \in \mathbb{Z}$ s.t. $d \mid a_0$

Then $p(X)$ has no roots in $\mathbb{Q}$

Example: $p(x) = x^7 - 7x^2 - 2x + 1$

Check: $x = \pm 1$ $\quad p(1) = 1^7 - 7\cdot 1^2 - 2\cdot 1 + 1 = -7 \neq 0$

$p(-1) = (-1)^7 - 7(-1)^2 - 2(-1) + 1 = -5 \neq 0$

$\Longrightarrow$ If $p(x)$ has any real roots, they are irrational.

Pf: $p\left(\frac{r}{s}\right) = a_0 + a_1\cdot\left(\frac{r}{s}\right) + a_2\left(\frac{r}{s}\right)^2 + \_\_\_ + a_n\left(\frac{r}{s}\right)^n$

$\overset{\|}{0}$

$\Longrightarrow \quad 0 = a_0\cdot s^n + a_1\cdot r\cdot s^{n-1} + a_2\cdot r^2\cdot s^{n-2} + \dots + a_n r^n.$

$\Longrightarrow$ (1) $a_n\cdot r^n = -a_0 s^n - a_1 r\cdot s^{n-1} - \dots - a_{n-1} r^{n-1}\cdot s$

$= -s\cdot(a_0 s^{n-1} - a_1 r s^{n-2} - \dots - a_{n-1} r^{n-1})$

$\gcd(r,s) = 0 \Longrightarrow s \mid a_n$

(2) $a_0 s^n = -a_1 r\cdot s^{n-1} - a_2 r^2 s^{n-2} - \dots - a_n r^n$

$= -r\cdot(a_1\cdot s^{n-1} - a_2 r\cdot s^{n-2} - \dots - a_n r^{n-1})$

$\gcd(r,s) \Longrightarrow r \mid a_0$

$\square$

Example: (1) $x^3 + 9x^2 - 2x + 1$

Check: $p(1) = 1^3 + 9\cdot 1^2 - 2\cdot 1 + 1 = 9 \neq 0$

$p(-1) = (-1)^3 + 9(-1)^2 - 2(-1) + 1 = 11 \neq 0$

$\Longrightarrow$ $x^3 + 9x^2 - 2x + 1$ has no roots in $\mathbb{Q}$

$\Longrightarrow$ $x^3 + 9x^2 - 2x + 1$ is irreducible over $\mathbb{Q}$.

(2) $x^2 - p$, $x^3 - p$, $p \in \mathbb{Z}$ is prime.

Claim: These are irreducible over $\mathbb{Q}[x]$

Pf: Only candidates for solutions are

$$\pm 1, \pm p$$

$$(1)^2 - p = (-1)^2 - p = 1 - p \neq 0$$

$$(p)^2 - p = (-p)^2 - p = p \cdot (p-1) \neq 0$$

(Similar for $x^3 - p$) $\square$

(3) $x^2 + 1$ irreducible over $\mathbb{R}[x]$

Check: $1^2 + 1 = 2 \neq 0$
$(-1)^2 + 1 = 2$

On the other hand

$x^2 + 1$ is reducible over $(\mathbb{Z}/2\mathbb{Z})[X]$

Check: $1^2 + 1 \equiv 0 \mod 2$

$x^2 + X + 1$ is irreducible over $(\mathbb{Z}/2\mathbb{Z})[X]$

Check: $0^2 + 0 + 1 = 1 \neq 0$
$1^2 + 1 + 1 = 1 \neq 0$

Prop: Let R be an integral domain, $I \subsetneq R$ a proper ideal. $p(X) \in R[X]$ non-constant, monic.

If $\overline{p(X)} \in (R/I)[X]$ is irreducible into polynomials of strictly lesser degree

Then $p(X)$ is irreducible in $R[X]$.

Pf: Suppose $p(X)$ is reducible in $R[X]$

Say $p(X) = a(X) \cdot b(X)$, $\deg a, \deg b < \deg p$.

Because p monic $\Longrightarrow$ can choose a, b to be monic, non-constant.

$$\overline{p(X)} = \overline{a(X)} \cdot \overline{b(X)} \in (R/I)[X]$$

$\lightning$

Examples: • X^2+X+1 irreducible in $(\mathbb{Z}/2\mathbb{Z})[X]$

$\Longrightarrow$ X^2+X+1 irreducible in $\mathbb{Z}[X]$

• X^2+1 is irreducible in $\mathbb{Z}[X]$ but reducible in $(\mathbb{Z}/2\mathbb{Z})[X]$

$\Longrightarrow$ The prop. cannot be "if and only if"

WARNING: $\exists$ polynomials, e.g. X^4+1 that are irreducible in $\mathbb{Z}[X]$ but reducible in every $(\mathbb{Z}/p\mathbb{Z})[X]$

Example: $X^2+XY+1 \in \mathbb{Z}[X,Y] = (\mathbb{Z}[X])[Y]$

$$\mathbb{Z}[X,Y]/_{Y\cdot\mathbb{Z}[X,Y]} \cong \mathbb{Z}[X]$$

$$\overline{X^2+XY+1} \in \mathbb{Z}[X,Y]/_{Y\cdot\mathbb{Z}[X,Y]}$$
$$\parallel$$
$$X^2+1 \longleftarrow \text{irreducible}$$

$\Longrightarrow$ X^2+XY+1 is reducible in $\mathbb{Z}[X,Y]$

Eisenstein's Criterion:

Let R be an int. dom.

$P \subset R$ a prime ideal.

$$q(X) = X^n + c_{n-1}X^{n-1} + \dots + c_1 X + c_0 \in R[X]$$

Suppose $c_0, c_1, \dots, c_{n-1} \in P$ and $c_0 \notin P^2$

Then $q(X)$ is irreducible in $R[X]$.

Example: $p(X) = X^4 + 3X^3 - 27X^2 + 9X + 6$

Claim: $p(X)$ is irreducible

Pf: $3, -27, 9, 6 \in 3\mathbb{Z}$, $\quad 6 \notin 9\mathbb{Z}$

$\square$

Pf: of Eisensteins Criterion

Suppose $q(X) = a(X) \cdot b(X)$, $a, b \in R[X]^{\times}$

Because q is monic, we may take a, b to be monic.

$$a(X) = X^k + a_{k-1} X^{k-1} + \dots + a_1 X + a_0$$
$$b(X) = X^\ell + b_{\ell-1} X^{\ell-1} + \dots b_1 X + b_0$$

$\implies \ell, k > 0$

If $c_0, c_1, \dots, c_{n-1} \in P$

$$\implies \overline{q(X)} = \overline{X^n + c_{n-1} X^{n-1} + \dots + c_0} = \overline{X}^n \in (R/p)[X]$$
$$= \overline{a(X)} \cdot \overline{b(X)}$$

i.e. $\overline{a(X)} \cdot \overline{b(X)} = \overline{X}^n$

$\implies \overline{a_0} \cdot \overline{b_0} = \overline{0} \implies a_0 \in P$ or $b_0 \in P$

wlog $a_0 \in P$

$$(X^k + a_{k-1} X^{k-1} + \_\_ + a_0)(X^\ell + b_{\ell-1} X^{\ell-1} + \_\_ + b_0)$$
$$= X^{k+\ell} + (a_{k-1} + b_{\ell-1}) \cdot X^{k+\ell-1} + \dots + (a_1 \cdot b_0 + a_0 \cdot b_1) X + a_0 \cdot b_0$$

$\implies a_0 \cdot b_1 \in P \implies a_1 \cdot b_0 \in P$

$\implies a_1 \in P$ or $b_0 \in P$ If $a_1 \in P$

$$(a_2 \cdot b_0 + \underbrace{a_1 \cdot b_1}_{\in P} + \underbrace{a_0 b_2}_{\in P}) \in P \implies a_2 \cdot b_0 \in P$$

$\implies a_2 \in P$ or $b_0 \in P$

$\dots \implies b_0 \in P \implies a_0 b_0 = c_0 \in P^2$ $\square$

Examples

(1) $X^n - p$ is irreducible if p is prime.

b/c $-p \in p\cdot\mathbb{Z}$ but $-p \notin p^2\cdot\mathbb{Z}$

Cor: $\sqrt[n]{p} \notin \mathbb{Q}$ $\forall n \geq 2$.

(2) $p(X) = X^4 + 1$

$1 \notin P$ not in any prime ideal.

Can't apply Eisenstein's Criterion directly.

Consider $q(X) = p(X+1) = (X+1)^4 + 1$

$$= (X^4 + 4X^3 + 6X^2 + 4X + 1) + 1$$

$$= X^4 + 4X^3 + 6X^2 + 4X + 2$$

$2, 4, 6 \in 2\mathbb{Z}$ but $2 \notin 4\mathbb{Z}$

Apply Eisenstein's Criterion to $q(X)$

Suppose $X^4 + 1 = a(X)\cdot b(X)$

Then $q(X) = (X+1)^4 + 1 = a(X+1)\cdot b(X+1)$

i.e. if X^4+1 is reducible then so is $q(X)$

Eisenstein $\Rightarrow$ $q(X)$ irred. $\Rightarrow$ X^4+1 irred.