L14: Factorization Techniques

The goal of this lecture is to factor (or check for factors) of polynomials

Proposition 14.1

Let F be a field and $p(X) \in F[X]$ a polynomial.
$p(X)$ has a factor of degree one in $F[X]$ *iff* $p(X)$ has a root in F, i.e $\exists \alpha \in F$, $p(\alpha) = 0$.

Proof.

$\Longrightarrow$

If $p(X)$ has a factor of degree one in $F[X]$ i.e $p(X) = (\alpha X - \beta) \cdot q(X)$, $\alpha, \beta \in F$ with $\alpha \neq 0$ Then

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

$\Longleftarrow$

Conversely, if $p(X)$ has a root $\alpha \in F$, then we can write

$$p(X) = q(X) \cdot (X - a) + r(X)$$

where $r(X) = 0$ or $\deg r(X) < \deg(X - \alpha) = 1$ (i.e $r(X) \equiv r$ is a constant). Then, by substituting α we see

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

and therefore $p(X) = q(X) \cdot (X - \alpha)$ where $(X - \alpha)$ is degree one factor we are looking for. ■

Corollary 14.2

If $p(X) \in F[X]$ has (not necessarily distinct) roots $\alpha_1, \alpha_2, \dots, \alpha_k$, then $p(X)$ has

$$(X - \alpha_1) \cdot (X - \alpha_2) \cdot \ldots \cdot (X - \alpha_2)$$

as a factor

Definition 14.3: Multiplicity

If $p(X) \in F[X]$ is divisible by $(X - \alpha)^k$, then we say that the root α has **multiplicity** k.

Corollary 14.4

If $\deg(p(X)) = n$, then it has at most n roots in F (even counting with multiplicity).

Corollary 14.5

If $p(X) \in F[X]$ and $\deg p = 2$ or 3, then $p(X)$ is reducible *iff* p has a root in F.

Proposition 14.6

Let

$$p(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n \in \mathbb{Z}[X]$$

If $\frac{r}{s} \in \mathbb{Q}$ is in lowest terms (i.e $\gcd(r,s) = 1$) and $p\left(\frac{r}{s}\right) = 0$, then $r|a_0$ and $s|a_1$.
In particular, if $a_n = 1$ (i.e p is monic) and $p(d) \neq 0$ for all $d \in \mathbb{Z}$ such that $d|a_0$, then $p(X)$ has no roots in $\mathbb{Q}$.

Example 14.1. Let $p(X) = X^7 - 7X^2 - 2X + 1$. Then check if $X = \pm 1$ are roots of $p(X)$:

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

Since neither are equal to 0, then if $p(X)$ has any real roots, they are irrational.

Proof. Let $\alpha = \frac{r}{s}$ be a root of a polynomial $p(X) \in \mathbb{Z}[X]$. Then one writes

$$p\left(\frac{r}{s}\right) = a_0 + a_1 \bullet \left(\frac{r}{s}\right) + a_2 \bullet \left(\frac{r}{s}\right)^2 + \cdots + a_n\left(\frac{r}{s}\right)^n$$
$$\Longrightarrow 0 = a_0 \bullet s^n + a_1 \bullet r \bullet s^{n-1} + a_2 \bullet r^2 \bullet s^{n-2} + \cdots + a_n \bullet r^n$$

First isolating r, we get

$$\begin{aligned} a_n \bullet r^n &= -a_0 \bullet s^n - a_1 \bullet r \bullet s^{n-1} - \cdots - a_{n-1} \bullet r^{n-1} \bullet s \\ &= -s \bullet \left(a_0 \bullet s^{n-1} - a_1 \bullet r \bullet s^{n-2} - \cdots - a_{n-1} \bullet r^{n-1}\right) \end{aligned}$$

Since $\gcd(r,s) = 1$ then it can only be that $s|a_n$.
Similarly, isolating s, we get

$$\begin{aligned} a_0 \bullet s^n &= -a_1 \bullet r \bullet s^{n-1} - a_2 \bullet r^2 \bullet s^{n-2} - \cdots - a_n \bullet r^n \\ &= -r \bullet \left(a_1 \bullet s^{n-1} - a_2 \bullet r \bullet s^{n-2} - \cdots - a_n \bullet r^{n-1}\right) \end{aligned}$$

Since $\gcd(r,s) = 1$ then it can only be that $r|a_0$. ■

Example 14.2. Consider $p(X) = X^3 + 9X^2 - 2X + 1$ with possible roots $X = \pm 1$. We check

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

Hence, $p(X)$ has no roots in $\mathbb{Q}$ and is thus **irreducible** over $\mathbb{Q}$.

Claim: The polynomials $X^2 - p, X^3 - p \in \mathbb{Z}[X]$ where $p \in \mathbb{Z}$ is prime are irreducible over $\mathbb{Q}[X]$.

Proof. The only candidates for soluutions are $X = \pm 1, \pm p$. We check for $q(X) = X^2 - P$:

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

The proof for $X^3 - p$ is similar (you should check it yourself). ■

Example 14.3. Consider $p(X) = X^2 + 1$. This is irreducible over $\mathbb{R}[X]$ as one can check

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

On the other hand, it **is** reducible over $\mathbb{Z}/2\mathbb{Z}[X]$

$$1^2 + 1 \equiv 0 \pmod{2}$$

Finally $X^2 + X + 1$ is irreducible over $\mathbb{Z}/2\mathbb{Z}[X]$ as

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

Proposition 14.7

Let R be an integral domain and $I \subsetneq R$ a proper ideal. Let $p(X) \in R[X]$ be a non-constant, monic polynomial.
If $\overline{p(X)} \in (R/I)[X]$ is irreducible into polynomials of strictly lesser degree, then $p(X)$ is irreducible in $R[X]$.

Proof. Suppose $p(X)$, a non-constant monic polynomial, is reducible in $R[X]$, say

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

Since p is monic then can also choose a, b to be non-constant, monic polynomials, hence

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

Example 14.4.

- $p(X) = X^2 + X + 1$ is irreducible in $\mathbb{Z}/2\mathbb{Z}[X]$ then it is irreducible in $\mathbb{Z}[X]$
- $p(X) = X^2 + 1$ is irreducible in $\mathbb{Z}[X]$ but **is** reducible in $(\mathbb{Z}/2\mathbb{Z})[X]$

The second example shows the proposition cannot be an "if and only if" statement.

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

Example 14.5. Let $p(X, Y) \in \mathbb{Z}[X, Y] = (\mathbb{Z}[X])[Y]$, then

$$\mathbb{Z}[X, Y]/(y \cdot \mathbb{Z}[X, Y]) \cong \mathbb{Z}[X]$$

Specifically, $\overline{X^2 + XY + 1} \in \mathbb{Z}[X, Y]/(y \cdot \mathbb{Z}[X, Y])$. Since $X^2 + 1$ is an element of the coset $\overline{X^2 + XY + 1}$ and it is irreducible, then $X^2 + XY + 1$ is irreducible in $\mathbb{Z}[X, Y]$.

Theorem 14.8: Eisenstein's Criterion

Let R be an integral domain and $P \subset R$ a prime ideal. Furthermore,

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

Suppose $c_0, c_1, \ldots, c_{n-1} \in P$ and $c_0 \notin P^2$, then $q(X)$ is irreducible in $R[X]$.

<u>**Claim:**</u> $p(X) = X^4 + 3x^3 - 27X^2 + 9X + 6$ is irreduicble

Proof. $3, -27, 9, 6 \in 3\mathbb{Z}$ however $6 \notin 9\mathbb{Z}$. ■

Proof of Eisenstein's Criterion. Suppose $q(X) = a(X) \cdot b(X)$ where $a, b \in R[X]^\times$. Since q is monic, we may take a, b to be monic

$$\begin{aligned} a(X) =& X^k + a_{k-1}X^{k-1} + \cdots + a_1 X + a_0 \\ b(X) =& X^l + b_{l-1}X^{l-1} + \cdots + b_1 X + b_0 \end{aligned}$$

where $l, k > 0$.
If $c_0, c_1, \ldots, c_{n-1} \in P$, then

$$\begin{aligned} \overline{q(X)} =& \overline{X^n + c_{n-1}X^{n-1} + \cdots + c_0} = \overline{X^n} \in (R/P)[X] \\ =& \overline{a(X)} \cdot \overline{b(X)} \end{aligned}$$

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

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

W.l.o.g let $a_0 \in P$, then $a(X) \cdot b(X)$ can be written

$$\begin{aligned} &(X^k + a_{k-1}X^{k-1} + \cdots + a_1 X + a_0) \cdot (X^l + b_{l-1}X^{l-1} + \cdots + b_1 X + b_0) \\ =& X^{k+l} + (a_{k-1} + b_{l-1})X^{k+l-1} + \cdots + (a_1 \cdot b_0 + a_0 \cdot b_1)X + a_0 \cdot b_0 \end{aligned}$$

Therefore $a_0 \cdot b_1, a_1 \cdot b_0 \in P$ implying $a_1 \in P$ or $b_0 \in P$.
If $a_1 \in P$ then

$$(a_2 \cdot b_0 + \underbrace{a_1 \cdot b_1}_{\in P} + \underbrace{a_0 \cdot b_2}_{\in P}) \implies a_2 \cdot b_0 \in P \implies a_2 \in P \text{ or } b_0 \in P \implies a_0 \cdot b_0 = c_0 \in P^2$$

■

Example 14.6. $X^n - p$ is irreducible if p is prime because $-p \in p \cdot \mathbb{Z}$ but $-p \notin p^2 \cdot \mathbb{Z}$.

Corollary 14.9

$\sqrt[n]{p} \notin \mathbb{Q}$ for all $n \geq 2$.

Example 14.7. Let $p(X) = X^4 + 1$ and notice that $1 \notin P$ for any prime ideal (otherwise its the whole ring and not a prime ideal), therefore we can't apply Eisenstein's Criterion directly.

Consider

$$\begin{aligned} q(X) =& p(X+1) = (X+1)^4 + 1 \\ =& (X^4 + 4X^3 + 6X^2 + 4X + 1) + 1 \\ =& X^4 + 4X^3 + 6X^2 + 4X + 2 \end{aligned}$$

See that $2, 4, 6 \in 2\mathbb{Z}$ but $2 \notin 4\mathbb{Z}$, therefore we can 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 $q(X)$.
But by Eisenstein's Criterion $q(X)$ is irreducible, therefore $X^4 + 1$ is too.