MA542 Lecture

Timothy Kohl

Boston University

February 7, 2025

More on Roots and Linear Factors

We saw this consequence of the Division Algorithm.

Corollary

Let $f(x) \in F[x]$ then $a \in F$ is a zero of $f(x)$ if and only if $x - a$ is a factor of $f(x)$.

This leads to another well-known fact we're familiar with.

Corollary

A polynomial of degree n over a field has at most n zeros counting multiplicity.

Proof.

(Induction on n) If $f(x)$ is constant then $f(x)$ has no zeros unless $f(x) = 0$.

Otherwise, let a be a zero of a multiplicity k in F i.e. $f(x)$ is divisible by $(x-a)^k$ but **not** $(x-a)^{k+1}$ so $f(x) = q(x)(x-a)^k$ where $q(a) \neq 0$.

Since $deg(f(x) = k + deg(q(x))$ where $deg(q(x)) = n - k$ where $k \leq n$.

If $f(x)$ has no other zeros we're done, otherwise let b be a different zero of $f(x)$ then $f(b) = 0 = (b-a)^k q(b)$ which implies $q(b) = 0$ since $(b-a) \neq 0$.

So any other root of $f(x)$ is a root of a degree $n-k$ polynomial $q(x)$ so inductively $q(x)$ has at most $n-k$ roots which means that $f(x)$ has at most $k + (n-k) = n$ roots. □

Now zeros $a \in F$ of $f(x) \in F[x]$ correspond to factors of the form $(x-a)^n$ but we may consider factorization more generally.

Definition

A non-constant polynomial $f(x) \in F[x]$ is irreducible over F if $f(x)$ cannot be expressed as a product of two lower degree polynomials.
If $f(x)$ is not irreducible it is reducible.

For example, $x^2 - 2 \in \mathbb{Q}[x]$ is irreducible over $\mathbb{Q}$ and $x^2 + 5x + 6$ is reducible over $\mathbb{Q}$ since $x^2 + 5x + 6 = (x+2)(x+3)$.

Note, if we view $x^2 - 2 \in \mathbb{R}[x]$ then the situation is different since then $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$ since $x \pm \sqrt{2} \in \mathbb{R}[x]$ (but not in $\mathbb{Q}[x]$ of course.)

For low degree polynomials in $F[x]$ we have:

Proposition

Let $f(x) \in F[x]$ for F a field where $deg(f(x)) = 2$ or 3, then $f(x)$ is reducible if and only if $f(x)$ has a zero in F.

Proof.

Say $f(x) = g(x)h(x)$ where $deg(g(x)) < deg(f(x))$ and $deg(h(x)) < deg(f(x))$ then without loss of generality we may assume $deg(g(x)) = 1$ and $deg(h(x)) = 1$ or 2.

So $g(x) = ax + b$ where $-a^{-1}b$ is therefore a zero of $g(x)$ and therefore of $f(x)$ too.

Conversely, if $f(c) = 0$ for some $c \in F$ then $x - c$ is a divisor of $f(x)$ and we have $f(x) = (x - a)h(x)$ where, since $deg(x - c) = 1$ means $deg(h(x)) = 1$ or 2. □

Now if $f(x) \in \mathbb{Z}[x]$ then we may view $f(x)$ as an element of $\mathbb{Q}[x]$ and if $f(x) = g(x)h(x)$ for $g(x), h(x) \in \mathbb{Q}[x]$ of lower degree, then can we show that $f(x)$ is factorable as a product of polynomials in $\mathbb{Z}[x]$?

The answer, surprisingly, is yes, but we need to establish some technical facts.

Definition

The <u>content</u> of a polynomial
$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ is
$c(f(x)) = gcd(a_n, a_{n-1}, \ldots, a_1, a_0)$ the greatest common divisor of the coefficients.
A polynomial $f(x) \in \mathbb{Z}[x]$ if <u>primitive</u> if $c(f(x)) = 1$.

e.g. $c(3x^2 + 12x + 6) = 3$, $c(x^2 + 2x + 3) = 1$.

Lemma (Gauss' Lemma)

The product of two primitive polynomials is primitive.

PROOF: Given $f(x) \in \mathbb{Z}[x]$ and a prime p, if one reduces the coefficients mod p then one gets a polynomial $\bar{f}(x) \in \mathbb{Z}_p[x]$, which is important since $\mathbb{Z}_p$ is a field.

Moreover, it's easy to show that for $f(x), g(x) \in \mathbb{Z}[x]$ that if $h(x) = f(x)g(x)$ then $\bar{h}(x) = \bar{f}(x)\bar{g}(x)$.

Now if $c(f)$ is the content of f and $c(g)$ is the content of g then assume $c(f) = 1$ and $c(g) = 1$ and suppose $c(fg) \neq 1$.

As such there is some prime p that divides the coefficients of $h = fg$ and so $\bar{h} = 0$ in $\mathbb{Z}_p[x]$.

PROOF: (continued)
However $\overline{h} = \overline{f}\,\overline{g}$ where $\overline{f}, \overline{g} \in \mathbb{Z}_p[x]$ which (since $\mathbb{Z}_p[x]$ is a domain) means that either $\overline{f} = 0$ or $\overline{g} = 0$ in $\mathbb{Z}_p[x]$.

If say $\overline{f} = 0$ in $\mathbb{Z}_p[x]$ then every coefficient $f \in \mathbb{Z}[x]$ must be divisible by p which contradicts the assumption that $c(f) = 1$.

As such $c(f) = 1$ and $c(g) = 1$ implies $c(fg) = 1$. $\square$

We can now prove that for an integer polynomial, being reducible over $\mathbb{Q}$ implies reducibility over $\mathbb{Z}$.

Theorem

Let $f(x) \in \mathbb{Z}[x]$ if $f(x)$ is reducible over $\mathbb{Q}$ then it is reducible over $\mathbb{Z}$.

PROOF: Let $f(x) = g(x)h(x)$ for $g(x), h(x) \in \mathbb{Q}[x]$. We may assume that $f(x)$ is primitive since otherwise we could divide $f(x)$ and $g(x)$ by $c(f(x))$.

Let

$$a = lcm(\text{denominators of coefficients of } g(x))$$
$$b = lcm(\text{denominators of coefficients of } h(x))$$

then $abf(x) = (ag(x))(bh(x))$ where now $ag(x) \in \mathbb{Z}[x]$ and $bh(x) \in \mathbb{Z}[x]$.

Let $c_1 = c(ag(x))$ and $c_2 = c(bh(x))$ so $ag(x) = c_1 g_1(x)$ for some $g_1(x) \in \mathbb{Z}[x]$ with $c(g_1(x)) = 1$ and similarly $bh(x) = c_2 h_2(x)$ for $h_2(x) \in \mathbb{Z}[x]$ where $c(h_2(x)) = 1$.

Thus

$$abf(x) = c_1 c_2 g_1(x) h_1(x) \text{ *}$$

but we have $c(abf(x)) = ab$ and $c(c_1 c_2 g_1(x) h_2(x)) = c_1 c_2$ but then (*) above implies that $f(x) = g_1(x) h_1(x)$ where $g_1(x)$ and $h_1(x)$ are polynomials in $\mathbb{Z}[x]$. $\square$

As a consequence, we have:

Corollary

If $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ with $a_0 \neq 0$ and if $f(x)$ has a zero in $m \in \mathbb{Q}$ then we may assume $m \in \mathbb{Z}$ where $m | a_0$.

Proof.

If $f(x)$ has a zero $a \in \mathbb{Q}$ then $f(x)$ has a linear factor $x - a \in \mathbb{Q}[x]$.

But then the previous theorem implies that $f(x)$ has a factorization with a linear factor in $\mathbb{Z}[x]$.

ergo $f(x) = (x - m)(x^{n-1} + \cdots - \frac{a_0}{m})$ where $(x - m) \in \mathbb{Z}[x]$ and also $(x^{n-1} + \cdots - \frac{a_0}{m}) \in \mathbb{Z}[x]$ as well.

But this means $\frac{a_0}{m} \in \mathbb{Z}$ so m divides a_0. $\square$

Mod p Irreducibility

In Gauss' Lemma we used the fact that $\rho : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ given by $\rho(f) = \overline{f}$ is a homomorphism.

We can use this idea further.

Theorem (mod p irreducibility)

Let p be a prime and suppose that $f(x) \in \mathbb{Z}[x]$ where $deg(f(x)) \geq 1$, let $\overline{f}(x) \in \mathbb{Z}_p[x]$.

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

PROOF: If $f(x)$ is reducible over $\mathbb{Q}$ then its reducible over $\mathbb{Z}$ so $f(x) = g(x)h(x)$ where $deg(g(x)) < deg(f(x))$ and $deg(h(x)) < deg(f(x))$.

Now suppose $\bar{f}(x)$ is irreducible over $\mathbb{Z}_p[X]$ then since $\bar{f}(x) = \bar{g}(x)\bar{h}(x)$ where $deg(\bar{f}(x)) = deg(f(x))$ then

$$deg(\bar{g}(x)) \leq deg(g(x))$$
$$deg(\bar{h}(x)) \leq deg(h(x))$$

but $deg(\bar{f}(x)) = deg(\bar{g}(x)) + deg(\bar{h}(x))$ and $deg(\bar{f}(x)) = deg(f(x)) = deg(g(x)) + deg(h(x))$ so $deg(\bar{g}(x)) = deg(g(x))$ and $deg(\bar{h}(x)) = deg(h(x))$ so $\bar{f}(x)$ is reducible in fact. (contradiction)

Example: $f(x) = x^3 + 3x + 2 \in \mathbb{Z}[x]$ is irreducible.

Let $p = 5$ and consider $\bar{f}(x) = x^3 + 3x + 2 \in \mathbb{Z}_5[x]$.

If $\bar{f}(x)$ is reducible in $\mathbb{Z}_5[x]$ it must be that it has a root in $\mathbb{Z}_5$ since it is degree 3.

However, one can verify that for no $a \in \mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ do we have $\bar{f}(a) = 0$.

So $\bar{f}(x)$ is irreducible in $\mathbb{Z}_5[x]$ and has the same degree so it must be irreducible over $\mathbb{Z}$ and hence over $\mathbb{Q}$!

Note, the converse is **false** since, for example, if $f(x) = x^3 + 3x + 2$ then in $\mathbb{Z}_3[x]$ we have $\bar{f}(x) = x^3 + 2$ and for $1 \in \mathbb{Z}_3$ we have $\bar{f}(1) = 0$ so that, in $\mathbb{Z}_3[x]$, $x - 1 \mid \bar{f}(x)$.

That is, it's reducible in $\mathbb{Z}_3[x]$, but of course, we already know it's irreducible in $\mathbb{Z}$.

Note also that in $\mathbb{Z}_p[x]$ there are only a finite number of polynomials of a given degree.

So if say $deg(f(x)) = 4$ then if for some p we have that $\bar{f}(x) \in \mathbb{Z}_p[x]$ has degree 4 as well then *if* its reducible we have $\bar{f}(x) = \bar{g}(x)\bar{h}(x)$.

Then either $deg(\bar{g}(x)) = 1$ or $deg(\bar{g}(x)) = deg(\bar{h}(x)) = 2$ and one could check (by brute force) to rule out either possibility.

Why? The reason is that for a given prime p, there are only a finite number of polynomials of given degree n since if

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

then there are $p - 1$ choices of a_n and p choices for each a_i for $i < n$.