MA294 Lecture

Timothy Kohl

Boston University

March 26, 2024

Factorization of Polynomials

In the Division Algorithm, when $f(x) = q(x)g(x) + r(x)$, if $r(x) = 0$ then $f(x) = q(x)g(x)$ so that $g(x)$ evenly divides $f(x)$ and we have a factorization of $f(x)$ into two *lower degree* polynomials.

We begin with a basic result relating factors with roots.

Definition

If $f(x) \in R[x]$ where say $f(x) = a_n x^n + \cdots + a_1 x + a_0$ then for $\alpha \in R$ one has

$$f(\alpha) = a_n \alpha^n + \cdots + a_1 \alpha + a_0$$

which is the result of evaluating $f(x)$ at $x = \alpha$ which yields an element of R.

Note: If $f(x) = x - \alpha$ then clearly $f(\alpha) = 0$.

Theorem

Let F be a field, and suppose $f(x) \in F[x]$ then $x - \alpha$ is a divisor of $f(x)$ if and only if $f(\alpha) = 0$.

Proof.

Assume $deg(f(x)) \geq 1$ then $f(x) = q(x)(x - \alpha) + r(x)$ for some $q(x)$, $r(x)$ so that $f(\alpha) = q(\alpha)(\alpha - \alpha) + r(\alpha)$ which equals $r(\alpha)$.

However $deg(r(x)) < deg(x - \alpha) = 1$ so $r(x)$ is constant, which means $r(x) = 0$. □

Note, if $f(\beta) = 0$ for some $\beta \in F$ as well, then if $\alpha \neq \beta$

$$\begin{array}{c} f(x) = q(x)(x - \alpha) \\ \downarrow \\ f(\beta) = q(\beta)(\beta - \alpha) \end{array}$$

so that $f(\beta) = 0$ if and only if $q(\beta) = 0$ meaning that $q(x) = \tilde{q}(x)(x - \beta)$ so, concordantly $f(x) = \tilde{q}(x)(x - \beta)(x - \alpha)$ where $deg(f(x)) = n$ implies $deg(q(x)) = n - 1$ and therefore $deg(\tilde{q}(x)) = n - 2$.

The result of this is the following fact about the roots (potentially repeated) of a polynomial $f(x)$.

Theorem

If F is a field and $f(x) \in F[x]$ where $deg(f(x)) = n$ then $f(x)$ has at most n distinct roots.

In general, finding roots/factors of a polynomial $f(x) \in \mathbb{R}[x]$ is difficult if $deg(f(x)) \geq 5$ since there are no explicit formulas, except for $deg(f(x)) = 2, 3, 4$.

Of course, trial and error can sometimes lead to factorizations of larger degree polynomials.

What about polynomials in $\mathbb{Z}_p[x]$.

Observation: For a given degree n, there are $(p-1)p^n$ polynomials of degree n since if $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ then $a_n \neq 0$ but each $a_i \in \mathbb{Z}_p$ for $i = 0, \ldots, n-1$.

So, in principal one could take a given $f(x) \in \mathbb{Z}_p[x]$ and look at all $q(x), g(x) \in \mathbb{Z}_p[x]$ such that $deg(q(x)) + deg(g(x)) = deg(f(x))$ and compute $q(x)g(x)$ to see if it equals $f(x)$.
e.g.

$$
\begin{aligned}
f(x) &= ax^2 + bx + c\\
g(x) &= dx + f\\
q(x) &= hx + k
\end{aligned}
$$

For simplicity though, we can assume that if

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

and $f(\alpha) = 0$ then if

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

where $\tilde{f}(\alpha) = 0$ too.

i.e. One can restrict attention to monic polynomials.

So in $\mathbb{Z}_p[x]$ we have say

$$\begin{aligned} f(x) &= x^2 + ax + b \\ &= (x-\alpha)(x-\beta) \end{aligned}$$

where there are p^2 monic quadratics $f(x)$, so we can ask, how many of these are irreducible, that is *not* factorable as $(x-\alpha)(x-\beta)$.

Since $(x-\alpha)(x-\beta) = (x-\beta)(x-\alpha)$ then there are

$$\underbrace{\frac{1}{2}p(p-1)}_{\alpha\neq\beta} + \underbrace{p}_{\alpha=\beta} = \frac{p^2+p}{2}$$

monic quadratics that are factorable.

As such there are $\frac{p^2-p}{2}$ irreducible (monic) quadratic polynomials $\mathbb{Z}_p$ polynomials.

Note: Sometimes a polynomial will have irreducible factors that are not linear. (degree 1)

Example: $x^4+1 \in \mathbb{Z}_3[x]$ is factorable as $(x^2+x+2)(x^2+2x+2)$ but neither are linear, and neither are themselves factorable.

Why? Simply plug in $x=0,1,2$ into $q(x)=x^2+x+2$ you get

$$q(0)=2$$
$$q(1)=1$$
$$q(2)=2$$

and similarly x^2+2x+2 has no roots in $\mathbb{Z}_3$ either.

Finite Fields

As $\mathbb{Z}_p$ is a field, we use the notation $\mathbb{F}_p$ to emphasize the fact that it's a field, albeit one with finitely many elements.

We shall now consider a (actually the) finite field with $9 = 3^2$ elements.

Consider $f(x) = x^2 + 1 \in \mathbb{F}_3[x]$ and observe that $f(0) = 1$, $f(1) = 2$, and $f(2) = 2$ which implies that $f(x)$ is irreducible.

Moreover, consider what happens if we take an arbitrary $p(x) \in \mathbb{F}_p[x]$ and divide it by $x^2 + 1$, i.e.

$$p(x) = q(x)(x^2 + 1) + r(x)$$

where $r(x) = 0$, or $deg(r(x)) < deg(x^2 + 1) = 2$

This means that $r(x) = ax + b$ for some $a, b \in \mathbb{F}_3$ and this is the case regardless of the degree of $p(x)$, so

$$r(x) \in \{0, 1, 2, x, x+1, x+2, 2x, 2x+1, 2x+2\}$$

so there are $3^2 = 9$ different remainders.

Consider the parallel with dividing an arbitrary integer n by a *fixed* integer (modulus) m to yield $n = qm + r$ where $r \in \{0, 1, \ldots, m-1\}$ which leads to the construction of the ring $\mathbb{Z}_m$.

We can make $\mathbb{F}_9 = \{0, 1, 2, x, x+1, x+2, 2x, 2x+1, 2x+2\}$ into a ring as well.

First, the addition is simply

$$\underbrace{(ax+b)}_{\in\mathbb{F}_9} + \underbrace{(a'x+b')}_{\in\mathbb{F}_9} = (a+a')x + (b+b') \in \mathbb{F}_9$$

and when we multiply according to the following rule, which stems from the roots of the polynomial $x^2+1=0$, namely $x^2 = -1 = 2$.

Thus

$$(ax+b)(a'x+b') = aa'x^2 + ab'x + a'bx + bb' = (ab'+a'b)x + (2aa'+bb') \in \mathbb{F}_9$$

and $0 = 0x+0$ and $1 = 0x+1$ are the additive and multiplicative identity elements.

In order to establish that $\mathbb{F}_9$ is a field, we need to show that each non-zero element has a multiplicative inverse, for example
$(x+1)(x+2) = x^2 + 3x + 2 = x^2 + 2 = 2 + 2 = 1$.

By direct calculation:

$$\begin{aligned}
1^{-1} &= 1 \\
(x+1)^{-1} &= x+2 \\
(2x+1)^{-1} &= 2x+2 \\
2^{-1} &= 2 \\
(x+2)^{-1} &= x+1 \\
(2x+2)^{-1} &= 2x+1 \\
x^{-1} &= 2x \\
(2x)^{-1} &= x
\end{aligned}$$

So $\mathbb{F}_9$ is a field.

In general, one can argue as follows:

Definition

A commutative ring with unity R is a domain (or integral domain) if, for $x, y \in R$, $xy = 0$ implies that $x = 0$ or $y = 0$, or both.

In a domain, one can show that if $x \neq 0$ then $xy = xz$ implies $y = z$.

Why? If $xy = xz$ then $xy - xz = 0$ that is $x(y - z) = 0$.

But being a domain, if $x \neq 0$ then $x(y - z) = 0$ implies that $y - z = 0$, but then $y = z$.

The relevence to $\mathbb{F}_9$ is the following useful fact due to Wedderburn.

Theorem

If R is an integral domain where $|R|$ is finite, then R is a field.

Proof.

Consider $R - \{0\} = \{r_1, r_2, \ldots, r_n\}$ where, we may assume $r_1 = 1$.
So now, pick any element $r \in R - \{0\}$ (i.e. $r = r_i$ for some i) and consider $\{rr_1, rr_2, \ldots, rr_n\}$.

We note that $rr_j = rr_k$ implies $r_j = r_k$ because R is a domain, so $\{rr_1, rr_2, \ldots, rr_n\}$ is a permutation of $R - \{0\}$ and so, for some r_j we have $rr_j = 1$ since $1 \in R - \{0\}$. Thus, r has an inverse. □

So applied to $\mathbb{F}_9$ we can easily show that it is a domain (just check the rule for multiplication) and so we can infer it's a field by Wedderburn's theorem.

Another way to view $\mathbb{F}_9$ is by the observation that 'x' in $\mathbb{F}_9$ has the property that $x^2 = 2 = -1$ which is very analgous to the imaginary unit i which has the property that $i^2 = -1$.

The analogy we draw is that $a + bx \leftrightarrow a + bi$ so that $\mathbb{F}_9$ is $\mathbb{F}_3$ with 'i' adjoined, just as $\mathbb{C}$ is $\mathbb{R}$ with 'i' adjoined to 'enlarge' it.

We can also compute powers of elements of the *group* $U(\mathbb{F}_9) = \mathbb{F}_9^*$,

$$
\begin{aligned}
(2x+1)^0 &= 1\\
(2x+1)^1 &= 2x+1\\
(2x+1)^2 &= x\\
(2x+1)^3 &= x+1\\
(2x+1)^4 &= 2\\
(2x+1)^5 &= x+2\\
(2x+1)^6 &= 2x\\
(2x+1)^7 &= 2x+2\\
(2x+1)^8 &= 1
\end{aligned}
$$

which shows that $U(\mathbb{F}_9) = \langle 2x+1 \rangle$, i.e. a cyclic group.