MATH 369 Fall 2025 - Class Notes

11/10/2025

Scribe: Muswe P

Warm Up

Question: Can we use Eisenstein's Criterion on f(x)?

$$f(x) = 10x^4 + 12x^2 + 36$$

Is there a prime p such that $p \mid a_i$ for all coefficients except the leading one a_n, and $p^2 \nmid a_0$?

Check for $p = 3$

$$3 \nmid 10, \quad 3 \mid 12, \quad 3^2 \mid 36$$

So $p = 3$ doesn't work because $3^2 \mid 36$ and it shouldnt.

Find the Content of the Polynomial

$$\gcd(10, 12, 36) = 2$$

So

$$f(x) = 2(5x^4 + 6x^2 + 18)$$

Now we can use Eisenstein's Criterion with $p = 2$:

$$2 \nmid 5, \quad 2 \mid 6, \quad 2 \mid 18, \quad 2^2 \nmid 18$$

Therefore, the polynomial is irreducible by Eisenstein's Criterion with $p = 2$.

p-th Cyclotomic Polynomial

If p is a prime, then the p-th cyclotomic polynomial is

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1.$$

Roots of Unity

z is an n-th root of unity if it is a root of the polynomial

$$x^n - 1 \in \mathbb{C}.$$

Square roots of unity are ± 1. Fourth roots of unity are $\pm 1, \pm i$.

z is a *primitive* n-th root of unity if it is an n-th root of unity but not a k-th root of unity for $k < n$.

The roots of $\Phi_p(x)$ are the p-th roots of unity.

Example

$$\Phi_3(x) = x^2 + x + 1$$

We can use Eisenstein's criterion and a shift to prove that Φ_3 is irreducible.

$$\Phi_p(x)(x-1) = (x^{p-1} + x^{p-2} + \cdots + x + 1)(x-1)$$
$$= (x^p + x^{p-1} + \cdots + x^2 + x) - (x^{p-1} + x^{p-2} + \cdots + x + 1)$$
$$= x^p - 1$$

Thus, as a polynomial,

$$\Phi_p(x) = \frac{x^p - 1}{x - 1}.$$

We can't use Eisenstein's Criterion directly on $\Phi_p(x)$, so we use a shift.

This polynomial $\Phi_p(x)$ is irreducible if and only if $\Phi_p(x+1)$ is irreducible.

$$\Phi_p(x+1) = \frac{(x+1)^p - 1}{x + 1 - 1} = \frac{(x+1)^p - 1}{x}.$$

Using the binomial expansion,

$$(x+1)^p = \sum_{i=0}^{p} \binom{p}{i} x^{p-i}(1)^i.$$

So,

$$\Phi_p(x+1) = \frac{\sum_{i=0}^{p} \binom{p}{i} x^{p-i}(1)^i - 1}{x} = \sum_{i=0}^{p-1} \binom{p}{i} x^{p-i}(1)^i.$$

$$\Phi_p(x+1) = \sum_{i=0}^{p-1} \binom{p}{i} x^{p-i-1}.$$

The binomial coefficient formula,

$$\binom{p}{i} = \frac{p!}{(p-i)!i!}.$$

If $i \neq 0, p$, this is divisible by p, since the numerator is divisible by p but the denominator is not.

Applying Eisenstein's Criterion

When $i = 0$, the leading coefficient is

$$\binom{p}{0} = \frac{p!}{(p-0)! \cdot 0!} = 1,$$

So p doesn't divide the leading coefficient.

Every lower-term coefficient is divisible by p, and the constant term is

$$\binom{p}{1} = \frac{p!}{(p-1)! \cdot 1!} = p,$$

and $p^2 \nmid p$.

Therefore, this polynomial is irreducible by Eisenstein's criterion.

Keep in mind that there exist irreducible polynomials that cannot be proven irreducible by Eisenstein's criterion, even using any shift. For example:

$$x^5 + x + 1$$

Fundamental Theorem of Algebra

Every polynomial $f(x) \in \mathbb{C}[x]$ factors completely into linear terms in $\mathbb{C}[x]$.

Corollaries

- The only irreducible polynomials in $\mathbb{C}[x]$ are the linear polynomials $ax + b$.
- Every polynomial $f(x) \in \mathbb{Q}[x]$ or $f(x) \in \mathbb{R}[x]$ has a root in $\mathbb{C}$, since $\mathbb{C}$ is an extension field of $\mathbb{Q}$ and $\mathbb{R}$.

Automorphisms and Complex Conjugation

Definition

An *automorphism* is a homomorphism from an object to itself.

The function $g : \mathbb{C} \to \mathbb{C}$ given by

$$g(a + bi) = a - bi$$

is an automorphism (*complex conjugation*).

Check bijection

Onto: Pick $c + di \in \mathbb{C}$. Then

$$g(c - di) = c + di.$$

Thus g is onto.

One-to-one: If $g(a + bi) = g(c + di)$, then

$$a - bi = c - di.$$

Hence $a = c$ and $b = d$, so $a + bi = c + di$. Thus g is one-to-one.

Check homomorphism on $(\mathbb{C}, +)$

$$g((a+bi)+(c+di)) = g((a+c)+(b+d)i) = (a+c)-(b+d)i = (a-bi)+(c-di) = g(a+bi)+g(c+di).$$

So g preserves addition.

Check multiplication

$$g((a + bi)(c + di)) = g((ac - bd) + (ad + bc)i) = (ac - bd) - (ad + bc)i.$$

On the other hand,

$$g(a + bi)g(c + di) = (a - bi)(c - di) = ac - bd - adi - bci = (ac - bd) - (ad + bc)i.$$

Thus g preserves multiplication.

Therefore, complex conjugation is an automorphism. We typically denote it with a bar over the number:

$$\text{If } z = a + bi, \text{ then } \overline{z} = a - bi.$$

Properties of Complex Conjugation

If $x \in \mathbb{R} \subseteq \mathbb{C}$, then $\overline{x} = x$.

Theorem

If $f(x) \in \mathbb{R}[x]$ and $z \in \mathbb{C}$ is a root of $f(x)$, then $\overline{z}$ is also a root.

Proof

Since z is a root of $f(x) = a_n x^n + \cdots + a_0$ then

$$f(z) = a_n z^n + a_{n-1} z^{n-1} + \cdots + a_0 = 0.$$

Apply complex conjugation to both sides:

$$\overline{a_n z^n + a_{n-1} z^{n-1} + \cdots + a_0} = \overline{0} = 0.$$

Since conjugation is an automorphism,

$$\begin{aligned} \overline{a_n z^n} + \overline{a_{n-1} z^{n-1}} + \cdots + \overline{a_0} &= 0, \\ \overline{a_n} * \overline{z}^n + \overline{a_{n-1}} * \overline{z}^{n-1} + \cdots + \overline{a_0} &= 0, \\ a_n (\overline{z})^n + a_{n-1} (\overline{z})^{n-1} + \cdots + a_0 &= 0, \end{aligned}$$

using $a_i \in \mathbb{R}$ and $\overline{z^i} = (\overline{z})^i$.

Thus,

$$f(\overline{z}) = 0.$$

So $\overline{z}$ is also a root.

Observe

If $z \in \mathbb{C}$, then

$$(x - z)(x - \overline{z}) \in \mathbb{R}[x].$$

Proof

Let $z = a + bi$ and $\overline{z} = a - bi$. Then:

$$(x - (a + bi))(x - (a - bi)) = (x - a - bi)(x - a + bi) = (x - a)^2 + b^2 \in \mathbb{R}[x].$$

Theorem.

Every polynomial in $\mathbb{R}[x]$ factors into linear and quadratic irreducible terms.

Proof.

Let $f(x) \in \mathbb{R}[x]$. Then by the Fundamental Theorem of Algebra, $f(x)$ factors completely in $\mathbb{C}[x]$.

$$f(x) = a_n(x - r_1)(x - r_2)\cdots(x - r_n)$$

where $r_1, r_2, \ldots, r_n \in \mathbb{C}$.

If $r_i \in \mathbb{R}$, then we have a linear term $(x - r_i) \in \mathbb{R}[x]$.

If $r_i \in \mathbb{C} \setminus \mathbb{R}$, then there is also a root $r_j = \overline{r_i}$. Then

$$(x - r_i)(x - r_j) = (x - r_i)(x - \overline{r_i}) \in \mathbb{R}[x]$$

is a quadratic irreducible in $\mathbb{R}[x]$.

By pairing them up, every root not already in $\mathbb{R}$ becomes part of a quadratic irreducible.

Finite Field

If p is prime, then $\mathbb{Z}_p$ is a field. If $q(x) \in \mathbb{Z}_p[x]$ is irreducible, then

$$\mathbb{Z}_p[x]/\langle q(x)\rangle$$

is a field.

If $\deg(q) = n$, then the remainders in $\mathbb{Z}_p[x]/\langle q(x)\rangle$ are polynomials of degree at most $n - 1$.

Every equivalence class looks like

$$[a] = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_0$$

There are p choices for each coefficient, so there are p^n elements in the field $\mathbb{Z}_p[x]/\langle q(x)\rangle$.

If $n = p$, then we can construct a finite field with n elements in this way.

In cryptography, AES (Advanced Encryption Standard) performs arithmetic in a field with $256 = 2^8$ elements. AES uses the irreducible polynomial

$$f(x) = x^8 + x^4 + x^3 + x + 1$$

to create the field $\mathbb{Z}_2[x]/\langle f(x)\rangle$ with 256 elements.

If n is not a prime power, then we cannot create a field with n elements.

Example: There does not exist a field with 6 elements.