MATH 369 Fall 2025 - Class Notes

11/10/2025

Scribe: Lola Scannell

Summary: Today, we reviewed Eisenstein's Criterion with an example, introduced cyclotomic polynomials (especially the pth cyclotomic polynomial $\Phi_p(x)$), and used a shifted version $\Phi_p(x+1)$ to prove irreducibility via Eisenstein. We discussed complex conjugation as an automorphism that comes in conjugate pairs, and concluded that any real polynomial factors as a product of linear and irreducible quadratic factors in $\mathbb{R}[x]$. Finally, we talked about constructing finite fields $\mathbb{F}_{p^n}$ as $\mathbb{F}_p[x]/(g(x))$ using irreducible polynomials, and saw how AES uses a field with $256 = 2^8$ elements.

Notes:

1. Eistenstein's Criterion example

We looked at the polynomial

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

First , we computed the *content*:

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

so

$$f(x) = 2g(x) \quad \text{where} \quad g(x) = 5x^4 + 6x^2 + 18.$$

To apply Eisentstien's Criterion to $g(x)$, take the prime $p = 2$:

- The leading coefficient 5 is not divisble by 2.
- All the other coefficents 6 and 18 are divisble by 2.
- The constant term 18 is *not* divisible by $2^2 = 4$

So by Eistenstein's Criterion with $p = 2$, $g(x)$ is irreducible over $\mathbb{Q}[x]$. Since $f(x) = 2g(x)$ only differs from $g(x)$ by a nonzero scalar in $\mathbb{Q}$, $f(x)$ is also irreducible in $\mathbb{Q}[x]$.

2. Cyclotomic polynomials and primitive roots of unity

An *nth root of unity* is a complex number z such that

$$z^n = 1$$

Examples:

- 1 and -1 are the 2nd roots of unity.
- The 3rd roots of unity are $1, \omega, \omega^2$ where $\omega = e^{2\pi i/3}$.
- The 4th roots of unity are $1, i, -1, -i$

A complex number z is a *primitive* nth root of unity if

$$z^n = 1 \quad \text{but} \quad z^k \neq 1 \text{ for } 1 \leq k < n.$$

For a prime p, the pth *cyclotomic polynomial* is

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

Its roots are exactly the primitive pth roots of unity.

Example: For $p = 3$,

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

We also used the identity

$$x^p - 1 = (x-1)\Phi_p(x)$$

to relate $\Phi_p(x)$ to $x^p - 1$.

3. **Using Eisenstein on $\Phi_p(x+1)$**

We cannot directly apply Eisenstein to

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

but we can shift the variable and look at

$$\Phi_p(x+1)$$

Recall

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

so

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

Using the binomial theorem,

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

Then

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

and dividing by x,

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

Key facts for a prime p:

- $\binom{p}{0} = 1$ and $\binom{p}{p} = 1$ are not divisible by p.
- For $1 \leq i \leq p-1$, $\binom{p}{i}$ is divisible by p.

So in $\Phi_p(x+1)$:

- The *leading* coefficient (of x^{p-1}) is 1, not divisible by p.
- Every other coefficient is divisible by p.
- The constant term is $\binom{p}{1} = p$, which is not divisible by p^2.

By Eisenstein's Criterion with this prime p, $\Phi_p(x+1)$ is irreducible in $\mathbb{Q}[x]$. A change of variable $x \mapsto x-1$ is an isomorphism of $\mathbb{Q}[x]$, so $\Phi_p(x)$ is also irreducible in $\mathbb{Q}[x]$.

4. **Complex conjugation as an automorphism**

Define $g : \mathbb{C} \to \mathbb{C}$ by

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

i.e. complex conjugation.

We checked that:

- g is bijective, with inverse g itself.
- g respects addition:

$$g\big((a+bi)(c+di)\big) = g(a+bi)\, g(c+di).$$

So g is a field automorphism of $\mathbb{C}$ that fixes $\mathbb{R}$.

Using this, if $f(x) \in \mathbb{R}[x]$ and z is a root of f, then

$$0 = g(f(z)) = f(g(z)) = f(\overline{z}),$$

so $\overline{z}$ is also a root of f.

5. **Factorization over $\mathbb{R}$**

By the Fundamental Theorem of Algebra, any polynomial $f(x) \in \mathbb{C}[x]$ can be written as a product of linear factors:

$$(x - r_i)(x - \overline{r_i}).$$

Writing $r_i = a + bi$ with $b \neq 0$,

$$(x - (a + bi))(x - (a - ab)) = (x - a)^2 + b^2.$$

which is a quadratic polynomial with real coefficients and no real roots, hence irreducible over $\mathbb{R}$.

So every polynomial in $\mathbb{R}[x]$ factors as a product of:

- linear factors $(x - r)$ with $r \in mathbbR$, and
- irreducible quadratic factors coming from non-real conjugate pairs.

6. **Finite fields via irreducible polynomials**

Let p be a prime and consider $\mathbb{F}_p[x]$.

If $g(x) \in \mathbb{F}_p[x]$ is irreducible of degree n, then the quotient

$$\mathbb{F}_p[x]/(g(x)$$

is a field. Every class can be represented by a polynomial of degree at most $n - 1$,

$$a_{n-1}x^{n-1} + \cdots + a_1x + a)0, \qquad a_i \in \mathbb{F}_p$$

Since there are p choices for each coefficient and n coefficients, this field has p^n elements.

Important facts:

- For every prime power p^n there exists a finite field with p^n elements.
- There is *no* field whose size is not a prime power (e.g. no field with 6 elements).

A cryptography example: AES works in a field with $256 = 2^8$ elements, which can be constructed as

$$\mathbb{F}_2[x]/(f(x)),$$

Theorems and Proofs:

Theorem 1. *For a prime p, the cyclotomic polynomial*

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

is irreducible in $\mathbb{Q}[x]$.

Proof. Consider $\Phi_p(x + 1)$. Using the binomial theorem and the fact that $\binom{p}{i}$ is divisible by p for $1 \leq i \leq p - 1$, we can see that:

- the leading coefficient of $\Phi_p(x + 1)$ and 1, not divisible by p

- all other coefficients are divisible by p, and
- the constant term is p, not divisible by p^2.

By Eisenstein's Criterion with respect to the prime p, $\Phi_p(x+1)$ is irreducible in $\mathbb{Q}[x]$. A change of variable $x \mapsto x-1$ shows that $\Phi_p(x)$ is also irreducible in $\mathbb{Q}[x]$. $\square$

Theorem 2. *If $f(x) \in \mathbb{R}[x]$ and $z \in \mathbb{C}$ is a root f, then $\overline{z}$ is also a root of f.*

Proof. Write $f(x) = a_n x^n + \cdots + a_1 x + a_0$ with $a_i \in \mathbb{R}$. Suppose $f(z) = 0$. Apply complex conjugation:

$$0 = \overline{f(z)} = \overline{a_n z^n + \cdots a_1 z + a_0} = a_n \overline{z}^n + \cdots + a_1 \overline{z} + a_0 = f(\overline{z}).$$

Thus $\overline{z}$ is also a root of f. $\square$

Theorem 3. *Every polynomial in $\mathbb{R}[x]$ can be factored as a product of linear factors and irreducible quadratic factors.*

Proof. By the Fundamental Theorem of Algebra, any $f \in \mathbb{C}$ factors as a product of linear factors $(x - r_i)$ with $r_i \in \mathbb{C}$. If f has real coefficients, then non-real roots come in conjugate pairs $r, \overline{r}$. The product $(x-r)(x-\overline{r}$ is a quadratic polynomial with real coefficients and no real roots, hence irreducible over $\mathbb{R}$. Grouping all such conjugate pairs gives the desired factorization into real linear and irreducible quadratic factors. $\square$