MATH 369 Fall 2025 - Class Notes

10/29/2025

Scribe: Hans Zook

Summary: We discussed Euclid's Algorithm, irreducibility, and subfields

Notes:

Euclid's Algorithm A way to find greatest common divisors of two polynomials.
Example

$$GCD(2x^4 + x^3 - 6x^2 + 7x - 2, 2x^3 - 7x^2 + 8x - 4)$$

From last lecture, we saw that $(2x^3 - 7x^2 + 8x - 4) \div (2x^4 + x^3 - 6x^2 + 7x - 2) = x + 4 + r$
$(14x^2 - 21x + 14) \div (2x^3 - 7x^2 + 8x - 4) = (1/7)x - (2/7) + 0$
So $GCD(2x^4 + x^3 - 6x^2 + 7x - 2, 2x^3 - 7x^2 + 8x - 4) = 14x^2 - 21x + 14$ Except it has to be monic. This gives us

$$GCD(2x^4 + x^3 - 6x^2 + 7x - 2, 2x^3 - 7x^2 + 8x - 4) = x^2 - (3/2)x + 1$$

The extended Euclidean Algorithm can be used to find polynomials $a(x), b(x)$ so that $GCD(f(x), g(x)) = d(x) = a(x)f(x) + b(x)g(x)$ where $a(x)f(x) + b(x)g(x)$ is the linear combination that we proved existed.

Two polynomials $f(x), g(x)$ are relatively prime if the $GCD(f(x), g(x)) = 1$.

Theorem 1. *If $p(x), f(x)$ are relatively prime, and $p(x)|f(x)g(x)$, then $p(x)|g(x)$.*

Proof. Since $p(x), f(x)$ are relatively prime,

$$GCD(p(x), f(x)) = 1$$

So there exist polynomials $a(x), b(x)$ with $1 = a(x)p(x) + b(x)f(x)$

Multiply through by $g(x)$.

$$g(x) = a(x)g(x)p(x) + b(x)f(x)g(x)$$

Since $p(x)|f(x)g(x)$, $f(x)g(x) = c(x)p(x)$ for some $c(x)$.
Now

$$g(x) = a(x)g(x)p(x) + b(x)c(x)p(x) = p(x)[a(x)g(x) + b(x)c(x)]$$

Where $[a(x)g(x) + b(x)c(x)]$ is some polynomial. So

$$p(x)|g(x)$$

□

Definition 1. *A polynomial $f(x) \in F[x]$ is irreducible if wherever $f(x) = g(x)h(x)$, one of $g(x)$ or $h(x)$ is a constant polynomial.*

Theorem 2. *A polynomial $p(x)$ is irreducible iff wherever $p(x)|f(x)g(x)$, either $p(x)|f(x)$ or $p(x)|g(x)$ (or both).*

Whether or not a polynomial is irreducible depends on the field of its coefficients.

Example Is $x^2 - 2$ irreducible?
$x^2 - 2 \in \mathbb{Q}[x]$ is irreducible
$x^2 - 2 \in \mathbb{R}[x]$ is reducible since

$$x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$$

.

Example Is $x^2 + 1$ irreducible?
$x^2 + 1$ is irreducible in $\mathbb{Q}[x]$ and $\mathbb{R}[x]$
$x^2 + 1$ is reducible in $\mathbb{C}[x]$ since

$$x^2 + 1 = (x - \sqrt{-1})(x + \sqrt{-1})$$

How about in $\mathbb{Z}_2$?

$$(x + 1)^2 = x^2 + 2x + 1 = x^2 + 0x + 1 = x^2 + 1$$

So $x^2 + 1$ is reducible in $\mathbb{Z}_2$.

Theorem 3. *A polynomial of degree 2 or 3 is irreducible iff it has no roots in its field.*

Proof. If such a polynomial were irreducible, the factorization would have to have a linear factor. The linear factor gives a root of the polynomial.
This does not work for polynomials of degree 4 or more. □

Example
$x^4 + 4x^2 + 4 = (x^2 + 2)^2 \in \mathbb{Q}[x]$ has no roots in $\mathbb{Q}$.

If $(x - a)^m | f(x)$, we call a a root of order m of $f(x)$.

Theorem 4. *If $f(x) \in \mathbb{Q}[x], \mathbb{R}[x]$, then $f(x)$ has a repeated factor (divisible by $p(x)^m$ where $m > 1$) iff $GCD(f(x), f'(x)) \neq 1$.*

Proof. (Key idea is product rule)

$$d/dx[f(x)g(x)] = f(x)g'(x) + f'(x)g(x)$$

$$\Rightarrow$$

Suppose $f(x)$ has a repeated factor $f(x) = p(x)^m g(x)$. Differentiate

$$f'(x) = p(x)mg'(x) + mp(x)m - 1p'(x)g(x)$$

where $m - 1 > 0$.
So

$$f'(x) = p(x)[p(x)^{m-1}g'(x) + mp(x)^{m-2}p'(x)g(x)]$$

So $p(x)|f(x)$ and $p(x)|f'(x)$. So

$$GCD(f(x), f'(x)) \neq 1$$

$$\Leftarrow$$

Suppose

$$GCD(f(x), f'(x)) \neq 1$$

then

$$GCD(f(x), f'(x)) = d(x)$$

pick $p(x)$ to be some irreducible factor of $d(x)$. So

$$p(x)|f(x) \Rightarrow f(x) = p(x)g(x)$$

for some polynomial $p(x)$. Differentiating

$$f'(x) = p(x)g'(x) + p'(x)g(x)$$

where $p(x)|f'(x)$ and $p(x)|p(x)g'(x)$.
Since $p(x)|f'(x)$ and $p(x)|p(x)g'(x)$, it must also divide $p'(x)g(x)$. $p(x)$ cannot divide $p'(x)$ (since $p'(x)$ has smaller degree).
So $p(x), p'(x)$ are relatively prime. Since $p(x)|p'(x)g(x)$, it must be that $p(x)|g(x)$. Since $f(x) = p(x)g(x)$, we have that

$$p(x)^2|f(x)$$

□

Theorem 5. *If F is a field, then any polynomial in $F[x]$ factors uniquely into irreducible factors (up to multiplication by elements of F).*

If E, F, G are fields where $G \subset F \subset E$, we call G a subfield of F and E an extension field of F.

Question: If $f(x) \in F[x]$ is irreducible can we find an extension field of F where $f(x)$ is reducible?

Key Idea: Extend modular arithmetic from $\mathbb{Z}$ to $F[x]$

In $\mathbb{Z}_n$ define $a \equiv b \pmod{n}$ if $n|(b-a)$.

Here we define $f(x) \equiv g(x) (\text{mod } p(x))$ if $p(x)|(g(x) - f(x))$.

With polynomials, the equivalence classes form a group under addition. Multiplication of congruence classes is well defined.

Question: When do we have multiplication inverses?