MATH 369 Fall 2025 - Class Notes

10/29/2025

Scribe: Dona Aldossary

Summary: Using Euclid's Algorithm for polynomials, degrees, and irreducibility, theorems involving relatively prime polynomials and gcds, and properties of fields

Notes:

Euclid's Algorithm for Polynomials is a way to find gcds for polynomials:
Find $\gcd(2x^4 + x^3 + 6x^2 = 7x - 2, 2x^3 - 7x^2 + 8x - 4)$

$$
\begin{array}{r}
\; x + 4 \\
(2x^3 - 7x^2 + 8x - 4)\big) \overline{2x^4 + x^3 - 6x^2 + 7x - 2} \\
\; 2x^4 - 7x^3 + 8x^2 - 4x \\
\hline
\; 8x^3 - 14x^2 + 11x - 2 \\
\; 8x^3 - 28x^2 + 32x - 16 \\
\hline
\; 14x^2 - 21x + 14
\end{array}
$$

We can't divide any further we continue dividing with our remainder, as our new divisor. To make dividing easier we can make it monic by dividing all the coefficents by 14, giving us our new divisor $x^2 - \frac{3}{2}x + 1$:

$$
\begin{array}{r}
\phantom{(x^2 - \frac{3}{2}x + 1)\big)}\; 2x + 4 \\
(x^2 - \frac{3}{2}x + 1)\big) \overline{2x^3 - 7x^2 + 8x - 4} \\
\phantom{(x^2 - \frac{3}{2}x + 1)\big)}\; 2x^3 - 3x^2 + 2x \\
\hline
\phantom{(x^2 - \frac{3}{2}x + 1)\big)}\; -4x^2 + 6x - 4 \\
\phantom{(x^2 - \frac{3}{2}x + 1)\big)}\; -4x^2 + 6x - 4 \\
\hline
\phantom{(x^2 - \frac{3}{2}x + 1)\big)}\; 0
\end{array}
$$

Since the remainder is 0, the gcd is $(x^2 - \frac{3}{2}x + 1)$

The extended Euclidean Algorithm can be used to find polynomials $a(x), b(x)$ so that:

$$\gcd(f(x), g(x)) = d(x) = a(x)f(x) + b(x)g(x)$$

Two polynomials, $f(x), g(x)$ are relatively prime if

$$\gcd(f(x), g(x)) = 1$$

Theorem: If $p(x)$ and $f(x)$ are relatively prime and $p(x)|f(x)g(x)$ then $p(x)|g(x)$

Proof:
Since $p(x)$ and $f(x)$ are relatively prime, $\gcd(f(x), g(x)) = 1$.

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

Multiply that equation by $g(x)$:

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

Since $p(x)|f(x)g(x)$

$f(x)g(x) = c(x)p(x)$ for some $c(x)$

Substitute now:

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

Thus $p(x)|g(x)$
Definition: A polynomial $f(x) \in F[x]$ is irreducible if whenever $f(x) = g(x)h(x)$ one of $g(x)$ or $h(x)$ is a constant polynomials
Another way to word this is:
A polynomial $f(x)$ is irreducible if and only if whenever $p(x)|f(x)g(x)$ either $p(x)|f(x)$ or $p(x)|g(x)$ or both.

Example:
Is $x^2 - 2 \in \mathbb{Q}[x]$ irreducible?

Yes, $x^2 - 2 \in \mathbb{Q}[x]$ is irreducible.
But $x^2 - 2 \in \mathbb{R}[x]$ is reducible, $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$

Is $x^2 + 1 \in \mathbb{Q}[x]$ irreducible?

Yes, $x^2 + 1 \in \mathbb{Q}[x]$ is irreducible
Yes, $x^2 + 1 \in \mathbb{R}[x]$ is irreducible
But $x^2 + 1 \in \mathbb{C}[x]$ is reducible, $x^2 + 1 = (x - \sqrt{-1})(x + \sqrt{-1})$
But $x^2 + 1 \in \mathbb{Z}_2[x]$ is reducible, $(x^2 + 1) = (x + 1)^2 = (x^2 + 2x + 1) = (x^2 + 1)$

Theorem:A polynomial of degree 2 and 3 is irreducible if and only if 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

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

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

Theorem: If $f(x) \in \mathbb{Q}[x], \mathbb{R}[x]$, then $f(x)$ has a repeated factor (meaning it is divisible by $p(x)^m > 1$) if and only if $\gcd(f(x), f'(x)) \neq 1$

Proof: The key idea of this proof is the product rule

$$\frac{d}{dx}[f(x)g(x)] = f(x)g'(x) + f'(x)g(x)$$

$\rightarrow$ Suppose $f(x)$ has a repeated factor

$$f(x) = p(x)^m g(x), \qquad m > 1$$

Differentiate both sides:

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

here $m - 1 > 1$ 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 $\gcd(f(x), f'(x)) = 1$
$\leftarrow$ 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:

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

Since $p(x)$ divides $f'(x)$ and $p(x)g'(x)$ it must also divide $p'(x)g(x)$, $p(x)$ cant divide $p'(x)$ since $p'(x)$ has a smaller degree.

So $p(x)$ and $p'(x)$ 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 $p(x)^2|f(x)$
Theorem: 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