MATH 369 Fall 2025 - Class Notes

10/27/2025

Scribe: Mya Freeman

Summary: In this class, we began discussing polynomials, including their properties such as degree and coefficients. We saw how the division algorithm for integers could be applied the same way to polynomials in order to identify the greatest common divisor of two polynomials.

Notes:

Polynomials with coefficients in a field F are denoted $F[x]$. These polynomials obey all the usual rules for polynomials (addition, subtraction, multiplication, etc.)

We call a polynomial $f(x) \in F[x]$ **monic** if $f(x) = 1x^n + a_{n-1}x^{n-1} + ... + a_0$ (leading coefficient of 1; $1 \in F$).

The **leading coefficient** of a polynomial is the coefficient of the highest power of x in the polynomial with a nonzero coefficient.

The **degree** of a polynomial is the highest power of x appearing in the polynomial with nonzero coefficient.

Example: $f(x) = \mathbb{Q}[x]; f(x) = \frac{2}{3}x^5 + \frac{1}{2}x + 2$.

This function has degree 5 with a leading coefficent of $\frac{2}{3}$.

The zero polynomial does not have a well-defined degree since the definition requires a non-zero coefficient. So, $0 \in F[x]$ is defined to have degree $-\infty$ for convenience.

Theorem 1. *If $f(x), g(x) \in F[x]$ with degrees m and n respectively, then the degree of $f(x)g(x)$ is $m + n$.*

Proof. Suppose $f(x)$ and $g(x)$ are not 0. Then, $f(x) = a_m x^m + ...$ where $a_m \neq 0$. $g(x) = b_n x^n + ...$

So, $f(x)g(x) = (a_m x^m + ...)(b_n x^n + ...) = (a_m b_n x^{m+n} + ...)$ and $a_m, b_n \neq 0$ since $a_m b_n \in F$, both nonzero. So, the degree of $f(x)g(x)$ is $m + n$. □

Note: Our definition of 0 having degree $-\infty$ works with the statement of this theorem.

Polynomials with coefficients in a field have many of the same properties as $\mathbb{Z}$.

Theorem 2. *The division algorithm applies to polynomials just like integers.*

Recall: for integers, if $a, b \neq 0, b > 0$, then we can find q and r such that $a = bq + r$ where $0 \leq r < b$.

If $f(x), g(x) \in F[x]$ and $g(x) \neq 0$, then there exists $q(x), r(x) \in F[x]$ where $f(x)) = q(x)g(x) + r(x)$ and the degree of $r(x)$ is less than the degree of $g(x)$ $(deg(r(x)) < deg(g(x)))$. Furthermore, these polynomials $q(x)$ and $r(x)$ are unique.

For the proof you would do long division for $\frac{f(x)}{g(x)}$.

If the remainder when $f(x)$ is divided by $g(x)$ is 0, we say that $g(x)|f(x)$.

If $\alpha \in F$ satisfies $f(\alpha) = 0$, then we say that α is a **root** of $f(x)$ in F.

Theorem 3. *If $\alpha \in F$ is a root of $f(x) \in F[x]$, then $(x-a)|f(x)$.*

Proof. By the division algorithm, we can find $q(x)$ and $r(x)$ with $f(x) = q(x)(x-\alpha)+r(x)$. $deg(r(x)) < deg(x-\alpha) = 1$.

So, $r(x) \equiv C \in F[x]$ and $f(x) = q(x)(x-\alpha)+C$.

Plug in α to both sides: $f(\alpha) = q(\alpha)(\alpha-\alpha)+C$, so $F(\alpha) = C$

$f(\alpha) = 0$, since α is a root. So, $0 = 0 + C; C = 0$. Since our remainder is 0, $(x-\alpha)$ divides $f(x)$. □

Polynomials are not necessarily equal if they result in the same function on F.

Example: $F = \mathbb{Z}_2$

Let $f(x) = x+1$ and $g(x) = x^2+1$

$\mathbb{Z}_2$	f(x)	g(x)
0	1	1
1	0	0

These polynomials produce the exact same function $\mathbb{Z}_2 \to \mathbb{Z}_2$, but $f(x) \neq g(x)$ as elements of $\mathbb{Z}_2[x]$.

We say that $d(x) \in F[x]$ is the greatest common divisor of $f(x)$ and $g(x)$ if $d(x)|f(x)$ and $d(x)|g(x)$, and if $m(x)|f(x)$ and $m(x)|g(x)$, then $m(x)|d(x)$ (so $deg(m(x) \leq deg(d(x)))$ and $d(x)$ is monic.

Theorem 4. *The greatest common divisor of any two polynomials exists.*

Proof. Suppose $i \subseteq F[x]$ with 3 properties:

1. $0 \in I$
2. If $f(x) \in I$ and $g(x) \in I$, then $a(x)f(x)+b(x)g(x) \in I$
3. If $f(x)$ and $g(x) \in I$, then $f(x)g(x) \in I$.

In other words, I is closed under addition, multiplication, and linear combination, and there exists a monic polynomial $d(x) \in F[x]$ such that $I = \{a(x)d(x)|a(x) \in F[x]$.

This is exactly the same as what we saw for integers, same idea of proof as the integers.

Let $d(x)$ be a polynomial of minimal degree in I. Multiply by the inverse of the leading coefficient to make it monic claim every element of I is a multiple of $d(x)$. Prove this by contradiction.

Suppose $g(x) \in I$ is not divisible by $d(x)$. We use the division algorithm to write $g(x) = q(x)d(x)+r(x)$ where $deg(r(x)) < deg(d(x))$.

$r(x) = g(x) - q(x)d(x)$. So, $r(x) \in I$, $r(x) \neq 0$ since $d(x) \nmid g(x)$.

This contradicts $d(x)$ having minimal degree in I. □

Now, if $f(x), g(x) \in F[x]$, then the set $I = a(x)f(x)+b(x)g(x)$ satisfies these three requirements.

So I has to be the set of all multiples of some polynomial $d(x)$. This $d(x)$ is the gcd of $f(x), g(x)$.

If $gcd(f(x), g(x)) = 1$, then we say $f(x), g(x)$ are **relatively prime**.

Euclid's algorithm for polynomials:

By repeatedly applying the division algorithm to $f(x)$ and $g(x)$ we can find their gcd.
Steps:

1. repeatedly divide with remainder
2. pull out the leading coefficient of remainder (can be saved until the end)
3. repeat until we get a 0 remainder
4. the last nonzero remainder is our gcd.

Example: Find the $gcd(2x^4 + x^3 - 6x^2 + 7x - 2, 2x^3 - 7x^2 + 8x - 4)$ in $\mathbb{Q}[x]$.
First perform long division of $\frac{2x^4+x^3-6x^2+7x-2}{2x^3-7x^2+8x-4}$.
We get: $(x + 4) + R : 14x^2 - 21x + 14$
So, $2x^4 + x^3 - 6x^2 + 7x - 2 = (x + 4)(2x^3 - 7x^2 + 8x - 4) + (14x^2 - 21x + 14)$.
Performing long division again on $\frac{2x^3-7x^2+8x-4}{14x^2-21x+14}$.
We get: $\frac{1}{7}x - \frac{2}{7}R : 0$.
So, $2x^3 - 7x^2 + 8x - 4 = (\frac{1}{7}x - \frac{2}{7})(14x^2 - 21x + 14) + 0$.
Since we get a remainder of 0, we have to go back to our last nonzero remainder, $14x^2 - 21x + 14$.
Factoring out the 14 to make it monic, we get:
$14(x^2 - \frac{3}{2}x + 1)$.
So the $gcd(2x^4 + x^3 - 6x^2 + 7x - 2, 2x^3 - 7x^2 + 8x - 4) = x^2 - \frac{3}{2}x + 1$.