MATH 369 Fall 2025 - Class Notes

10/27/2025

Scribe: Brooke McConnell

Summary: These notes review polynomials concepts such as degree, leading coefficient, and the division algorithm. They explain roots, divisibility, and how to find the gcd of polynomials using Euclid's Algorithm.

Quiz #8 Question 1 Brief Go Over
Let $H =< (2,1) > \subseteq \mathbb{Z}_3 \times \mathbb{Z}_3$
$H = \{(0,0),(2,1),(1,2)\}$
$\mathbb{Z}_3 \times \mathbb{Z}_3 / < (2,1) >=$ group of all cosets of H
What are the cosets?
1 coset is $H = \{(0,0),(2,1),(1,2)\}$
and another is $(1,1) + H = \{(1,1),(0,2),(2,0)\}$
$(1,0) + H = \{(1,0),(0,1),(2,2)\}$

	$(0,0)+H$	$(1,1)+H$	$(1,0)+H$
$(0,0)+H$	$(0,0)$	$(1,1)$	$(1,0)$
$(1,1)+H$	$(1,1)$	$(1,0)$	$(0,0)$

Polynomials with coefficients in a field F are denoted F[x]. These polynomials obey all the usual rules for polynomials.

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

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. $f(x) = \mathbb{Q}[x]$
$f(x) = \frac{2}{3}x^5 + \frac{1}{2}x + 2$ has degree 5 and leading coefficient $\frac{2}{3}$.

The 0 polynomial doesn't have a degree, but for convenience we sometimes define it to have degree $-\infty$.

Theorem. 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 $f(x), g(x)$ are not 0 then $f(x) = a_m x^m + ...$ where $a_m \neq 0$ and $g(x) = b_n x^n + ...$ 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. The division algorithm applies to polynomials just like the integers.
Recall for integers: If $a, b \neq 0, b > 0$ then we can find q and r so that $a = bq + r$ and $0 \leq r < b$.

Analogous Statement for polynomials. 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 that the degree of $g(x)$
$(deg(r(x)) < deg(g(x))$ furthermore these polynomials $q(x)$ and $r(x)$ are unique.

Proof. Do long division of polynomials. $f(x) = a_m x^m + ...$ and $g(x) = b_n x^n + ...$
Note that $f(x) - \frac{a_m}{b_n} x^{m-n} g(x)$ has degree less than m so we can use induction on the degrees of the polynomials to show that the division algorithm works. □

If the remainder when $f(x)$ is divided by $g(x)$ is zero we say that $g(x)$ divides $f(x)$ and write $g(x)|f(x)$.

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

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

Proof. By the division algorithm we can find $q(x)$ and $r(x)$ with $F(x) = q(x)(x - \alpha) + r(x)$ and $deg(r(x)) < deg(x - \alpha) = 1$ so $r(x) = c \in F[x]$ and $f(x) = q(x)(x - \alpha) + c$. Plug in α to both sides. $f(\alpha) = q(x)(\alpha - \alpha) + c$ so $0 = 0 + c$ so $c = 0$. Since our remainder is 0, $(x - \alpha$ divides $f(x)$. □

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

Definition. 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 $d(x)|g(x)$, 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. Th 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 $q(x)f(x) + b(x)g(x) \in I$
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. Then there exists a monic polynomial $d(x) \in F[x]$ such that $I = \{a(x)d(x)|a(x) \in F[x]\}$
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 $d(x)$.
Proof by contradiction:
Suppose $g(x) \in I$ is not divisible by $d(x)$. Use the division algorithm to write $g(x) = q(x)d(x) + r(x)$ where $deg(r) < deg(d), r(x) = g(x) - q(x)d(x)$. So $r(x) \in I$ $r(x) \neq 0$ since $d(x) \not| g(x)$, 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 this I is the set of all multiples of some polynomial $d(x)$. This $d(x)$ is the gcd of $f(x), g(x)$. □

Definition. 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 the gcd.
Steps:
1. Repeatedly divide with the remainder
2. Pull out leading coefficient of remainder
3. Repeat until we get a remainder of 0
4. Last nonzero remainder is our gcd