Lecture 38

1 Polynomial Rings

1.1 Notation and Terminology

Definition 1.1 (Ring of Polynomials over R)**.** Let R be a commutative ring.

$$R[x] = \{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \mid a_i \in R,\ n \in \mathbb{Z}_{>0}\}$$

is called the ring of polynomials over R in the indeterminate x.

Addition and multiplication are as usual.

$$f = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

If $a_n \neq 0$, then $\deg(f) = n$ and a_n is called the leading coefficient of f.

If $a_n \neq 0$ is the multiplicative identity of R, then f is called a monic polynomial.

a_0 is called the constant term of f.

If $f(x) = a_0$ then f is called a constant polynomial.

Theorem 1.1. If D is an integral domain, then $D[x]$ is an integral domain.

Proof. $f(x) = a_n x^n + \underbrace{\cdots}_{\text{lower degree}}$, $g(x) = a_m x^m + \underbrace{\cdots}_{\text{lower degree}}$, $a_n^{\neq 0}, a_m^{\neq 0} \in D$

$f(x) \cdot g(x) = (a_n \cdot a_m)x^{m+n} + \underbrace{\cdots}_{\text{lower degree}}$

D integral domain $\implies a_n \cdot a_m \neq 0 \implies f(x) \cdot g(x) \neq 0$ since the leading term is nonzero. □

Theorem 1.2 (Division Algorithm for $F[x]$)**.** Let F be a field and $f(x), g(x) \in F[x]$ with $g(x) \neq 0$. Then there exists unique polynomials $q(x)$ and $r(x)$ in $F[x]$ such that

$$f(x) = q(x)g(x) + r(x) \quad \text{and} \quad \text{either } r(x) = 0 \text{ or } \deg r(x) < \deg g(x)$$

***Pf sketch*.**

- May assume $g(x)$ is monic (F = field).

  Say $g = x^n + a_{n-1}x^{n-1} + \cdots$

- use x^n to "cancel" terms in $f(x)$

  $f(x) = b_m x^m + \cdots$ with $m \geq n$

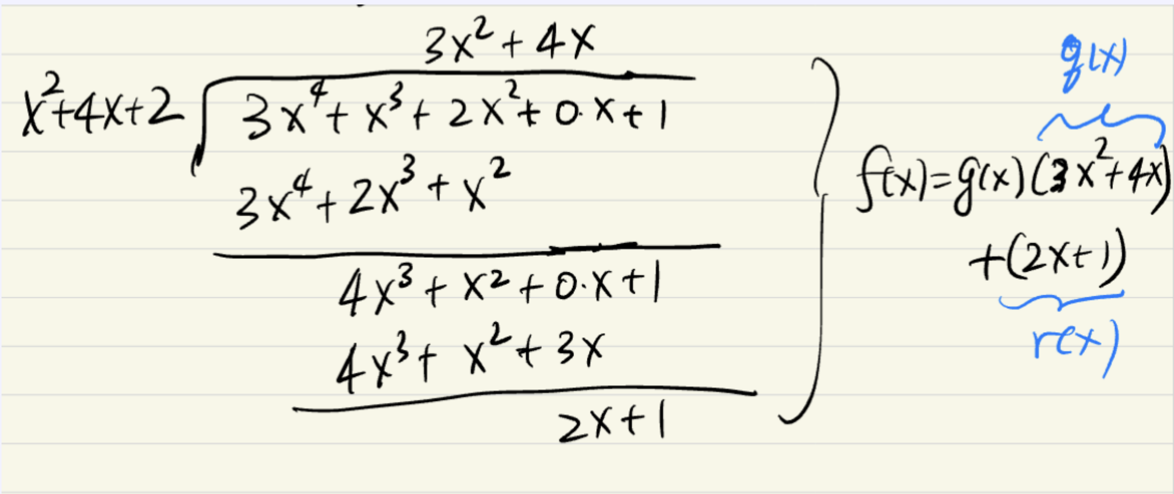
  $f(x) - b_m x^{m-n} \cdot g(x) =$ polynomial of degree $< m$

  Then proceed by induction on degree.

□

Example 1.1. In $\mathbb{Z}_5[x]$,

$$f(x) = 3x^4 + x^3 + 2x^2 + 1$$
$$g(x) = x^2 + 4x + 2$$



Corollary 1.2.1 (Remainder Theorem)**.** Let F be a field and $f(x) \in F[x]$. THen a is a zero of $f(x)$ $\iff$ $x - a$ is a factor of $f(x)$

Proof. $f(x) = (x - a)q(x) + r$ (where r is a constant)

$$\begin{aligned} a \text{ is a zero of } f \iff & f(a) = 0 \iff r = 0 \\ \iff & f(x) = (x-a)q(x) \\ \iff & (x-a) \text{ is a factor of } f \end{aligned}$$

□

Corollary 1.2.2 (Factor Theorem)**.** A polynomial of degree n over a field has at most n zeros counting multiplicity.

Pf sketch. use Cor 16.2.1 □

Example 1.2. Every polynomial in $\mathbb{C}[x]$ of deg n has exactly n zeros counting multiplicity.

Cor is not true for arbitrary polynomial rings.

Example 1.3. $x^2 + 3x + 2$ in $\mathbb{Z}_6[x]$ has <u>four</u> zeros in $\mathbb{Z}_6$ (1, 2, 4, 5).

Definition 1.2 (Principal Ideal Domain (PID))**.** A <u>principal ideal domain (PID)</u> is an integral domain R such that every ideal has the form $\langle a \rangle = \{ra \mid r \in R\}$ for some $a \in R$

Theorem 1.3. For any field F, $F[x]$ is a PID.

Proof. Let I be an ideal in $F[x]$.

Assume $I \neq \{0\} = \langle 0 \rangle$

Let g be a polynomial in I that has minimum degree.

Then $I = \langle g(x) \rangle$ by the division algorithm $\square$

Theorem 1.4. $\mathbb{Z}$ is a PID.

Example 1.4. $\mathbb{Z}$[x] is *not* a PID. (e.g. $\langle x, 2 \rangle$ is not principal)