

## Polynomials

## Remarks

- ① Office hours today: by appointment only
- ② HW: by end of today, next HW will be posted.  
2 HW's combined: due next week

## Polynomials

## ① Division algorithm

for integers: if  $p, s$  are non-negative integers  
 $s \neq 0$

then  $\exists!$  non-negative integers  $r, q$  s.t.

Ⓐ  $p = q \cdot s + r$  and

Ⓑ  $0 \leq r < s$

("q": quotient, "r": remainder).

We want the same for polynomials

example) suppose  $p = x^3 + 1$ ,  $s = x^2 + 1$

divide  $p$  by  $s$ , find  $q, r$ .

Soln

19 Oct 2020  
Lecture #20

2

$$\begin{array}{r} x \\ x^2 + 1 \overline{) x^3 + 1} \\ \underline{-(x^3 + x)} \phantom{1} \\ -x + 1 \end{array}$$

have:

$$\begin{array}{ccccccc} x^3 + 1 & = & x \cdot & (x^2 + 1) & + & (-x + 1) \\ \text{"} & & \text{"} & \text{"} & & \text{"} \\ P & & q & s & & r \end{array}$$

Division algorithm

theorem Suppose  $p, s \in P(F)$ ,  $s \neq 0$ .

then  $\exists!$  polynomials  $q, r \in P(F)$  s.t.

(a)  $P(x) = q(x)s(x) + r(x)$

(b)  $\deg r < \deg s$ .

cool proof from Axler Let  $n = \deg p$   
 $m = \deg s$ .

if  $m > n$ , then  $q(x) = 0$   
 $r(x) = p(x)$  is the only solution

$\therefore$  assume  $m \leq n$ .

define  $\dim : (n-m+1) + m = n+1$

$$T : \underbrace{P_{n-m}(\mathbb{F}) \times P_{m-1}(\mathbb{F})}_{\dim = n+1} \longrightarrow P_n(\mathbb{F}) \stackrel{\dim = n+1}{=} P(x)$$

$$T(q(x), r(x)) = s(x)q(x) + r(x)$$

in breakout rooms:

(a) T is linear? yes it is.

(b) ker T? im T?

$$\ker T = \left\{ (q(x), r(x)) : \underbrace{s(x)q(x)}_{\substack{\text{degree} \\ \geq m}} + \underbrace{r(x)}_{\substack{\text{deg} \\ \leq m-1}} = 0 \right\} = \{0\}$$

$\therefore T$  is an isomorphism  
 $\therefore$  surjective.

$\hookrightarrow q(x) = 0$   
 $\therefore r(x) = 0$

$\therefore \exists! (q(x), r(x)) \in P_{n-m}(\mathbb{F}) \times P_{m-1}(\mathbb{F})$  s.t.  
 $\int P(x) = s(x)q(x) + r(x)$

T is inj + surj!

# Roots (Zeros) of polynomials

19 Oct 2020  
Lecture #20

4

## Proposition

Suppose  $p(x) \in \mathcal{P}(F)$ , and  $\lambda \in F$ .

then

$$p(\lambda) = 0 \iff p(x) = (x - \lambda)q(x)$$

(in  $F$ ) for some  $q(x)$ .

## Proof

$\Leftarrow$  this direction is immediate.

$\Rightarrow$  divide  $p(x)$  by  $x - \lambda$ .  $= s(x)$   $\deg s = 1$

get  $\exists!$   $q(x), r(x)$  s.t.

- $p(x) = (x - \lambda)q(x) + r(x)$

- $\deg r(x) \leq 0$

ie:  $r(x) = \text{constant}$ , or  $0$   
 $= r$

plug in  $x = \lambda$ :

$$p(\lambda) = (\lambda - \lambda)q(\lambda) + r$$

"

0

(hypothesis)

"

0 + r

$$\therefore r = 0$$

$$\therefore p(x) = (x - \lambda)q(x)$$

**Corollary** For any field  $\mathbb{F}$ ,

if  $m = \deg p(x) \geq 0$  (ie:  $p(x)$  not identically 0)

then # zeros of  $p(x) \leq \deg p(x) = m$ .

$$\# \{ \lambda \in \mathbb{F} : p(\lambda) = 0 \}$$

**proof** induction on  $m = \deg p(x)$ .

if  $m = 0$ , then  $p(x) = a \neq 0$

has no roots:  
# zeros  $\leq 0$  ✓

suppose statement is true for

$\deg = m-1$ , show true for  $m$ .

consider  $p(x)$  of degree  $m$ .

suppose  $\lambda$  is a zero.

$$\therefore p(x) = (x - \lambda)q(x) \quad \deg q(x) = m-1$$

$$\therefore \text{zeros of } p = \{ \lambda \} \cup \{ \text{zeros of } q(x) \}$$

$$\therefore \# \text{ zeros of } p \leq 1 + m-1 = m$$

# Fundamental theorem of Algebra

19 Oct 2020

Lecture #20

6

Every non-zero polynomial in  $\mathbb{P}(\mathbb{C})$  has a zero.

proof in an analysis class.

we will assume this, but not prove it.

if  $p(x)$  has degree 2 : quadratic formula

3 :  $\exists$  formula

4 :  $\exists$  bigger mess  
of a formula.

Galois : proved, while he was a teenager,  
that there is no formula in degree 5 or higher

---

Corollary if  $p(x) \in \mathbb{P}(\mathbb{C})$ , then  $\exists ! \lambda_1, \lambda_2, \dots, \lambda_m \in \mathbb{C}$   
of degree  $m$  (up to ordering)

st.

$a \in \mathbb{C}$

$$p(x) = a(x - \lambda_1)(x - \lambda_2) \dots (x - \lambda_m).$$

(unique up to order of the factors.

proof (see Axler pg. 125, FIS appendix D.)