## Math 128B, Mon Feb 22

- Use a laptop or desktop with a large screen so you can read these words clearly.
- In general, please turn off your camera and mute yourself.
- Exception: When we do groupwork, please turn both your camera and mic on. (Groupwork will not be recorded.)
- Please always have the chat window open to ask questions.

▲□▶ ▲□▶ ▲□▶ ▲□▶ ■ ●の00

- Reading for today: Ch. 16. For next Mon: Ch. 17.
- PS03 due tonight.
- Exam review tonight, 4–5pm, on Zoom (use office hour/problem session link).
- Exam 1 on Wed Feb 24.

True/false/justify problems

Given a statement:

If true, write TRUE for full credit.

If false, write FALSE and then justify as specifically as possible, which often means coming up with a counterexample.

Example:

True or false: Every element of Z is a unit.

FALSE: 2 is not a unit in Z because 2x = 1 has no solutions in Z.

Polynomials with coefficients in a ring R

# comm

Let R be a ring. We define the ring R[x], the ring of polynomials with coefficients in R, as follows.

Set: All expressions of the form

$$\sum_{i=1}^{n} a_i x^i = a_n x^n + a_{n-1} x^{n-1} + \dots + a_2 x^2 + a_1 x + a_0,$$
  
and x is an "indeterminate",  
i.e., a symbol, not a var,

where each  $a_i$  is an element of the ring R.

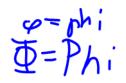
Addition and multiplication: in R[x] are each defined to work like addition and multiplication of polynomials with real coefficients, except that all coefficient arithmetic is performed in the ring R.

ample Take  $\mathbb{P}_{q}$   $\mathbb{P}_{x}$   $\mathbb{P}_{x}$ Example ring of coefficients f(x) + q(x) $= 3 x^{3} + (3+6) \sqrt{2} + (5+4) x + (2+1)$ = 3x3+2x+2x+3 3x2+3x2+5x+2 6×+4×+1

5x4+5x3+6x2+x 45+4++22+5x2 +6x+2  $4x^{5}+7x^{4}+3x^{3}$  $\langle f(x) \rangle = \langle p(x) + bx \rangle \left( p(x) + \mathcal{U}_{1}(x) \right)$ 

# The substitution-reduction homomorphim

R, S commutative rings.



Suppose  $\varphi : R \to S$  is a homomorphism, and  $\alpha \in S$ . Define  $\Phi : R[x] \to S$  for  $p(x) = a_n x^n + \cdots + a_1 x + a_0$ by the formula  $\Phi(p(x)) = \overline{p}(\alpha)$ , where  $\overline{p}(x) = \varphi(a_n)x^n + \cdots + \varphi(a_1)x + \varphi(a_0)$ . I.e., apply  $\Phi$  by reducing the coefficients of p(x) by the homomorphism  $\varphi$  and plugging in  $\alpha$ .

### Theorem

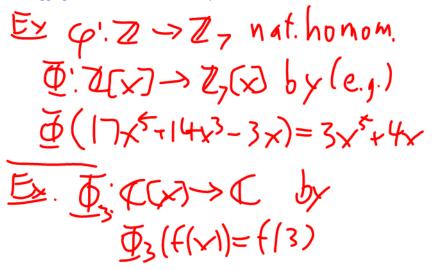
The above map  $\Phi$  is a homomorphism. I.e., substitution is a homomorphism, and reduction of coefficients is also a homomorphism.

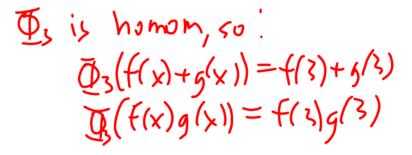
**Idea of proof:** Since the operations of R[x] are what is required by the distributive law, those operations end up being preserved when applied to elements of S.

Points:

\* Reducing coefficients is a homomorphism

\* Plugging in elements is a homomorphism.





I.e.: Plugging in is a homomorphism.

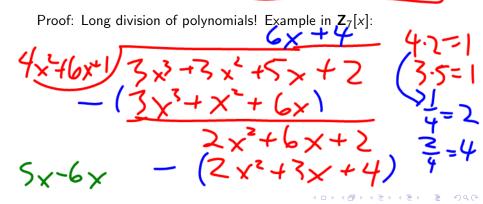
A key property of F[x]: Division with remainder

#### Theorem

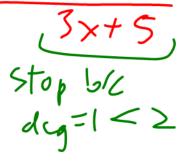
Let F be a field, and let a(x) and d(x) be polynomials in F[x] with  $d(x) \neq 0$ . There exist unique  $q(x), r(x) \in F[x]$  such that

$$a(x) = d(x)q(x) + r(x),$$

with  $\deg(r(x)) < \deg(d(x))$ .



--X 6X 2-4=7 =5



## Consequences of long division

### Corollary (Remainder Theorem)

Let F be a field, let  $f(x) \in F[x]$  be a polynomial, and let  $\alpha$  be an element of F. When we divide f(x) by  $(x - \alpha)$ , the remainder is a constant, namely  $r = f(\alpha)$  (the element of F obtained by substituting  $\alpha$  for x in f(x)).

### Corollary (Factor Theorem)

Let F be a field,  $f(x) \in F[x]$ , and  $\alpha \in F$ . Then  $(x - \alpha)$  divides f(x) (i.e., with a remainder of 0) exactly when  $f(\alpha) = 0$ .

#### Theorem (Degree n has <= n zeros)

Let F be a field and let  $f(x) \in F[x]$  be a polynomial of degree  $n \ge 1$ . Then f(x) has at most n distinct zeros in F, i.e., there are at most n distinct elements  $\alpha \in F$  such that  $f(\alpha) = 0$ .

PF Rem (EF[x] aFF Dirfby (x-2). f(x) = q(x)(x - a) + r(x)Plug 2(homon): degr<1 f(z) = q(z)(z - z) + r()=r

Ex. 4x2+bx+1 6 2, [v] Dues (x-5) div f(x)? Ans ((5)=4(5)+6(5)+1 -24(4)+6(5)+1 =み4241=5 No: f(x)=q(x)(x-5)+5. A= (x-S); then in Z, [x]/A 4x2+6x+1+A=5+A. (Z,C+)/A:5Z,(x)~/x=s)

Consequences of long division  $\langle \times 4 - 4 \rangle + 7 \rangle$ **Q**: What are the elements of  $\mathbf{R}[x]/\langle x^4 + x^2 - x + 1 \rangle$ ? **A:** Let  $A = \langle x^4 + 2x^2 - 4x + 7 \rangle$ . Claim: Every element of Red can be represented uniquely as -RIVA p(x) + A, where deg  $p(x) \le 3$ . -4(x)+A( Agy 4 + A 4 + 2 + 2 + 4 + 7 + r(x)= q(x)(x)dir Wrenninder hult dry4-22-4-47,50 in A = r(x) + AUnig of dir =)r uniqu

Another method for r(x): ModA means setting ~4+2~2-4~+7=0 (mod A)  $4 = -2x^{2} + 4x - 7$  (mod A)

Applying this repeatedly allows us to reduce any poly of degree  $\geq 4$  to a polynomial of degree  $\leq 3$ . (This is equivalent to long division by  $x^4 + 2x^2 - 4x + 7$ , paying attention only to remainders.)

In general, working in F[x]/(p(x)), with A =(p(x)), we can get unique coset representatives r(x)+A for every element of F[x]/A, if we take deg  $r(x) < \deg p(x)$ .

# F[x] is a PID

### Definition

A **principal ideal domain** is an integral domain *R* in which every ideal has the form  $\langle a \rangle = \{ra \mid r \in R\}$  for some  $a \in R$ .

Non-example:  $\langle x, 2 \rangle$  in **Z**[x] can't be generated by a single element.

▲□▶ ▲□▶ ▲□▶ ▲□▶ ■ ●の00

Theorem If F is a field, then F[x] is a PID.

Finding a generator of an ideal of F[x]

#### Theorem

F a field, I a nonzero ideal of F[x],  $g(x) \in I$ . Then  $I = \langle g(x) \rangle$  exactly when g(x) is a nonzero polynomial of smallest possible degree in I.