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.
- 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

$$\sum_{i=1}^{n} a_i x^i = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0,$$

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.

Example

Take R be $\mathbb{Z}_7[x]$.

ring of coefficients

$f(x) = 3x^3+3x^2+5x+2$

$g(x) = 6x^2+4x+1$

elements of R

$$f(x)+g(x) = 3x^3+(3+6)x^2+(5+4)x+(2+1)$$
$$= 3x^3+2x^2+2x+3$$

$$\begin{array}{r} 3x^3+3x^2+5x+2 \\ 6x^2+4x+1 \\ \hline 3x^3+3x^2+5x+2 \end{array}$$

$$5x^4+5x^3+6x^2+x$$

$$4x^5+4x^4+2x^3+5x^2$$

$$4x^5+2x^4+3x^3 \qquad +6x+2$$

$$\langle f(x)\rangle = \{p(x)f(x) \mid p(x)\in\mathbb{Z}_7[x]\}$$

The substitution-reduction homomorphim

$\varphi = $ phi
$\Phi = $ Phi

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 Φ by reducing the coefficients of $p(x)$ by the homomorphism φ and plugging in α.

Theorem

The above map Φ 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.

Ex $\varphi: \mathbb{Z} \to \mathbb{Z}_7$ nat. homom.

$\Phi: \mathbb{Z}[x] \to \mathbb{Z}_7[x]$ by (e.g.)

$\Phi(17x^5 + 14x^3 - 3x) = 3x^5 + 4x$

Ex. $\Phi_3: \mathbb{C}[x] \to \mathbb{C}$ by

$\Phi_3(f(x)) = f(3)$

Φ_3 is homom, so:

$$\Phi_3(f(x)+g(x)) = f(3)+g(3)$$

$$\Phi_3(f(x)g(x)) = f(3)g(3)$$

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

$$a(x) = d(x)q(x) + r(x), \qquad \boxed{\text{with } \deg(r(x)) < \deg(d(x)).}$$

Proof: Long division of polynomials! Example in $\mathbf{Z}_7[x]$:

$$
\begin{array}{r|l}
 & 6x + 4 \\
\hline
4x^2+6x+1 & 3x^3 + 3x^2 + 5x + 2 \\
 & -(3x^3 + x^2 + 6x) \\
\hline
 & 2x^2 + 6x + 2 \\
 & -(2x^2 + 3x + 4)
\end{array}
$$

$5x - 6x$

$4 \cdot 2 = 1$

$3 \cdot 5 = 1$

$\frac{1}{4} = 2$

$\frac{3}{4} = 4$

$= -x$

$= 6x$

$2 \cdot 4 = -2$

$= 5$

$\underbrace{3x+5}$

stop b/c

deg $= 1 < 2$

Consequences of long division

Corollary (Remainder Theorem)

Let F be a field, let $f(x) \in F[x]$ be a polynomial, and let α 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 α 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 $n \geq 1$. 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 $f \in F[x]$ $\alpha \in F$

Div f by $(x-\alpha)$:

$$f(x) = q(x)(x-\alpha) + \underbrace{r(x)}_{\substack{\deg r < 1 \\ \text{so } r \text{ const.}}}$$

Plug α (homom):

$$f(\alpha) = q(\alpha)\underbrace{(\alpha - \alpha)}_{=0} + r$$

$$f(\alpha) = r$$

__Ex:__ $f(x)=4x^2+6x+1 \in \mathbb{Z}_7[x]$

Does $(x-5)$ div $f(x)$?

__Ans:__ $f(5)=4(5^2)+6(5)+1$

$=4(4)+6(5)+1$

$=2+2+1=5$

No: $f(x)=q(x)(x-5)+5$.

$A=\langle (x-5)\rangle$; then in $\mathbb{Z}_7[x]/A$,

$4x^2+6x+1+A=5+A$.

$(\mathbb{Z}_7[x]/A$ is $\mathbb{Z}_7[x]$ w/ $x=5)$

Consequences of long division $\langle x^4+2x^2-4x+7\rangle$

Q: What are the elements of $\mathbf{R}[x]/\langle \cancel{x^4+x^2-x+1}\rangle$?

A: Let $A=\langle x^4+2x^2-4x+7\rangle$.
Claim: Every element of ~~R/A~~ $R[x]/A$ can be represented uniquely as $p(x)+A$, where $\deg p(x)\le 3$.

Pf

$$f(x)+A$$

$$= \underbrace{q(x)(\overbrace{x^4+2x^2-4x+7}^{\deg 4})+\overbrace{r(x)}^{\deg\le 3}}_{\text{div w/remainder}}+A$$

mult of x^4+2x^2-4x+7, so in A

$$= r(x)+A$$

Uniq of div $\Rightarrow$ r unique

Another method for $r(x)$:

Mod A means setting

$$x^4 + 2x^2 - 4x + 7 = 0 \pmod{A}$$

$$x^4 = -2x^2 + 4x - 7 \pmod{A}$$

Applying this repeatedly allows us to reduce any poly of degree >= 4 to a polynomial of degree <= 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 $\mathbf{Z}[x]$ can't be generated by a single element.

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.