Math 127, Wed Feb 17

- 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: 3.6, 4.1; reading for Mon: 4.2–4.3.
- PS03 outline due tonight, full version due Mon Feb 22.
- Next problem session Fri Feb 19, 10:00–noon on Zoom.
- **Exam 1 now on Wed Feb 24**, in one week.

Hand out review and sample. . . .

Mechanics of in-class exam in one week

* Exam will be proctored by Zoom
* Cameras on and mic **ON**
  (If background noise bothers you, turn off speakers)
* Exam handed out over chat
* Camera starts on face, moves to hands
* Write on your own paper, one problem per page
* Turned in on Gradescope as a HW assignment
* 65 min work time, 10 min scan time
* Have to stay until scan time -- have something analog to read if you finish early.

Recap: A meta-principle; polynomial GCDs

Let F be a field, and let $f(x), g(x), d(x) \in F[x]$ be polynomials with coefficients in F.

> The ring $F[x]$ works just like the ring of ordinary integers, except replacing the integer Division Theorem with the Division Theorem for Polynomials.

Definition

To say that $d(x)$ **divides** $f(x)$ in $F[x]$ means that $f(x) = q(x)d(x)$ for some $q(x) \in F[x]$. Similarly, to say that $d(x)$ is a **common divisor** of $f(x)$ and $g(x)$ means that $d(x)$ divides both $f(x)$ and $g(x)$.

Definition

To say that $d(x) \in F[x]$ is a **greatest common divisor** of $f(x)$ and $g(x)$ means that $d(x)$ is a common divisor of $f(x)$ and $g(x)$ of highest possible degree.

Note: $\gcd(f(x), g(x))$ only up to nonzero constant multiple.

The Polynomial Euclidean Algorithm

Let $r_{-1}(x) = a(x)$, $r_0(x) = b(x)$. To calculate $\gcd(a(x), b(x))$:

$$
\begin{aligned}
r_{-1}(x) &= q_1(x) r_0(x) + r_1(x) & \quad (\deg r_1 < \deg r_0) \\
r_0(x) &= q_2(x) r_1(x) + r_2(x) & \quad (\deg r_2 < \deg r_1) \\
r_1(x) &= q_3(x) r_2(x) + r_3(x) & \quad (\deg r_3 < \deg r_2) \\
&\vdots \\
r_{N-4}(x) &= q_{N-2}(x) r_{N-3}(x) + r_{N-2}(x) & \quad (\deg r_{N-2} < \deg r_{N-3}) \\
r_{N-3}(x) &= q_{N-1}(x) r_{N-2}(x) + r_{N-1}(x) & \quad (\deg r_{N-1} < \deg r_{N-2}) \\
r_{N-2}(x) &= q_N(x) r_{N-1}(x)
\end{aligned}
$$

gcd(a(x), b(x))

Example

Find $\gcd(x^4+4x^3+3x^2+4x+2,\ x^3+4x^2+2x+2)$ in $\mathbf{F}_5[x]$.

mod 5

#1

deg 3

$b(x)$: x^3+4x^2+2x+2

$a(x)$: $x^4+4x^3+3x^2+4x+2$

$$
\begin{array}{r}
x \\
x^3+4x^2+2x+2\ \big)\ \overline{x^4+4x^3+3x^2+4x+2} \\
x^4+4x^3+2x^2+2x \\
\hline
x^2+2x+2
\end{array}
$$

deg 2 < 3

#2

$$
\begin{array}{r}
x+2 \\
x^2+2x+2\ \big)\ \overline{x^3+4x^2+2x+2} \\
x^3+2x^2+2x \\
\hline
2x^2 \qquad +2 \\
2x^2+4x+4
\end{array}
$$

pick 2 to cancel

highest Term

$x+3$ ← mod 5

← deg 1 < 2

$$
\begin{array}{r}
x + 4 \\
x+3 \overline{\smash{)}\, x^2+2x+2} \\
\underline{x^2+3x} \\
4x+2 \\
\underline{4x+2} \\
0
\end{array}
$$

mod 5

Last nonzero:

$\boxed{x+3} = \gcd(a(x), b(x))$

$\boxed{\text{Is } x \text{ a unit in } \mathbb{F}_5[x]?}$

Well: If $f(x) \in \mathbb{F}_5[x]$, $f(x) \neq 0$,

$\deg(x f(x))$

$= \deg x + \deg f$

$= 1 + \deg f > 0$

So $x f(x) \neq 1$.

$\Rightarrow x$ not unit in $\mathbb{F}_5[x]$.

Polynomial Bezout's identity

Just as with integers:

Theorem

Let F be a field, and let $a(x), b(x) \in F[x]$ be polynomials with coefficients in F. The equation

$$a(x)f(x) + b(x)g(x) = \gcd(a(x), b(x))$$

has a solution $f(x), g(x) \in F[x]$.

Corollary

Let F be a field, and let $a(x), b(x), c(x) \in F[x]$ be nonzero polynomials with coefficients in F. The equation

$$a(x)f(x) + b(x)g(x) = c(x)$$

has a solution $f(x), g(x) \in F[x]$ if and only if $\gcd(a(x), b(x))$ divides $c(x)$.

Polynomial Bezout, in calculation form

Again let $r_{-1}(x) = a(x)$, $r_0(x) = b(x)$. To solve $a(x)f(x) + b(x)g(x) = \gcd(a(x), b(x))$ for f, g:

Solve for rems

$$\begin{aligned}
r_1(x) &= r_{-1}(x) - q_1(x)r_0(x) \\
r_2(x) &= r_0(x) - q_2(x)r_1(x) \\
r_3(x) &= r_1(x) - q_3(x)r_2(x) \\
&\vdots \\
r_{N-3}(x) &= r_{N-5}(x) - q_{N-3}(x)r_{N-4}(x) \\
r_{N-2}(x) &= r_{N-4}(x) - q_{N-2}(x)r_{N-3}(x) \\
r_{N-1}(x) &= r_{N-3}(x) - q_{N-1}(x)r_{N-2}(x)
\end{aligned}$$

This is again called **Euclidean rewriting**.

Example

Let $a(x) = x^4 + 4x^3 + 3x^2 + 4x + 2$, $b(x) = x^3 + 4x^2 + 2x + 2$ in $\mathbf{F}_5[x]$.

Solve $a(x)f(x) + b(x)g(x) = \gcd(a(x), b(x))$ for f, g:

$$a(x) = x\,b(x) + (x^2+2x+2) \quad (1)$$

$$b(x) = (x+2)(x^2+2x+2) + (x+3) \quad (2)$$

gcd

$$x^2+2x+2 = a(x) - x\,b(x) \quad (1)$$

$$x+3 = b(x) - (x+2)(x^2+2x+2) \quad (2)$$

$$= b(x) - (x+2)(a(x) - x\,b(x))$$

$$= b(x) - (x+2)a(x) + (x^2+2x)b(x)$$

$$= (x^2+2x+1)b(x) - (x+2)a(x)$$

$$\|$$

$$\boxed{x+3}$$

END MATERIAL THAT IS FAIR GAME FOR EXAM 1

What is the point of abstraction?

Abstraction $\Rightarrow$ Simplification $\Rightarrow$ Generalization $\Rightarrow$ Power

- **Abstraction:** Replace specific objects with more general ones defined by axioms.
- **Simplification:** Reduce ideas to their axiomatic essentials.
- **Generalization:** The abstract version may apply to new examples.
- **Power:** Whatever we can solve/prove in general applies to the new examples as well.

Definition of ring (finally!)

A **ring** is a set R and binary operations $+$ and $\cdot$ on R s.t.:

- (*+ associative*) For any $a, b, c \in R$, $(a+b)+c = a+(b+c)$.
- (*+ commutative*) For any $a, b \in R$, $a+b = b+a$.
- (*Zero*) There exists some $0 \in R$ such that for all $a \in R$, $0+a = a = a+0$.
- (*Negatives*) For every $a \in R$, there exists some $-a \in R$ such that $(-a)+a = 0 = a+(-a)$.
- (*· associative*) For any $a, b, c \in R$, $(ab)c = a(bc)$.
- (*· commutative*) For any $a, b \in R$, $ab = ba$.
- (*One*) There exists some $1 \in R$ such that for all $a \in R$, $1a = a = a1$.
- (*Distributive*) For any $a, b, c \in R$, $a(b+c) = ab+ac$ and $(a+b)c = ac+bc$.

We also define $a - b$ to be an abbreviation for $a + (-b)$.

+

·

Examples (review)

can't divide in $\mathbb{Z}$.

- $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{C}$, $\mathbf{R}$ (integers, rationals, complexes, reals)
- Polynomials $R[x]$ (R any ring)
- $\mathbf{Z}/(m)$. Special case: $\mathbf{F}_p$ for p prime.

$$\parallel$$

$$\mathbb{Z}/(p)$$

Point: Since each of these structures satisfies the axioms of a ring, we can use the usual manipulations of HS algebra inside each of these structures.
I.e., to say that R is a ring <=> HS algebra works in R.
(Except division, perhaps.)

Domains, inverses, units, fields

Definition

To say that a ring R is a **domain** (or sometimes, an **integral domain**) means that if $a, b \in R$ and $ab = 0$, then either $a = 0$ or $b = 0$.

Definition

Let R be a ring. For $a \in R$, an **inverse of** a is some $b \in R$ such that $ab = 1$. Since an element can have only one inverse, we use a^{-1} to denote *the* inverse of a. To say that a is a **unit** in R means that a has an inverse in R.

Definition

A **field** is a ring R in which every nonzero element is a unit and $1 \neq 0$. In other words, to say that a nonzero ring R is a field means that for every $a \neq 0$ in R, there exists some $b \in R$ such that $ab = 1$.

Some helpful facts we saw before, restated

Corollary

If R is a domain and $f(x), g(x) \in R[x]$, then

$$\deg(f(x)g(x)) = \deg(f(x)) + \deg(g(x)),$$

where $-\infty$ plus anything is $-\infty$.

Theorem

If F is a field, then F is a domain.

Not every ring is a domain; not every domain is a field

Examples/diagram: