Math 128B, Mon Mar 08

- 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 and Wed: Ch. 18.
- PS04 due tonight; PS05 outline due Wed Mar 10.
- Problem session Fri Mar 12, 10am–noon.

WWW
tonight

Counting is never (just) about formulas; it's about stories. $F_p = \mathbb{Z}_p$

(a) Formula for # of irreducible polynomials of form x^2+bx+c in F_p[x].

(b) How many polynomials are there of form (x-a)(x^2+bx+c), where x^2+bx+c is irreducible?

Better Q: How can you choose a polynomial of form (x-a)(x^2+bx+c), where x^2+bx+c is irreducible?

1. Choose $(x-a)$, $a \in \mathbb{Z}_p$. p choices

2. Chose (x^2+bx+c) irr ×
(Assume list of ↗) part (a) choices

$$\overline{}$$
= # poss.

$\underline{p=3}$: $x-0, x-1, x-2$

Constructing new fields

Theorem

F a field, $p(x) \in F[x]$. Then TFAE:

1. $\langle p(x) \rangle$ *maximal*
2. $p(x)$ *irreducible*

Cor: $F[x]/\langle p(x) \rangle$ is a field iff $p(x)$ irreducible.

Proof of thm: Last time $1 \Rightarrow 2$.

$\boxed{2 \Rightarrow 1}$ (A) $p(x)$ irred

S'pose $\langle p(x) \rangle \subset I \subseteq F[x]$ ideals.

(A) $r(x) \in I$, $r(x) \notin \langle p(x) \rangle$

$\rightarrow p$ doesn't div r. ✱

B/c $F[x]$ is PID, $\langle p, a\rangle = \langle d\rangle$

So $d \in \langle p, a\rangle$, and d divs p, a.

p irr $\Rightarrow$ $d = up$ or u for some unit u

If $d = up$, up divs a; contra ✗.

So $d = u \Rightarrow \langle d\rangle = F[x]$

But $\langle d\rangle \subseteq I$ so:

(✓) $I = F[x]$

(c) $\langle p(x)\rangle$ max in $F[x]$.

We really showed

If D is PID, TFAE

1. $\langle p \rangle$ max
2. p irred.

D domain, $a \in D$; TFAE

a unit $\iff \langle a \rangle = D$

Irreducibles are prime in $F[x]$

Thm: If $p(x)$ irred and $p(x)$ divides $a(x)b(x)$, then either $p(x)$ divides $a(x)$ or $p(x)$ divides $b(x)$.
Proof: Suppose $p(x)$ irred, $p(x)$ divides $a(x)b(x)$, and $p(x)$ doesn't divide $a(x)$. Then

$$\langle p(x)\rangle \subseteq \langle p(x), a(x)\rangle =$$

in gen'l later

Example: A field of order 49 $= 7^2$.

Take

$\mathbb{Z}_7[x]/\langle p(x)\rangle$

deg $= 2$, $p(x)$ irred.

B/c deg 2, p irr $\Leftrightarrow$ no zeros.

Take

$p(x) = x^2 - a$ $\quad p(x) = 0$ no sol'ns

$x^2 = a$ no sol'ns

Squares in $\mathbb{Z}_7$: 1, 4, 2; 3 nonsquare

So $\mathbb{Z}_7[x]/\langle x^2 - 3\rangle$ is field order 49

Why order $49 = 7^2$?

Div by x^2-3 w/rem, rems are $ax+b$. $a, b \in \mathbb{Z}_7$

So elts of $\mathbb{Z}_7[x]/\langle x^2-3\rangle$ are uniquely: $\underbrace{ax+b+I}_{\text{49 elts of } \mathbb{Z}_7[x]/I.}$ where $I = \langle x^2-3\rangle$

Not $\mathbb{Z}_{49}$

$\mathbb{Z}_7 = \{0,1,2,-3,-2,-1\}$

Unique factorization in $\mathbf{Z}[x]$

Can leverage Gauss' Lemma to show:

Theorem

Every nonzero non-unit $f(x) \in \mathbf{Z}[x]$ can be written **uniquely** *as*

$$f(x) = b_1 b_2 \cdots b_s p_1(x) p_2(x) \cdots p_m(x),$$

where the b_i are prime integers and the $p_j(x)$ are primitive and irreducible over $\mathbf{Q}$.

Easier after we prove unique factorization in $\mathbf{Q}[x]$.

Divisibility: The big picture

Ch. 18

We'll show that:

TBD Euclidean domain $\Rightarrow$ PID $\Rightarrow$ Unique factorization

and converses all false. Start with terminology.

$\frac{1}{7}(x-3)$

Definition

$D = \mathbb{Q}[x]$

D integral domain, $a, b \in D$.

$(x-3)$, $(\frac{1}{7}x - \frac{3}{7})$

a, b **associates**: $a = ub$, u a unit of D.

a **irreducible**: $a \neq 0$, a not a unit, and if $a = bc$, then one of b, c is a unit.

$D = \mathbb{Z}$! $7 = 7 \cdot 1 = (-7) \cdot (-1)$

p **prime**: $p \neq 0$, p not a unit, and if p divides ab, then p divides a or p divides b.

$D = \mathbb{Z}$: 7 div ab $\Rightarrow$ 7 div a or 7 div b

Irreducible $\not\Rightarrow$ prime:

$D = \mathbb{Z}[\sqrt{-5}]$

$6 = (1+\sqrt{-5})(1-\sqrt{-5}) = 2 \cdot 3$

all irr. not prime

Prime $\Rightarrow$ irreducible

D int dom.

A: p is prime. $(p \text{ div } ab \Rightarrow p \text{ div } a \text{ or } b)$

(A) $p = ab = 1ab \Rightarrow p$ div a or b

WLOG p div a, so $a = pd$ $(d \in D)$

$p = pdb$

$1 = db$, ie., b unit

(Int dom $\Rightarrow$ cancel)

(C) a unit or b unit

C: p is irreducible. $(p = ab \Rightarrow a \text{ unit or } b \text{ unit})$

In a PID, irreducible $\Rightarrow$ prime

A: D is a PID, a is irreducible.

($a = bc \Rightarrow$ one unit)

(A) a div bc, a doesn't div b ☆

So $\langle a, b\rangle = \langle d\rangle$ for some $d \in D$ PID

By defn $\exists\, x, y \in D$ s.t. $ax + by = d$,

d div $a \Rightarrow d = au$ or u unit in D

If $d = au$, d div b contra ☆

So d unit, $\langle a, b\rangle = \langle 1\rangle \Rightarrow ax' + by' = 1$ for $x', y' \in D$

$acx' + bcy' = c$

C: a is prime.

div by a

a div bc,
so div by a.

(c) a div c

Note: Z is a PID, so this works in the integers, which is why "prime" and "irreducible" are interchangeable ideas for integers.

Unique factorization domains (UFDs)

Definition

D a UFD means D is a domain such that for $a \in D$, $a \neq 0$, a not a unit:

- We have
$$a = p_1 \dots p_k$$
for some irreducibles p_i.
- If
$$a = p_1 \dots p_k = q_1 \dots q_s$$
for some irreducibles p_i, q_j, then $k = s$ and can rearrange factors s.t. p_i and q_i are associates.

Note: How could a factorization not exist?

Ascending chain condition (ACC)

Definition

Domain D satisfies ACC means: If $I_1 \subseteq I_2 \subseteq \cdots$ is a chain of ideals of D, then there exists k such that $I_k = I_{k+1} = \cdots$.

Theorem

A PID D satisfies ACC.

Proof: Suppose $I_1 \subseteq I_2 \subseteq \cdots$ is a chain of ideals of D. Let $I = \bigcup_{n=1}^{\infty} I_n$; can show that I is an ideal of D.

PID implies UFD: Factorization exists

Suppose $a \in D$, D a PID, $a \neq 0$, a not a unit, a doesn't factor into irreducibles.

PID implies UFD: Factorization unique

Suppose $a \in D$, D a PID, $a \neq 0$, a not a unit, and

$$a = p_1 \dots p_k = q_1 \dots q_s,$$

where p_i and q_j are irreducibles. Since irreducibles are prime: