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.

tonight

イロト 不得 トイヨト イヨト

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

Counting is never (just) about formulas; it's about stories.

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

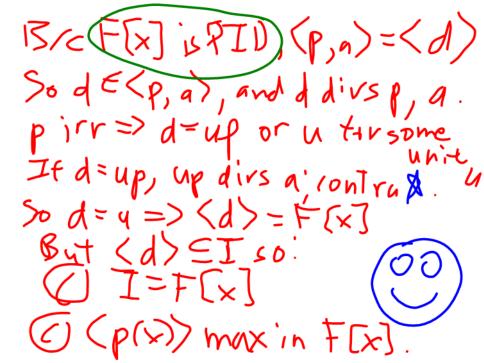
(b) How many polynomials are there of form $(x-a)(x^2+bx+c)$, where x^2+bx+c is irreducible?

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) 2. Choose (234 (Assume list of

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 $1 \Rightarrow 2$. (A) pla irrel S'pose <p(x)>CIEF(x) iters $\kappa(x) \in \mathbb{T}, \kappa(x) \notin \langle p(x) \rangle$ docsn't L'.V



We really showed IF D is PID, THE 1. msk Z. p irred. D domain, a CD; TFAE q unit (=) < a > = 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

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

ingen'l later

Example: A field of order $49 = 7^2$ Tate Z, [x]/<p(x1) deg=2, p(x) irred. Bledey 2, pirr > hozetos. Take p(x)= x2-a p(x)=0 no sol'as p(x)= x2=1 no sol'as SquaresinZn: 1,4,2; 3 nonsquare 50 Z7[x]/(x2-37 is tield order 49

Why order 49=72? D'iv by x'-Jw/vew, rems Are ax+b. $a, b \in \mathbb{Z}$, I So elts of $\mathbb{Z}_{7}[x]/(x^{2}-3)$ are uniquely: ax+b+I, $\mathbb{Z}_{7}^{7}=\{0,1,2\},3,2\}$ Not \mathbb{Z}_{49} elts of $\mathbb{Z}_{7}[x]/I$.

Unique factorization in Z[x]

Can leverage Gauss' Lemma to show:

Theorem

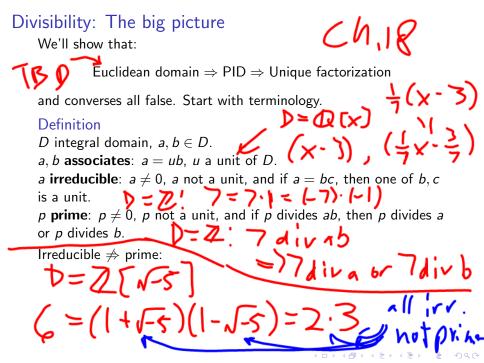
Every nonzero non-unit $f(x) \in \mathbf{Z}[x]$ can be written uniquely as

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

▲□▶ ▲□▶ ▲□▶ ▲□▶ ■ ●の00

where the b_i are prime integers and the $p_j(x)$ are primitive and irreducible over **Q**.

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



Prime \Rightarrow irreducible A: p is prime. (p Air ab \Rightarrow p dir a or b)

In a PID, irreducible \Rightarrow prime A: D is a PID, a is irreducible. A a divic, a ruesh't livba So (a,b)=<d>torsome d ED By define $\exists x_{1}y \in D_{x}$, ax + by = d, PID d div a => d = an or n unnit ind If d = an, d d ivb conting <math>xSo d mit, $\langle a, b \rangle = \langle 1 \rangle = 7\pi x + by = 1$ For x, 5'ED C: a is prime. acx'+ bcy =

Cadir c

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

a div be, >0 div byg.

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

$$a=p_1\ldots p_k=q_1\ldots q_s$$

▲□▶ ▲□▶ ▲□▶ ▲□▶ ■ ●の00

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

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

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