Math 128B, Wed Mar 03

- 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. 17. Reading for Mon: Ch. 18.
- PS04 outline due tonight, full version due Mon Mar 08.
- Problem session Fri Mar 05, 10am–noon.

Gauss' Lemma and consequences

Definition Content of

$$a_n x^n + \cdots + a_1 x + a_0 \in \mathbf{Z}[x]$$

is $gcd(a_n, \ldots, a_1, a_0)$. $f \in Z[x]$ primitive means content of f is 1. Gauss' Lemma: Product of primitive polynomials is primitive.

Suppose $f \in \mathbf{Z}[x]$. If f reducible over \mathbf{Z} , reducible over \mathbf{Q} unless factorization is just pulling out a constant. Conversely:

Theorem (Cor to Gauss' Lemma)

If $f \in \mathbf{Z}[x]$ reducible over \mathbf{Q} , reducible over \mathbf{Z} .

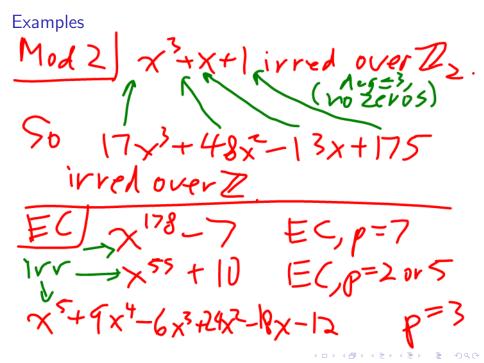
Proof in text; main point is that if f irreducible over Z, then f irreducible over Q.

(日) (四) (日) (日) (日)

Tests for proving irreducibility over Z

= 0 (mont p m 2 d Suppose $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$, p prime. Theorem (Mod *p* irreducibility test) Let $\overline{f}(x)$ be f(x) with coefficients reduced (mod p). If f(x) is irreducible over \mathbf{Z}_p , then f(x) is irreducible over $\frac{1}{2}$ (and therefore 🛶 er Q 🎢 (mod p Theorem (Eisenstein criterion If p divides a_{n-1}, \ldots, a_0 , p doesn't divide a_n , and p^2 doesn't divide a_0 , then f irreducible over **Z** (and therefore, over **Q**).

Side note: Can show that a random polynomial w/ integer coefficients is irreducible over Q with probability 1. (Hilbert irreducibility theorem)



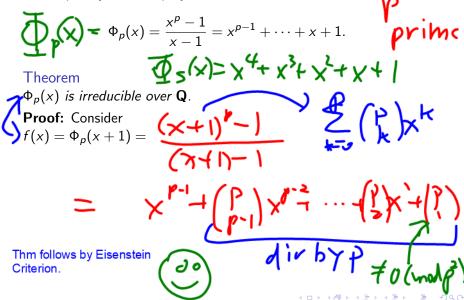
Proofs of irreducibility tests Mody fred => fred sverly Pt fred => f=gh (g,h EQ(x)) over & Aigg, digh ≥ 1. =) f= g=h. g., h= EZ[X] (reAyre =) f= go ho go ho Eq.(x) no Ap) => F ved . over Ze.

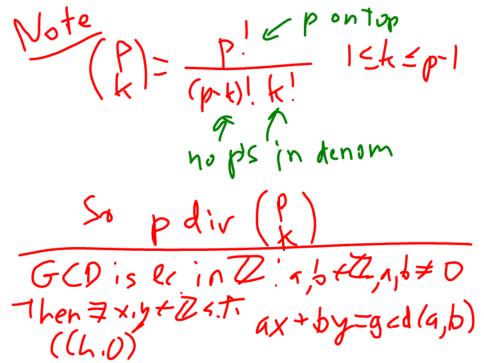
Why replace -3x-10= (2x-

Gauss' Lemma: When you multiply two integer polynomials, no surprise factors of p appear in product. Cor to GL: When you multiply two rational polynomials, no surprise way to cancel out denominators in product.

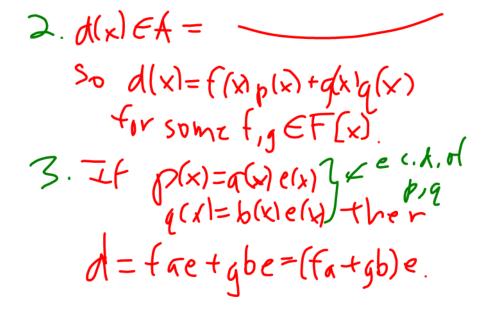
The pth cyclotomic polynomial is irreducible

Define *p*th cyclotomic polynomial to be:

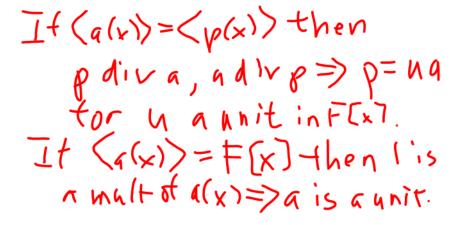




GCD is a linear combination Not in Gallian!!!! F a field, $p(x), q(x) \in F[x]$. Because F[x] is a PID, $\langle p(x), q(x) \rangle = \langle d(x) \rangle$ for some $d(x) \in F[x].$ **Thm:** d(x) divides both p(x) and q(x). d is a polynomial Conversely, there exist $f(x), g(x) \in F[x]$ such that linear combination of p and q f(x)p(x) + g(x)q(x) = d(x),which means that any common divisor of p(x) and q(x) must divide d(x). (So d is a common divisor of p and q of greatest possible degree.) Proof: $A = \{f(x) \mid g(x) \neq g(x) \mid f, g \in F[x]\}$ = < d (x))= 111 ma Its of d(x). (i 1. p(x), q(x) EA => P, 1 mults



Constructing new fields Theorem $f = f(x) \in F[x]$. Then TFAE: $A = \langle p(x) \rangle$ 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: (=72) A. A=<p(x)> max'. S'pose p(x)= a(x) b(x) a, b = F[x] (Think: (2))<6) $\langle \langle x \rangle \rangle \geq \langle p(x) \rangle$ $So \langle a(x) \rangle = \langle p(x) \rangle_{or} \langle a(x) \rangle = F_{x}$



So either way, in the factorization p(x) = a(x) b(x), one of a and b must be a unit.

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

・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・

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

Example: A field of order 49

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 $\mathbf{Q}[x]$.

Next up

$\mathsf{Euclidean} \Rightarrow \mathsf{PID} \Rightarrow \mathsf{UFD}$

▲□▶ ▲圖▶ ▲≣▶ ▲≣▶ = のへで