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.
- 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 $\gcd(a_n, \ldots, a_1, a_0)$. $f \in \mathbf{Z}[x]$ **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 $\mathbf{Z}$, then f irreducible over $\mathbf{Q}$.

want

prove

Tests for proving irreducibility over $\mathbf{Z}$

$\neq 0$ mod p $\quad = 0 \pmod{p}$ $\quad \neq 0 \pmod{p^2}$

Suppose $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbf{Z}[x]$, p prime.

Theorem (Mod p irreducibility test)

Let $\overline{f}(x)$ be $f(x)$ with coefficients reduced $\pmod{p}$. If $\overline{f}(x)$ is irreducible over $\mathbf{Z}_p$, then $f(x)$ is irreducible over ~~$\mathbf{Z}$ (and therefore, over $\mathbf{Q}$)~~.

$a_n \neq 0 \pmod{p}$

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 $\mathbf{Z}$ (and therefore, over $\mathbf{Q}$).

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

Examples

Mod 2 | x^3+x+1 irred over $\mathbb{Z}_2$.
($\deg \le 3$, no zeros)

So $17x^3+48x^2-13x+175$
irred over $\mathbb{Z}$

EC | $x^{178}-7$ EC, $p=7$

Irr $x^{55}+10$ EC, $p=2$ or 5

$x^5+9x^4-6x^3+24x^2-18x-12$ $p=3$

Proofs of irreducibility tests

Mod p) f red over $\mathbb{Q}$ $\Rightarrow$ $\bar{f}$ red over $\mathbb{Z}_p$

Pf f red over $\mathbb{Q}$. $\Rightarrow f = gh$ ($g, h \in \mathbb{Q}[x]$) $\deg g, \deg h \geq 1$.

$\Rightarrow f = g_0 h_0 \quad g_0, h_0 \in \mathbb{Z}[x]$

(reduce mod p) $\Rightarrow \bar{f} = \bar{g}_0 \bar{h}_0 \quad \bar{g}_0, \bar{h}_0 \in \mathbb{Z}_p[x]$

$\deg \bar{g}_0, \deg \bar{h}_0 \geq 1$

$\Rightarrow \bar{f}$ red. over $\mathbb{Z}_p$.

Why replace $g \to g_0$?
$h \to h_0$

$$\underbrace{x^2-3x-10}_{f} = \underbrace{\left(\tfrac{1}{2}x-\tfrac{5}{2}\right)}_{g}\underbrace{(2x+4)}_{h}$$

$$= \underbrace{(x-5)}_{g_0}\underbrace{(x+2)}_{h_0}$$

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 pth cyclotomic polynomial to be:

p prime

$$\Phi_p(x) = \Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + \cdots + x + 1.$$

$$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$$

Theorem

$\Phi_p(x)$ is irreducible over $\mathbf{Q}$.

Proof: Consider

$$f(x) = \Phi_p(x+1) = \frac{(x+1)^p - 1}{(x+1) - 1} \qquad \sum_{k=0}^{p} \binom{p}{k} x^k$$

$$= x^{p-1} + \underbrace{\binom{p}{p-1} x^{p-2} + \cdots + \binom{p}{2} x + \binom{p}{1}}_{\text{div by } p}$$

$\binom{p}{1} \not\equiv 0 \pmod{p^2}$

Thm follows by Eisenstein Criterion.

Note

$$\binom{p}{k} = \frac{p!}{(p-k)!\,k!} \qquad 1 \le k \le p-1$$

p on top

no p's in denom

So $p \text{ div } \binom{p}{k}$

GCD is lc in $\mathbb{Z}$: $a, b \in \mathbb{Z}$, $a, b \neq 0$

Then $\exists\, x, y \in \mathbb{Z}$ s.t. $ax + by = \gcd(a,b)$

(Ch. 0)

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 $d(x) \in F[x]$.

"A"

Thm: 1. $d(x)$ divides both $p(x)$ and $q(x)$.

2. Conversely, there exist $f(x), g(x) \in F[x]$ such that

$$f(x)p(x) + g(x)q(x) = d(x),$$

d is a polynomial linear combination of p and q

which means that 3. 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: $A = \{f(x)p(x) + g(x)q(x) \mid f, g \in F[x]\}$

$= \langle d(x)\rangle =$ all mults of $d(x)$.

1. $p(x), q(x) \in A \Rightarrow p, q$ mults of d.

2. $d(x) \in A = $ ______

So $d(x) = f(x)p(x) + g(x)q(x)$ for some $f, g \in F[x]$.

3. If $\left.\begin{array}{l} p(x) = a(x)e(x) \\ q(x) = b(x)e(x) \end{array}\right\}$ ← e c.d. of p, q then

$d = fae + gbe = (fa + gb)e.$

Constructing new fields

Theorem $\deg p \geq 1$

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

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

$A = \langle p(x) \rangle$

main app'l.

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

Proof of thm:

$1 \Rightarrow 2$ A. $A = \langle p(x) \rangle$ max'l.

S'pose $p(x) = a(x)\, b(x)$ $a, b \in F[x]$

$\langle a(x) \rangle \supseteq \langle p(x) \rangle$ (Think: $\langle 2 \rangle \supseteq \langle 6 \rangle$)

So $\langle a(x) \rangle = \langle p(x) \rangle$ or $\langle a(x) \rangle = F[x]$

If $\langle a(x)\rangle = \langle p(x)\rangle$ then

p div a, a div $p \Rightarrow p = ua$

for u a unit in $F[x]$.

If $\langle a(x)\rangle = F[x]$ then 1 is

a mult of $a(x) \Rightarrow a$ is a unit.

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

<u>Next</u> $2 \Rightarrow 1$.

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 $\mathbf{Z}[x]$

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 $\mathbf{Q}[x]$.

Next up

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