Math 128B, Mon Mar 01

- 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. 17.
- PS04 outline due Wed, full version due Mon Mar 08.
- Problem session Fri Mar 05, 10am–noon.

Recall: Division with remainder in $F[x]$

Theorem

Let F be a field, and let $a(x)$ and $d(x)$ be polynomials in $F[x]$ with $d(x) \neq 0$. There exist unique $q(x), r(x) \in F[x]$ such that

$$a(x) = d(x)q(x) + r(x), \qquad \text{with } \boxed{\deg(r(x)) < \deg(d(x)).}$$

Ex. $F = \mathbb{Z}_5$

$a(x) = x^2 + 2x + 4$

$d(x) = x + 2$

$a(x) = x\, d(x) + 4$

$q(x) = x$

$r(x) = 4$

$F[x]$ is a PID

Definition

A **principal ideal domain** is an integral domain R in which every ideal has the form $\langle a \rangle = \{ra \mid r \in R\}$ for some $a \in R$.

Non-example: $\langle x, 2 \rangle$ in $\mathbf{Z}[x]$ can't be generated by a single element.

all polynomials with even constant term

Theorem

If F is a field, then $F[x]$ is a PID.

$\deg(0) = -\infty$

$\deg(\text{non-0 const}) = 0$

Pf

S'pose A is an ideal of F[x].
If A = {0}, then A = <0>, done.
So assume A contains nonzero elements.
Let d(x) be a nonzero element of A with smallest possible degree.

WTS: A = <d(x)> = { q(x)d(x) | q(x) in F[x] }.
We know <d(x)> contained in A, so enuf to show A contained in <d(x)>.

A) $a(x) \in A$

Long div: $a(x) = q(x)d(x) + r(x)$

for some $q, r \in F[x]$, $\deg r < \deg d$

So $r(x) = a(x) - q(x)d(x) \in A$

$\in A$ $\quad$ $\in A$, ideal $\quad$ $\in A$

But d is non-0 elt of A w/ min deg, $\deg r < \deg d$!

So $r(x) = 0$.

$\Rightarrow a(x) = q(x)d(x)$ for some $q \in F[x]$

$\Rightarrow a(x) \in \langle d(x) \rangle$

Corollary

F a field, I a nonzero ideal of $F[x]$, $g(x) \in I$.
Then $I = \langle g(x) \rangle$ exactly when $g(x)$ is a nonzero polynomial of smallest possible degree in I.

Factoring in $D[x]$

like defn of primes in $\mathbb{Z}$.

D an integral domain.

Definition

$f(x) \neq 0$, f not a unit. in $D[x]$.

- f is **reducible** over D if $f(x) = a(x)b(x)$ and neither of $a, b \in D[x]$ is a unit.
- Otherwise f is **irreducible**, i.e., whenever $f(x) = a(x)b(x)$, then one of $a, b \in D[x]$ is a unit.

Ex. x^2+1 irred over $\mathbb{Q}$, $\mathbb{R}$

" red over $\mathbb{C}$."

$x^2+1=(x-i)(x+i)$

x^2+1 irred over $\mathbb{Z}_3$

$x^2+1=(x+1)^2$ over $\mathbb{Z}_2$ red!

(Over $\mathbb{Z}_2$: $(x+1)^2=x^2+2x+1$
$=x^2+1$.)

$2x^2+2$ red over $\mathbb{Z}$: $(2x^2+2)=(x^2+1)(2)$

$2x^2+2$ irred over $\mathbb{Q}$ (2 unit in $\mathbb{Q}$)

Note: By definition, factorization in Z[x] contains factorization in Z as a subcase. So factorization in Z[x] is strictly more complicated than factorization in Q[x].

Fact: Factorization in Z[x] is (more or less)

factorization in Q[x] + factorization in Z

Why do we care about factorization?

Meta-principle: As it goes in Z, so it goes in F[x].

$\mathbb{Z}/\langle p \rangle$ field $\iff$ p prime

- **Fact:** $F[x]/\langle p(x)\rangle$ is a field if and only if $p(x)$ is irreducible. over F (This follows from long division, but we'll prove that later.)
- So to construct interesting examples of fields, we need to be able to test if $p(x) \in F[x]$ is irreducible, especially for $F = \mathbf{Q}$ and $F = \mathbf{Z}_p$.
- Turns out that the most common irreducibility techniques are based on factoring $f(x)$ over $\mathbf{Z}$. Fortunately, turns out that reducibility over $\mathbf{Q}$ is basically equivalent to reducibility over $\mathbf{Z}$ (!!).

Main case of interest: Given f(x) in Z[x], figure out if f(x) is reducible or irreducible over Q.

Degrees 2 and 3

Theorem

F a field, $f \in F[x]$, $\deg f = 2$ or 3. Then TFAE:

1. *f is reducible.*
2. *f has a zero in F.*

Proof:

$\alpha \in F$

(2) $\Rightarrow$ (1): If $f(\alpha) = 0$ then $(x-\alpha)$ div. f (factor thm).

(1) $\Rightarrow$ (2) If $f(x) = g(x)h(x)$, g, h not units

So $\deg g, \deg h > 0$, so one has deg 1:

$2 = 1+1$; $3 = 1+2 = 2+1$.

So if $g(x) = ax + b$ $\quad a \neq 0$

$$g(x) = a\left(x + \frac{b}{a}\right)$$ F field

So $f\left(-\frac{b}{a}\right) = g\left(-\frac{b}{a}\right) h\left(-\frac{b}{a}\right)$

$$= 0 \cdot h\left(-\frac{b}{a}\right) = 0.$$

$\underline{\text{Ex}}$. $F = \mathbb{Z}_2 = \{0,1\}$

$f(x) = x^3 + x + 1$ $\quad f(0) = 1$ $\quad$ f irred.

$f(1) = 1$

$\underline{\text{Ex}}$. $g(x) = x^4 + x^2 + 1$

$g(0) = 1$, $g(1) = 1$ $\quad$ deg 4

But $g(x) = (x^2 + x + 1)^2$. $\quad$ FAIL

$F = \mathbb{Z}_3$: $g(x) = x^4 + x^2 + 1$

$g(1) = 0$ so $(x-1)$ div g.

Gauss' Lemma

prim

$\text{cont}(10x^2+6x+15)=1$

$\text{cont}(4x^2+6x-30)=2$

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.
Proof: Suppose $f, g \in \mathbf{Z}[x]$, f, g primitive, $h(x) = f(x)g(x)$.
Suppose prime p divides gcd of coefficients of $h(x)$.

ABC

$\bar{h}(x) = h(x)$, coeffs reduced (mod p)

So $\bar{h}(x) = 0$ in $\mathbb{Z}_p[x]$.

But $\bar{h}(x) = \bar{f}(x)\bar{g}(x)$ (mod p homom)

And $\mathbb{Z}_p[x]$ is an int. dom

So either $\bar{f}(x)=0$ or $\bar{g}(x)=0$ in $\mathbb{Z}_p[x]$

$\Rightarrow p$ div $\text{cont}(f)$ or $\text{cont}(g)$

Contra: Assumed $\text{cont}(f)=1=\text{cont}(g)$.

Reducible over $\mathbf{Q}$ implies reducible over $\mathbf{Z}$

Suppose $f \in \mathbf{Z}[x]$. If f reducible over $\mathbf{Z}$, reducible over $\mathbf{Q}$ *a fortiori*. Conversely:

Theorem

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

Proof: WLOG f primitive. Suppose $f(x) = g(x)h(x)$, $g, h \in \mathbf{Q}[x]$. Clear denominators of g and h: $abf(x) = (ag(x))(bh(x))$.

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

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 (mod p). If $\overline{f}(x)$ is irreducible over $\mathbf{Z}_p$, then $f(x)$ is irreducible over $\mathbf{Z}$ (and therefore, over $\mathbf{Q}$).

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 $\mathbf{Q}$).

Examples

Proofs of irreducibility tests

The pth cyclotomic polynomial is irreducible

Define pth cyclotomic polynomial to be:

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

Theorem

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

Proof: Consider

$f(x) = \Phi_p(x+1) =$