Math 128B, Wed Mar 10

- 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 Mon: Ch. 19. (New arc in the book: Fields!)
- PS05 outline due tonight, full version due Mon Mar 15.
- Problem session Fri Mar 12, 10am–noon.

The big picture

p prime: p div $ab \Rightarrow p \mid a$, $p \mid b$

a irreducible: If a = bc, then one of b,c is a unit.

Prime vs. irreducible:

Always: prime $\Rightarrow$ irreducible

PID: irr $\Rightarrow$ prime

b/c fact not uniq.

Euclidean domain, PID, UFD:

ED $\Rightarrow$ PID $\Rightarrow$ ACC

Can factor into irreducibles

PID $\Rightarrow$ Every irreducible is prime

$\Rightarrow$ UFD

Converses are false: E.g., Z[x] is a UFD but not a PID.

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.

$\boxed{\mathbb{Z} \text{ is UFD: } 12 = 2 \cdot 2 \cdot 3 = (-3)(-2) \cdot 2}$

$p_1 \sim q_1, p_2 \sim q_2, \dots$

Note: How could a factorization not exist?

$D = \mathbb{Z}[\sqrt{2}, \sqrt[4]{2}, \sqrt[8]{2}, \sqrt[16]{2}, \dots]$

There:

$$2 = \sqrt{2}\sqrt{2}$$
$$= (\sqrt[4]{2})^4$$
$$= (\sqrt[8]{2})^8$$
$$\vdots$$

No such thing as irreds.

factoring never stops!

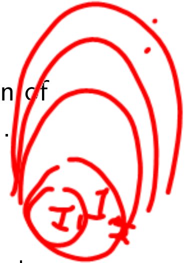
3 divides 15

$\langle 15\rangle \subset \langle 3\rangle$

$\langle 2\rangle \subset \langle\sqrt{2}\rangle \subset \langle\sqrt[4]{2}\rangle \subset \langle\sqrt[8]{2}\rangle \subset \cdots$

ACC fails

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.

Noetherian ring: Every ideal is *finitely* generated.

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.

B/c D is PID, $I = \langle d \rangle$ for some $d \in D$.

By defn of union, $d \in I_k$ for some k.

So $I = \langle d \rangle \subseteq I_k \subseteq I_{k+1} \cdots \subseteq I$.

C $\exists\, k$ s.t. $I_k = I_{k+1} = \cdots$

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.

$a = b_1 b_2 \longleftarrow$ one reducible, say b_1

$b_1 = c_1 c_2 \longleftarrow$ one reducible

$c_1 = d_1 d_2 \longleftarrow$ " "

$\vdots$

Then:

$\langle a \rangle \subset \langle b_1 \rangle \subset \langle c_1 \rangle \subset \cdots$

is an infinite ascending chain of ideals that never terminates. Contradiction.

PID implies UFD: Factorization unique

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

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

ind on k

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

$k=1$: $a = p = q_1 \cdots q_s$

(By defn, irreducibles are not units)

So $s=1$, $q_1 = p$ ✓

$k>1$: IH assume for $k-1$ irr.

$a = p_1 \cdots p_{k-1} p_k = q_1 \cdots q_s$.

B/C irrs prime, p_k divs $q_1 \cdots q_s$, p_k div one of q_j's, say p_k divs q_s.

$q_s = p_k u$; B/C q_s irr, p_k not unit, u unit.

So:

$$p_1 \cdots p_{k-1} p_k = q_1 \cdots q_{s-1} p_k u$$

$$\Rightarrow p_1 \cdots p_{k-1} = (u q_1) q_2 \cdots q_{s-1}$$

By ind, $t-1=s-1$, and can rearrange as claimed.

If we allow units to be irreducible, the statement of unique factorization is no longer true:

$$12 = 2\cdot 2\cdot 3 = 1\cdot 2\cdot 2\cdot 3$$
$$= (-1)(-1)2\,2\,3$$

So we choose the definition of irreducible to avoid this problem.

Euclidean domains

Definition

Let R be a domain. A **size function** on R is a function $\sigma : R \to \mathbf{Z} \cup \{-\infty\}$ such that for all nonzero $r \in R$, $\sigma(r) \geq 0$ and $\sigma(r) > \sigma(0)$.

$\sigma(0) = 0$ or $-\infty$

Definition

A **Euclidean domain** is a domain R with a size function σ that satisfies the following axiom: For $a, d \in R$, $d \neq 0$, there exist $q, r \in R$ such that

$$a = qd + r \qquad \text{with } \sigma(r) < \sigma(d).$$

div w/ rem

Examples:

- $\mathbf{Z}$, with $\sigma(a) = |a|$.
- $\mathbf{F}[x]$, with $\sigma(f(x)) = \deg f(x)$. (Take $\deg 0 = -\infty$.)
- $\mathbf{Z}[i] = \{a + bi \mid a, b \in \mathbf{Z}\}$, with $\sigma(a + bi) = a^2 + b^2$.

ED implies PID

Theorem

If D is a Euclidean domain, then D is a PID.

Proof:

A D is ED $\qquad (\{0\} = \langle 0 \rangle)$

A I ideal of D, $I \neq \{0\}$

Choose $d \neq 0$ in I w/ smallest $\sigma(d)$.

A $a \in I$ ED $\Rightarrow a = dq + r$, $\sigma(r) < \sigma(d)$

$\Rightarrow r = a - dq \in I$

B/c d has smallest possible size among nonzero elements of I, we must have r=0.

C $a = dq$ for some $q \in D$.

C $\exists\, d \in D$ s.t. $I = \langle d \rangle$

C D is PID

~~Corollary~~

$\mathbf{Z}$ and $F[x]$ are "the same"

$\mathbf{Z}$	$F[x]$
$\sigma(a) = \lvert a \rvert$	$\sigma(f(x)) = \deg f$
Euclidean domain: $a = dq + r$, $\lvert r \rvert < \lvert d \rvert$	Euclidean domain: $a = dq + r$, $\deg(r) < \deg(d)$
PID: $I = \langle d \rangle$, $\lvert d \rvert$ min over nonzero	PID: $I = \langle d(x) \rangle$, $\deg d(x)$ min over nonzero
UFD: Every $a \neq 0$ is a unique product of primes (up to assoc and ordering)	UFD: Every $a \neq 0$ is a unique product of irreducibles (up to assoc and ordering)

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

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 $\mathbf{Q}$.

As usual, uniqueness is up to associates (i.e., ± 1) and order of the factors.

Why unique factorization works in $\mathbf{Z}[x]$

Enough to prove two things (of independent interest):

1. The irreducible elements of $\mathbf{Z}[x]$ are prime integers and primitive polynomials that are irreducible over $\mathbf{Q}$.
2. Every irreducible of $\mathbf{Z}[x]$ is prime in $\mathbf{Z}[x]$.

Generalization

Theorem

If D is a UFD, then $D[x]$ is a UFD.

Most notably: $F[x, y]$ is a UFD (but not a PID), and so is $F[x, y, z]$, $F[w, x, y, z]$, etc.