Math 221B, Wed Feb 09

- Use a laptop or desktop with a large screen so you can read these words clearly.
- In general, you may 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.
- **IN-PERSON CLASSES START MON FEB 14!!!!**
- Reading for today: 12.1–12.2.
- Reading for Mon Feb 14. is 12.3.
- PS02 due Mon Feb 14.
- Problem session Fri Feb 11, 10:00–noon on Zoom.

Integral domains

(Or domains for short)

Definition

To say that a ring R is an **integral domain** means that it has the **zero factor property:** If $a, b \in R$ and $ab = 0$, then either $a = 0$ or $b = 0$.

Non-example of an integral domain:

$R = \mathbb{Z}/(6)$ $\quad a = 2, b = 3$

$ab = 6 = 0, \quad a \neq 0, b \neq 0.$

Note: Not having ZFP = not having cancellation makes thinking about factoring/factorization really difficult.

Thm: Zero Factor Property is equivalent to:
Cancellation Property: If $ab = ac$, $a \neq 0$, then $b = c$.

(ZFP is case where c=0)

The field of fractions of an integral domain

Let D be a domain. Define the **field of fractions** F of D to be:

- **Set:** Symbols $\frac{a}{b}$, where $a, b \in D$, $b \neq 0$, and $\frac{a}{b}$ is equivalent to $\frac{a'}{b'}$ exactly when $ab' = a'b$.
- **Addition:**

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$

- **Multiplication:**

$$\left(\frac{a}{b}\right)\left(\frac{c}{d}\right) = \frac{ac}{bd}$$

This gives well-defined operations of addition and multiplication that make F a field. (Hard/annoying part: Show well-defined.)

See: Jim Tanton, *Fractions are Hard!*
`https://www.jamestanton.com/?p=1461`

w/ D as a subring.
Also: F is smallest poss such field.

Maximal ideals and fields

Defn: I an ideal of a ring R. To say that I is **maximal** in R means that $I \neq R$ and if A is an ideal of R such that $I \subset A \subset R$, then either $I = A$ or $A = R$.

No ideal properly contained between I and R.

Theorem

An ideal I of a ring R is maximal iff $\overline{R} = R/I$ is a field.

Proof: Corresp. Thm says that ideals of R/I <=> ideals between I and R.

So:

I is maximal in R
<=> no ideal contained properly between I and R
<=> no ideal contained properly between 0 ideal of R/I and R/I
<=> R/I has exactly two ideals
<=> R/I is a field.

The examples to keep in mind: $\mathbf{Z}$, $F[x]$

- Maximal ideals of $\mathbf{Z}$ are the principal ideals (p), where p is prime.
- Maximal ideals of $F[x]$ are the principal ideals $(f(x))$, where $f(x)$ is irreducible.

12, 13 Factoring

15, 16 Field Thy (Solving Poly)

Divisibility: Defns

R a ring, $a, b, d, q, u \in R$.

Defn: u is a **unit** means u has a mult inv in R (i.e., some $v \in R$ such that $uv = 1$).

Defn: d **divides** a means $a = dq$ for some $q \in R$.

Defn: d is a **proper divisor** of a means $a = dq$ and neither d nor q is a unit.

Improper ex: 7 = (-1)(-7) = (1)(7)

Defn: a, b are **associates** if $a = bu$, u a unit.

Defn: a is **irreducible** means a is not a unit and a has no proper divisors.

Defn: p is **prime** means: If p divides ab, then either p divides a or p divides b.

I.e.: R/(p) =R (mod p) is a ring with ZFP.

Not the same!!

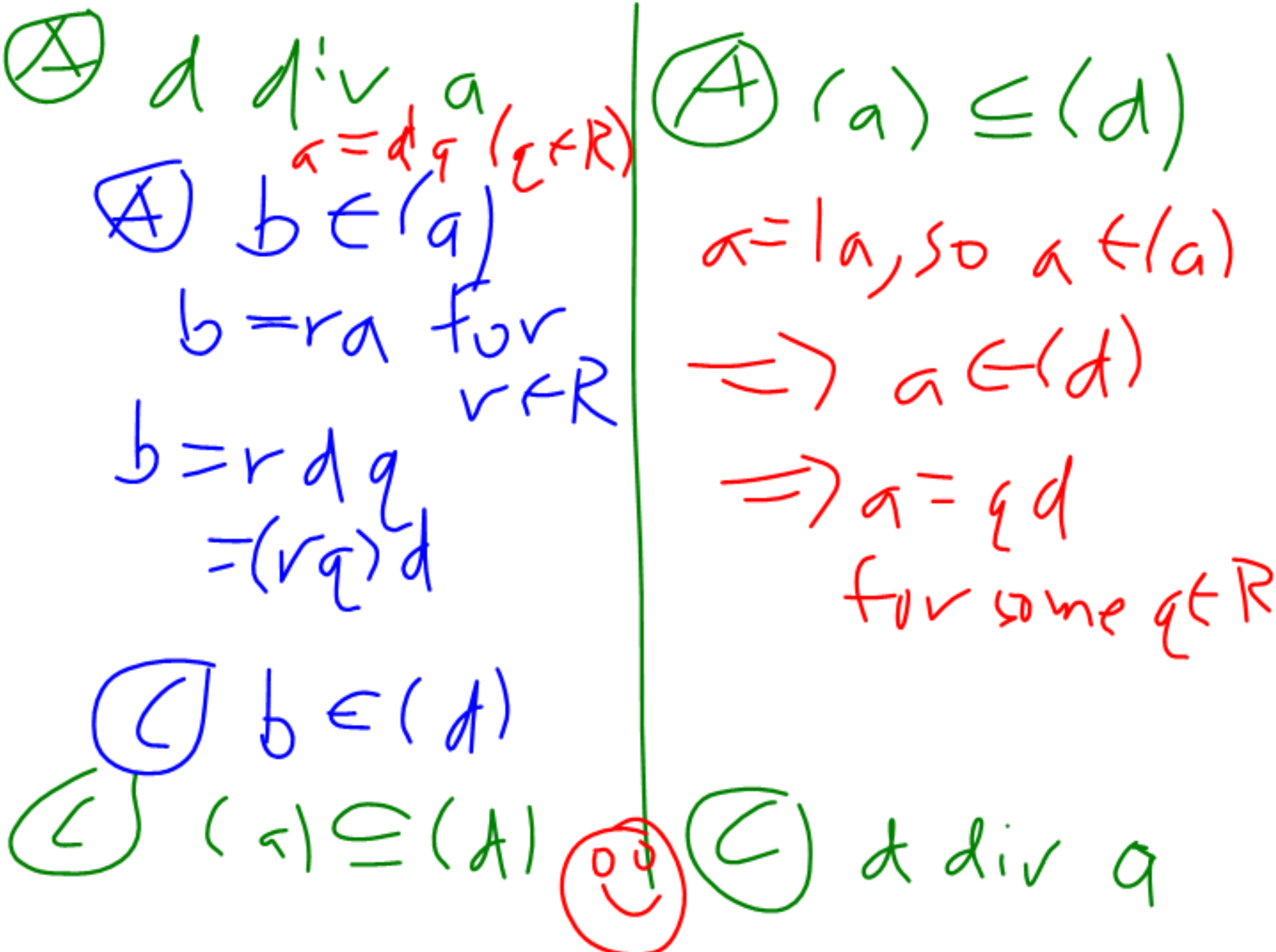
Divisibility and ideals

Each of those ideas can be restated in terms of ideals:

In terms of elements	In terms of ideals
u a unit	$(u) = (1)$
d divides a	$(d) \supseteq (a)$
d is a proper divisor of a	$(1) \supset (d) \supset (a)$
a, b associates	$(a) = (b)$
a irreducible	$(a) \neq (1)$, $(a) \subset (d) \subset (1)$
p prime	$ab \in (p)$, $\Rightarrow a \in (p)$ or $b \in (p)$

$2\mathbb{Z} \supset 6\mathbb{Z}$

$(d) > (a)$


(A) d div a
a = dq (q ∈ R)
(A) b ∈ (a)
b = ra for r ∈ R
b = r d q
= (rq) d
(C) b ∈ (d)
(C) (a) ⊆ (d)
(A) (a) ⊆ (d)
a = 1a, so a ∈ (a)
⟹ a ∈ (d)
⟹ a = qd for some q ∈ R
(C) d div a

A motivating counterexample: $R = \mathbf{Z}[\sqrt{-5}]$

Observe:

$$2 \cdot 3 = 6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

So in $R = \mathbf{Z}[\sqrt{-5}]$, elements can factor into irreducibles **non-uniquely**, i.e., factorization in R is not unique.

Note that the elements 2, 3, $1 \pm \sqrt{-5}$ are all irreducible (can check by brute force) but not prime. That is basically the obstruction preventing unique factorization.

The big picture: ED $\Rightarrow$ PID $\Rightarrow$ UFD

R an integral domain. (Otherwise, factoring is too weird!)

Defn: To say that R is a **Euclidean domain** means that there exists a nonnegative size function $\sigma : R \to \mathbf{Z} \cup \{-\infty\}$ such that for all $a, d \in R$, there exists $q, r \in R$ such that

$d \neq 0$

d = divisor
q = quotient
r = remainder

$$a = dq + r, \qquad \sigma(r) < \sigma(d).$$

$\sigma(0) = -\infty$

Defn: To say that R is a **principal ideal domain** means every ideal of R is equal to (a) for some $a \in R$.

Defn: To say that R is a **unique factorization domain** means that for $a \in R$: $a \neq 0$, a not unit

- (Existence) a can be expressed as a product of irreducibles of R.
- (Uniqueness) If $a = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_m$, where each p_i and q_j is irreducible, then $m = k$ and we can rearrange so that p_i and q_i are associates for each i.

The point of 12.2: ED $\Rightarrow$ PID $\Rightarrow$ UFD.

Examples of EDs

- $R = \mathbf{Z}$, $\sigma(a) = |a|$.
- F a field, $R = F[x]$, $\sigma(f(x)) = \deg f(x)$.
- $R = \mathbf{Z}[i]$, $\sigma(a + bi) = |a + bi|^2 = a^2 + b^2$.

Division for $\mathbf{Z}$ and $F[x]$ we've seen before.
In $\mathbf{Z}[i]$, approximate q by division in $\mathbf{C}$ and then round off.
Example:

$q = 3+2i \quad d = 1+i$

$\sigma(d) = 1^2 + 1^2 = 2$

$3+2i = 2(1+i) + 1$

$\sigma(1) = 1^2 = 1$

ED $\Rightarrow$ PID

Theorem

Let R be a Euclidean domain. For any ideal I of R, we have that $I = (a)$ for some $a \in R$.

Proof:

PIDs have GCDs and Bezout

Cor: Let R be an ED, $a, b \in R$. Suppose the ideal (a, b) is equal to (d) for some $d \in F[x]$. Then:

- d divides a and b.
- If e divides a and b, then e divides d.
- There exist $x, y \in R$ such that $ax + by = d$.

Proof:

UFDs

Defn: To say that an integral domain R is a **unique factorization domain** means that for $a \in R$:

- (Existence) a can be expressed as a product of irreducibles of R.
- (Uniqueness) If $a = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_m$, where each p_i and q_j is irreducible, then $m = k$ and we can rearrange so that p_i and q_i are associates for each i.

Venn diagram:

The big picture for UFDs

Let R be an integral domain. The main points to understand about UFDs are:

- The question of whether factoring terminates can be expressed in ideals.
- It is always the case that prime $\Rightarrow$ irreducible.
- Assuming factoring terminates, TFAE:
  - Irreducible $\Rightarrow$ prime.
  - Factorization is unique.
- In a PID, factoring terminates and irreducible $\Rightarrow$ prime.
- ED $\Rightarrow$ PID $\Rightarrow$ UFD.