Math 3032 (March 23, 2021)

OH Today 12 - 2 pm

Longer for HW:

- Optional assignment now due Thursday, March 25.
- HW 8 due Tuesday, March 30.
- HW 9 (last assignment) due Tuesday, April 6.

Plan for Final Exam:

- You select 72 hour window $\subseteq$ April 10 - 21.
- Next day: 15 minute meeting to discuss.
- Allowed resources: textbook, notes, HW, these lectures, etc.
- Disallowed resources: friends, internet, etc.

BE HONOURABLE.

Exam emailed to you at start of window, due at end of window.

Return to unique factorization

Let R be an integral domain and $a, b \in R$.

a <u>divides</u> b if $\exists c \in R$ s.t. $b = ac$. "$a | b$".

Since R is integral domain, c is unique if it exists.
(if $b = ac_1 = ac_2$ then cancel a's.)

except if $a = b = 0$.

<u>E.g.</u>: $\forall r \in R$, $r | 0$. Because take $c = 0$ find $0 = r \cdot 0$.

If a does not divide b then write $a \nmid b$.

If $0 | r$, then $r = 0$.

$\forall r \in R$, $1 | r$.

If $r | 1$, then r is a unit.

In terms of ideals:

$$a \mid b \iff b \in \langle a \rangle \iff \langle b \rangle \subseteq \langle a \rangle .$$

"Divides" is a preorder.

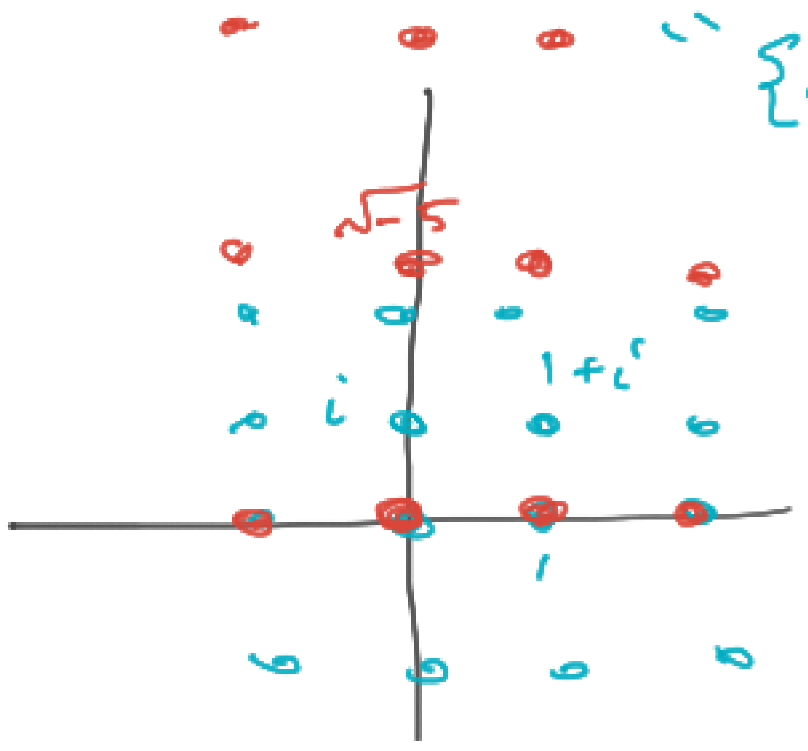
<u>E.g.</u>: In $R = \mathbb{Z}$, $-2 \mid 6$ because $6 = (-2)\cdot(-3)$.

In $\mathbb{Z}$, units are ± 1

In $\mathbb{Z}[i] \subseteq \mathbb{C}$, $(1+i) \mid 2$ because $(1+i)(1-i) = 2$.

"$\{a+bi,\ a,b \in \mathbb{Z}\}$"

$(1+i) \mid 2i$ because $(1+i)(-1+i) = 2i$



In $\mathbb{Z}[\sqrt{-5}]$ $\quad (1+\sqrt{-5}) \mid 6 = (1+\sqrt{-5})(1-\sqrt{-5})$

$2 \mid 6 = 2\cdot 3$

$$\mathbb{C} \supseteq \{a + b\sqrt{-5},\ a,b \in \mathbb{Z}\}$$

In $\mathbb{Z}[\sqrt{-5}]$, units are ± 1.

$$(a+b\sqrt{-5})(a'+b'\sqrt{-5}) = (aa' - 5bb') + (ab' + a'b)\sqrt{-5}$$

$\sqrt{-5} = i\sqrt{5}$

$\sqrt{5} \approx 2.1\ldots$

In $\mathbb{Z}[i]$, units are $\pm 1, \pm i$.

<u>Lemma:</u> If R an integral domain, then

$$[\, a \mid b \text{ and } b \mid a \,] \iff b = a \cdot u \text{ for some unit } u.$$

If this happens, a and b are <u>associates</u>, $a \sim b$.

$\sim$ is the equivalence relation induced from preorder $\mid$.

<u>E.g.</u>: In $\mathbb{Z}[\frac{1}{2}] \subseteq \mathbb{Q}$, units are $\pm 2^k$, $k \in \mathbb{Z}$

$\{\frac{m}{n}$ where $m \in \mathbb{Z}$, $n = 2^k$ for some $k \in \mathbb{N}\}$.

$3 \sim 6$ in this ring.

In a field, all nonzero elts are associate.

$r \in R$ is <u>irreducible</u> if

- r is not itself a unit, and
- for any factorization $r = ab$ one of a or b is a unit, and other is associate of r.

i.e.: if $s \mid r$ and s not a unit, then $s \sim r$.

<u>E.g</u>: (to be proved later) In $\mathbb{Z}[\sqrt{-5}]$, $2, 3, 1+\sqrt{-5}, 1-\sqrt{-5}$ are all irreducible.

Main Defn: A Unique factorization domain (UFD) is an integral domain R s.t.:

1. Every nonzero non-unit $r \in R$ can be factored as a product $r = p_1 \cdots p_m$ where $m < \infty$ and all p_i are irred.

2. If $r = p_1 \cdots p_m = q_1 \cdots q_n$ are two different factorizations into irreds, then $m = n$ and there is some reordering $\sigma : \{1, \dots, m\} \circlearrowleft$ s.t. $p_i \sim q_{\sigma(i)}$ $\forall i$.

E.g.: Desperately want $\mathbb{Z}$ to have unique fact.
(Fundamental Thm of Arithmetic)

$$-6 = (-3)\cdot 2 = (-2)\cdot(+3)$$

Non-examples of UFDs:

- In $\mathbb{Z}[\sqrt{-5}]$, I asserted $2, 3, 1+\sqrt{-5}, 1-\sqrt{-5}$ all irred.

  non are associate to each other.

  But $6 = 2.3 = (1+\sqrt{-5}).(1-\sqrt{-5})$.

- Take $\mathbb{F}$ a field. Look at polynomials in 2 variables $f(x,y)$ s.t. $f(x,y) = f(-x,-y)$

this ring is $\underbrace{\mathbb{F}[x^2, xy, y^2]}_{\text{subring is not a UFD.}} \subseteq \underbrace{\mathbb{F}[x,y]}_{\text{will prove that } \mathbb{F}[x,y] \text{ is UFD.}}$

$$x^2 \cdot y^2 = (xy) \cdot (xy)$$

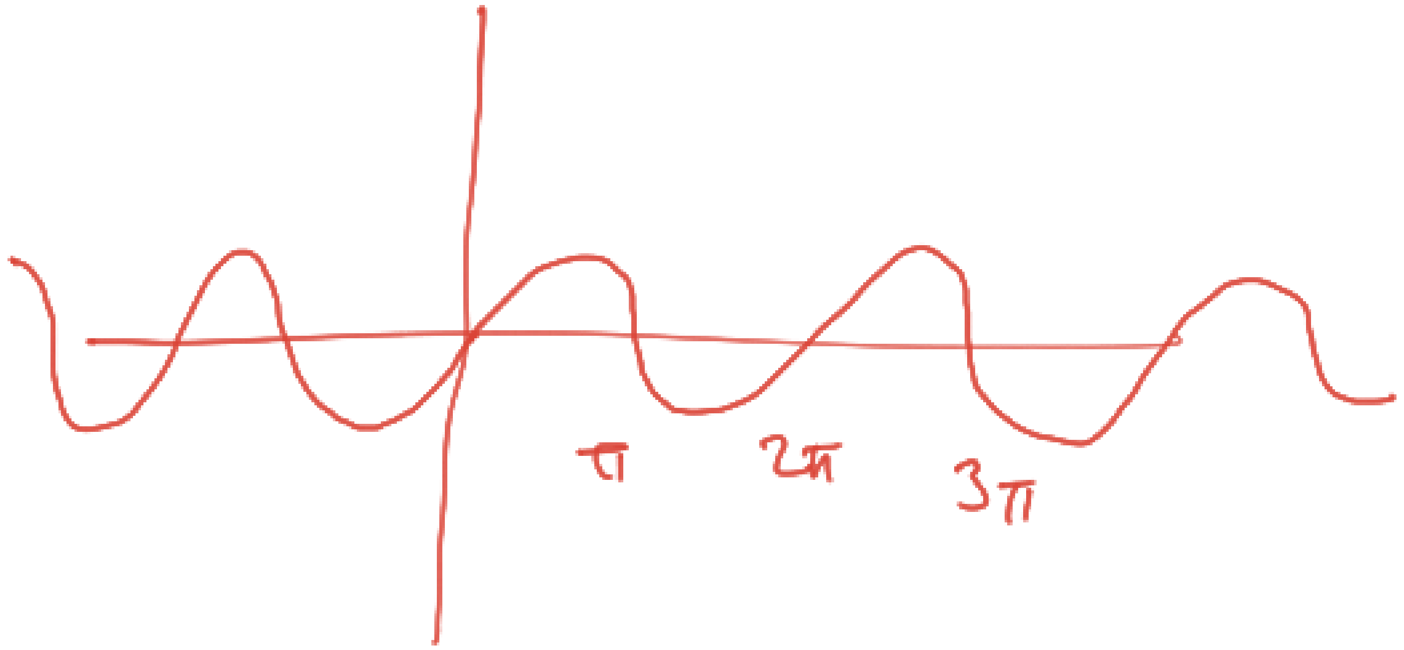
① Can also fail! Rings in which it fails are "large"!
$\mathcal{C}^{\omega}(\mathbb{R})$ ring of real-analytic functions.
(a little hard, but true, that this is an integral domain).
($\mathcal{C}^{\infty}(\mathbb{R})$ smooth functions not int. domain).

① Can also fail! Rings in which it fails are "large".

$R := \mathcal{C}^\omega(\mathbb{R})$ ring of real-analytic functions.
(a little hard, but true, that this is an integral domain).

($\mathcal{C}^\infty(\mathbb{R})$ smooth functions not int. domain).

$\sin(x) \in R$



for each n,

$$\frac{\sin(x)}{(x-\pi)(x-2\pi)\cdots(x-n\pi)}$$

↑ can be continued continuously

So can keep factoring out lin. terms. infinitely much.

A few weeks ago we very quickly proved:

Thm: Every PID is a UFD.

We'll give the proof. We have to confirm ①, ②.

An ascending chain of ideals is (descending along divisibility).

inclusion order

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$$

where each I_n is an ideal.

Lemma: If $I_1 \subseteq I_2 \subseteq \cdots$ is an asc. chain, then

$$I := \bigcup_{n=1}^{\infty} I_n \quad \text{is an ideal.}$$

Lemma: If $I_1 \subseteq I_2 \subseteq \ldots$ is an asc. chain, then

$$I := \bigcup_{n=1}^{\infty} I_n$$ is an ideal.

Pf: To prove that a nonempty subset of a ring is an ideal, have to prove:

(a) closed under $+$.
(b) absorbing under $\times$.

For (a): Let $a, b \in I$. Then $\exists\, m, n$ s.t. $a \in I_m$ and $b \in I_n$. Then $a, b \in I_{\max(m,n)}$. So $a+b \in I_{\max(m,n)} \subseteq I$.

For (b): similar.

__Defn:__ A ring R is __noetherian__ if it satisfies "ascending chain condition": every ascending chain stabilizes, i.e. for any ascending chain

$$I_1 \subseteq I_2 \subseteq \cdots$$

$$\exists\, N \text{ s.t. } \bigcup_{n=1}^{\infty} I_n = I_N.$$

__Ruled out:__ $I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \cdots$ all inclusions proper.

Lemma: Every $\boxed{\text{PID}}$ is Noetherian.

every ideal is singly gen.

Pf: Given ascending chain as above, $I = \bigcup_{n=1}^{\infty} I_n$ is an ideal, hence principal, i.e. $I = \langle r \rangle$ for some $r \in R$, but $r \in I_n$ for some n.

On HW: In fact, R is noetherian $\iff$ every ideal is finitely generated.

Proposition: If R is noetherian then ① holds, i.e. factorizations into irreds exist.

Pf: Suppose $a_1 \in R$ not a unit.

If a_1 is irred, then done: we've factored it. Otherwise, $a_1 = a_2 \cdot b_2$ both not units.

$\langle a_1 \rangle \subsetneq \langle a_2 \rangle$. and $\langle a_1 \rangle \subsetneq \langle b_2 \rangle$.

If both irred, done: we've factored.

Otherwise, at least one is not irred, say a_2.

$$a_2 = a_3 \cdot b_3$$

Then repeat: $\langle a_1 \rangle \subsetneq \langle a_2 \rangle \subsetneq \langle a_3 \rangle \subsetneq \dots$

If Noeth, must stop.

<u>Remark</u>: Noetherian is stronger than ability to factor elts into irreds.

<u>E.g.</u>: $\mathbb{F}[x_1, x_2, \ldots] = R$

polynomial ring in ∞ variables.

Is <u>not</u> Noetherian.

It does satisfy (1) because

if $f(x_1 \ldots) \in R$ then there is some n s.t.

$f(x_1, \ldots) \in \mathbb{F}[x_1, \ldots, x_n]$

and Hilbert basis thm says that are Noeth.

So f does factor into irreds.

In fact, we will prove that $\mathbb{F}[x_1, \ldots, x_n]$ is a UFD

$\Rightarrow R$ is UFD.

Prop: In a PID, $\langle p \rangle$ is max iff p is irred.

Pf: If $\langle p \rangle$ not max, then there exists ideal I s.t. $\langle p \rangle \subsetneq I \subsetneq R$.

Since R is a PID, $I = \langle a \rangle$ for some $a \in R$.

Then $p = ab$.

this properness means b is not a unit.

this properness means a is not a unit.

Conv: if $\langle p \rangle$ is maximal, then for any factorization $p = ab$, either $p \subsetneq \langle a \rangle = R$

or $p = \langle a \rangle \subsetneq R$. ∎

Cor: If $p \in R$ a PID is irred, then it is prime, i.e. if $p | ab$ then $p | a$ or $p | b$. **Pf:** max ideals are prime.

Thm: Every PID is a UFD.

Pf: We already showed PID $\Rightarrow$ noetherian $\Rightarrow$ existence of factorizations, all we need to show is uniqueness.

Let's suppose $r \in R$ is factored as

$r = p_1 \cdots p_m = q_1 \cdots q_n$ all p_i, q_j are irred.

Only use $p_1 \cdots p_m \sim q_1 \cdots q_n$.

Since p_1 irred, it is prime.

$p_1 \mid p_1 \cdots p_m$ so $p_1 \mid q_1 \cdots q_n$ so $\exists j$ s.t. $p_1 \mid q_j$.

$\exists\, j$ s.t. $p_1 \mid q_j$. But q_j is irred.

So $p_1 \sim q_j$. i.e. $q_i = p_1 \cdot u$ for some unit u.

So $\cancel{p_1} \cdots p_m \sim q_1 \cdots q_{j-1} (\cancel{p_1} \cdot u)\, q_{j+1} \cdots q_n$

Can cancel (because in a domain)

So $p_2 \cdots p_m \sim q_1 \cdots q_{j-1} q_{j+1} \cdots q_n$.

Repeat until you run out of terms. (must have $m=n$ else would get $1 \sim$ non unit.)

Find the reordering σ s.t. $q_{\sigma(i)} \sim p_i$. $\forall i$.

$\square$

Favorite examples:

(1) $\mathbb{F}[x]$ is a PID hence UFD.

(0) $\mathbb{Z}$ is a PID hence a UFD.

$\hookrightarrow$ Fundamental thm of arithmetic (Euclid).

Non-example: $\mathbb{Z}[\sqrt{-5}]$ is not a UFD.

because $1+\sqrt{-5}$, $1-\sqrt{-5}$, 2, 3

all irred but none are prime.

Next time: If R is a UFD
then $R[x]$ is a UFD.
(usually not a PID).