Def: a ring is a set $R$ of two operations $+$ and $\cdot$ sat. 7 axioms.

A ring is commutative if we also have $ab = ba$.

Non-example: matrices

\[
\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}
\]

\[
\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}
\]

An element $a \in R$ is a unit if $\exists b \in R$ with $ab = ba = 1$.

Example: in $\mathbb{Z}$, $\pm 1$ are the units, in $\mathbb{R}$, everything but 0.

A non-zero element $a \in R$ is a zero-divisor if $\exists c \neq 0$ with $ac = 0$ or $ca = 0$.

Example: $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$
on a worksheet, every example:

\[ R = \{ \text{subsets of plane} \} \]

\[ x \oplus y = "\text{symmetric difference}" \]

\[ (x \cup y) \cap (y \cup x) \]

\[ x \cap y = \emptyset \]

\[ \emptyset = \emptyset \]

units? \( x \cdot y = 1 \) means \( x \cap y = \text{whole plane} \)

hard to do: must have \( x \cap y = 1 \)

zero-divisors? \( x \cdot y = \emptyset \) means \( x \cap y = \emptyset \)

\[ x \bigtriangleup y \]

every thing but \( 0 \) and \( 1 \)

is a zero-divisor.

which axiom fails if we took \( x \oplus y = x \cup y \)?

\[ \forall x \exists y \text{ s.t. } x \oplus y = 0, \text{ all the rest still work.} \]
Prop. Let \( R \) be a ring. If \( a \in R \) is a unit then \( a \) is not a zero-divisor.

(Equiv: if \( a \) is a zero-div. then \( a \) is not a unit.)

Pf. Since \( a \) is a unit, 
\[ \exists b \in R \text{ such that } ab = ba = 1. \]

Let \( c \in R \).
if \( ac = 0 \)
then \( c = 1 \cdot c = (ba)c = b(ac) = b \cdot 0 = 0 \)

Similarly, if \( ca = 0 \) then \( c = 0 \).

So \( a \) is not a zero-divisor
(because that would mean \( \exists c \neq 0 \)
with \( ac = 0 \) or \( ca = 0 \)).

**WARNING:** don't think that every \( a \in R \) has to be either a unit or a zero-divisor.

in \( \mathbb{Z} = \mathbb{Z}, a = 2 \) is neither a unit nor a zero-divisor.
More def's:

- An **integral domain** is a commutative ring with no zero-divisors.

- Examples: \( \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C} \) polynomial rings w/ coeffs in these

\[
A = \{ a + b\sqrt{2} \mid a, b \in \mathbb{Z} \} \subset \mathbb{R}
\]

-from last week

- A **field** is a commutative ring where every non-zero element is a unit.

- Examples: \( \mathbb{Q}, \mathbb{R}, \mathbb{C} \)

- Not \( \mathbb{Z} \), polynomial rings.

- Lots about fields in 392.
The Ring \( \mathbb{Z}_m \) or \( \mathbb{Z}/m\mathbb{Z} \).

1. Low-brow definition:

\[ \mathbb{Z}_m = \{ 0, 1, 2, \ldots, m-1 \} \]

\( a + b = a \text{ mod } m \) if the honest \( a + b \) then reduce mod \( m \)

\[ a \cdot b = a \cdot b \text{ mod } m \]

Example: in \( \mathbb{Z}_{12} \), \( 3 + 11 = 2 \)

\[ 3 \cdot 11 = 9 \]

Is it a ring?

\[ |a + b| \text{ mod } m = a + (6 + \ldots) \]

Reduce this \( + \), \( \text{reduce again} \)

\[ a + \text{reduce} \]

\[ \text{works, but messy to prove.} \]

2. High-brow model

\[ \mathbb{Z}_m = \{ \text{equivalence classes of integers (mod } m) \} \]

For an integer \( x \), the equivalence class

\[ \overline{x} = \{ y \in \mathbb{Z} / x \equiv y \text{ (mod } m) \} \]

\[ = \{ x, x + m, x - m, x + 2m, x + 3m, \ldots \} \]
Example:

\[ \mathbb{Z}_2 = \{ \text{even numbers}, \text{odd numbers} \} \]

set with two elements, but those elements are sets.

\[ \mathbb{Z}_3 = \{ \ldots, -6, -3, 0, 3, 6, \ldots \} \]
\[ \{ \ldots, -5, -2, 1, 4, 7, \ldots \} \]
\[ \{ \ldots, -4, -1, 2, 5, 8, \ldots \} \]

How do we + and \( \cdot \)?

Define \( \bar{x} + \bar{y} = \bar{x + y} \), \( \bar{x} \cdot \bar{y} = \bar{x y} \).

Is it well-defined?

If \( \bar{x} = \bar{x}' \) and \( \bar{y} = \bar{y}' \),

do we have \( \bar{x} + \bar{y} = \bar{x' + y'} \) and \( \bar{x} \cdot \bar{y} = \bar{x' y'} \)? Yes.

Example: in \( \mathbb{Z}_4 \),

\[ \bar{3} + \bar{1} = \bar{4} \text{ by def} \]

But \( \bar{1} = -1 \) (Same set!)

and \( \bar{3} + \bar{-1} = \bar{2} \text{ by def} \).

But it's ok, because \( \bar{1} + 1 = \bar{2} \).

\[ \bar{x} = \bar{y} \text{ is the same as } x \equiv y \text{ (modm)}. \]
You've been reading about ordered rings fields.

On \( \mathbb{Z}_m \), there is no ordering that's compatible with + and .

On \( \mathbb{Z}_3 \), if \( l > 0 \)
then \( 1+1+1 > 0+0+0 \)
but \( 1+1+1 = 0 \).

If \( l < 0 \), same problem.

---

**Proposition:** \( \bar{a} \in \mathbb{Z}_m \) is a unit
iff \( \gcd(a, m) = 1 \)
otherwise it's a zero-divisor.

**Proof (i)** \( \bar{a} \) is a unit
iff \( \exists \bar{x} \in \mathbb{Z}_m \) with \( \bar{a} \bar{x} = \bar{1} \)
iff we can solve \( ax \equiv 1 \pmod{m} \)
seen: this is possible iff \( \gcd(a, m) = 1 \).

\((i)\) if \( \bar{a} \) is not a unit,
then \( \gcd(a, m) = d > 1 \).

---

Interlude

**Example:** in \( \mathbb{Z}_{10} \),
\( 3 \) is a unit because \( \gcd(3, 10) = 1 \)
\( 3 \cdot \bar{7} = \bar{1} \) in \( \mathbb{Z}_{10} \).
\[ 4 \text{ is a zero-divisor} \quad \gcd (4, 5) = 2 \]

\[ 4 \cdot 5 = 0 \]

Back in the proof, let \( b = n/d \).

Then \( ab = a \cdot \frac{m}{d} = a \cdot \frac{m}{d} \cdot m \)

is a multiple of \( m \).

So \( a b = 0 \) in \( \mathbb{Z}_m \). \( \Box \)