Defn: a <u>ring</u> is a set R
w/ two operations $+$ and $\cdot$
sat. 7 axioms.

a ring is <u>commutative</u> if we also have
$ab = ba$

non-example: matrices

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

an element $a \in R$ is a <u>unit</u>

if $\exists\, b \in R$ with $ab = ba = 1$

example: in $\mathbb{Z}$, ± 1 are the units,
in $\mathbb{Q}$, everything but 0.

a non-zero element $a \in R$ is a <u>zero-divisor</u>
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 worksheet, crazy example:

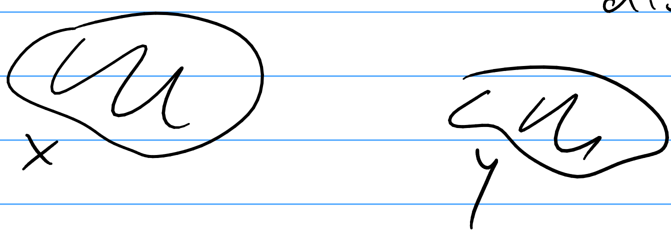
$R = \{ \text{subsets of plane} \}$

$X + Y =$ "symmetric difference"
$(X \setminus Y) \cup (Y \setminus X)$

$X \cdot Y = X \cap Y$
$1 =$ whole plane
$0 = \phi$

units? $X \cdot Y = 1$ means $X \cap Y =$ whole plane
hard to do: must have $X = Y = 1$

zero-divisors? $X \cdot Y = 0$ means $X \cap Y = \phi$
disjoint



everything but 0 and 1
is a zero-divisor.

which axiom fails if we took
$X + Y = X \cup Y$?

$\forall X \; \exists Y$ s.t. $X + Y = 0$. 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
$\exists b \in R$ such that $ab = \underline{ba = 1}$.

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-div.

in $R = \mathbb{Z}$, $a = 2$ is
neither a unit
nor a zero-divisor.

More defs:

an <u>integral domain</u> is a commutative ring with no zero-divisors.

examples: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$
polynomial rings w/ coeffs in those

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

from last week

a <u>field</u> 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 $\underset{\sim}{\mathbb{Z}_m}$ or $\mathbb{Z}/_m$ or $\mathbb{Z}/m\mathbb{Z}$.

① low-brow definition:

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

$a+b$ = do the honest $a+b$, then reduce mod m.
$a \cdot b$ - - - - - - $a \cdot b$ - - - - —

example: in $\mathbb{Z}_{12}$, $3+11 = 2$
$3 \cdot 11 = 9$

is it a ring?

$(a+b)+c = a+(b+c)$

reduce this $+c$ → reduce again

$a +$ reduce → reduce again

works, but messy to prove.

② high-brow model.

$\mathbb{Z}_m = \{$ equivalence classes of integers (mod m) $\}$

for an integer x, the equivalence class

$\bar{x} = \{ y \in \mathbb{Z} \mid x \equiv y \pmod m \}$

$= \{ x, x+m, x-m, x \pm 2m, x \pm 3m, \ldots \}$

example:

$\mathbb{Z}_2 = \Big\{ \{\text{even numbers}\}, \{\text{odd numbers}\} \Big\}$

set with two elements,
but those elements are sets..

$$\mathbb{Z}_3 = \left\{ \begin{array}{l} \{\dots, -6, -3, 0, 3, 6, \dots\} \\ \{\dots, -5, -2, 1, 4, 7, \dots\} \\ \{\dots, -4, -1, 2, 5, 8, \dots\} \end{array} \right\}$$

how do we + and $\cdot$?

define $\bar{x} + \bar{y} = \overline{x+y}$ $\quad \bar{x} \cdot \bar{y} = \overline{xy}$

is it well-defined?

if $\bar{x} = \overline{x'}$ and $\bar{y} = \overline{y'}$
do we have $\overline{x+y} = \overline{x'+y'}$
and $\overline{xy} = \overline{x'y'}$? yes.

example: in $\mathbb{Z}_{12}$,

$\bar{3} + \overline{11} = \overline{14}$ by def

but $\overline{11} = \overline{-1}$ (same set!)

and $\bar{3} + \overline{-1} = \bar{2}$ by def.

but it's ok, because $\overline{14} = \bar{2}$

☆ Think about: $\bar{x} = \bar{y}$ is the same as $x \equiv y \pmod{n}$.

You've been reading about <u>ordered</u> rings + fields.

on $\mathbb{Z}_m$, there is no ordering that's compatible with $+$ and $\cdot$

on $\mathbb{Z}_3$, if $1 > 0$
then $1+1+1 > 0+0+0$
but $1+1+1 = 0$ ...

if $1 < 0$, same problem.

Proposition: $\bar{a} \in \mathbb{Z}_m$ is a unit
iff $\gcd(a, m) = 1$

otherwise it's a zero-divisor.

<u>Proof</u> 1) $\bar{a}$ 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 $\gcd(a, m) = 1$.

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

interlude

example: in $\mathbb{Z}_{10}$,
$\bar{3}$ is a unit because $\gcd(3, 10) = 1$
$\bar{3} \cdot \bar{7} = \bar{1}$ in $\mathbb{Z}_{10}$

$\bar{4}$ is a zero-divisor. $\gcd(4, 10) = 2$

$\bar{4} \cdot \bar{5} = \bar{0}$

back in the proof, let $b = m/d$

then $ab = a \cdot \frac{m}{d} = \frac{a}{d} \cdot m$

is a multiple of m

so $\bar{a}\,\bar{b} = \bar{0}$ in $\mathbb{Z}_m$. $\boxtimes$