Last time: a ring is a set R

with two binary operations $+$, $\cdot$

satisfying 7 axioms:

$$a+b = b+a$$
$$(a+b)+c = a+(b+c)$$
$$\exists\ 0 \text{ s.t. } a+0=a \quad \forall a$$
$$\forall a\ \exists -a \text{ s.t. } a+-a=0$$
3 more

worksheet: some familiar properties follow from axioms

e.g. $0\cdot a = 0 \quad \forall a \in R$

proof: $\cancel{0\cdot a} = (0+0)\cdot a$
$= 0\cdot a + \cancel{0\cdot a}$

add $-(0\cdot a)$ to both sides

$$0\cdot a + -(0\cdot a) = (0\cdot a + 0\cdot a) + -(0\cdot a)$$
$$= 0\cdot a + (0\cdot a + -(0\cdot a))$$
$$0 = 0\cdot a + 0 = 0\cdot a$$

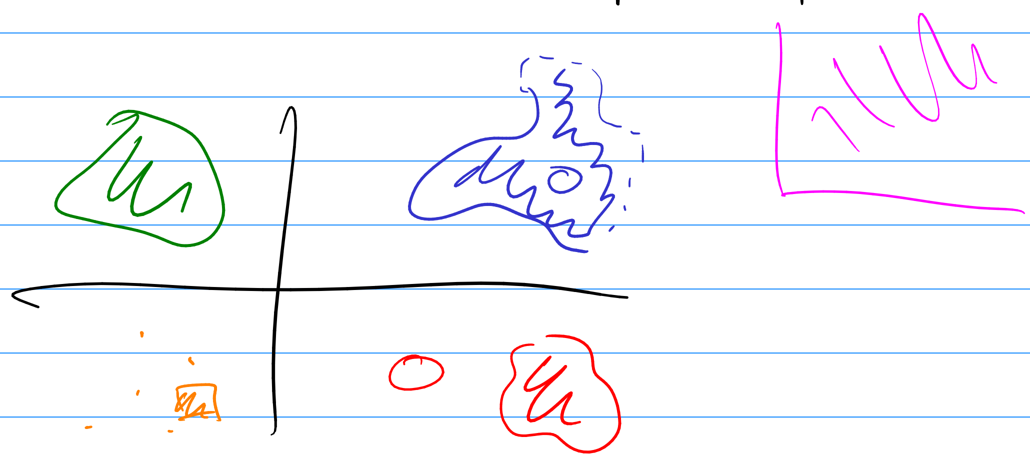
$\boxtimes$

required $1\neq 0$, but it doesn't follow that $1+1\neq 0$...

Examples of rings: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ ...
polynomial rings
matrix rings

Crazy example:

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

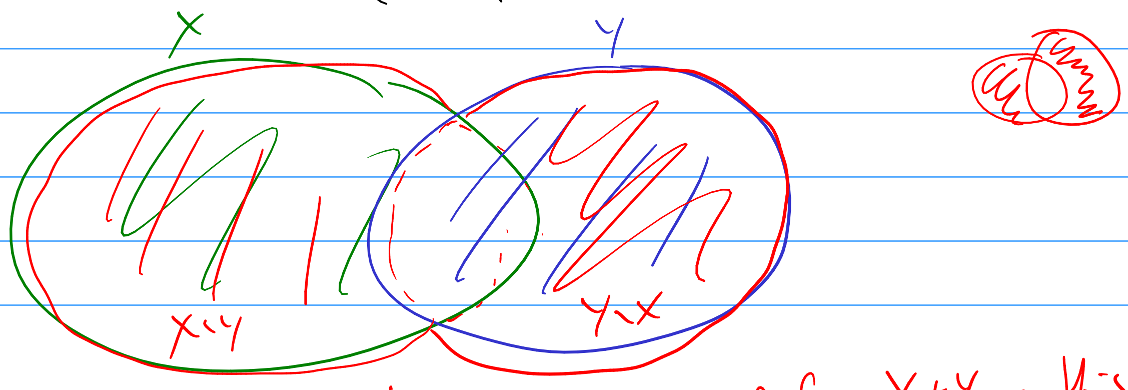


for $X, Y \subset$ plane, define

$$X+Y = (X\setminus Y)\cup(Y\setminus X)$$

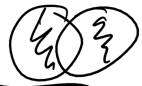
$$= \{p \mid p\in X \text{ or } Y \text{ but not both}\}$$

$$= (X\cup Y)\setminus(X\cap Y)$$



together, define $X+Y$ = this.

$X+Y = (X \setminus Y) \cup (Y \setminus X)$



define $X \cdot Y = X \cap Y$.

does this even satisfy the axioms?

mult. is associative?

$(X \cdot Y) \cdot Z = (X \cap Y) \cap Z$

$X \cdot (Y \cdot Z) = X \cap (Y \cap Z)$

same ✓

what is 1?

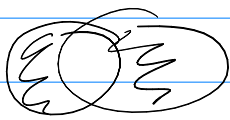
1 = some subset of plane

such that $1 \cdot X = X \quad \forall X$

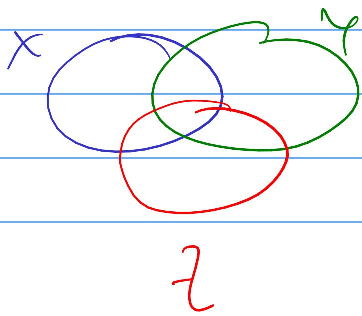
i.e. $1 \cap X = X \quad \forall X$

1 = whole plane

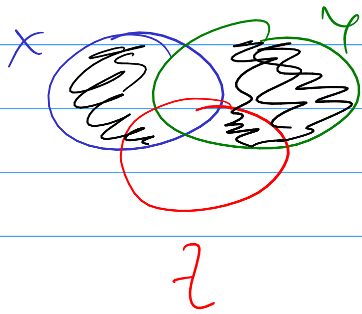
is + commutative?

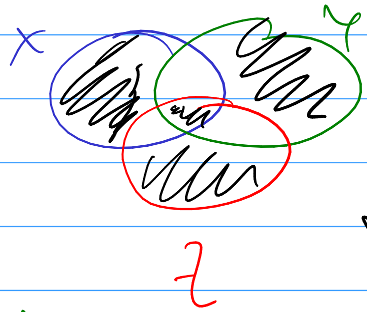
$X+Y =$  $= Y+X$

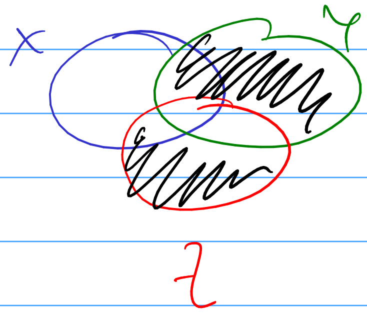
is + associative? is $(X+Y)+Z = X+(Y+Z)$



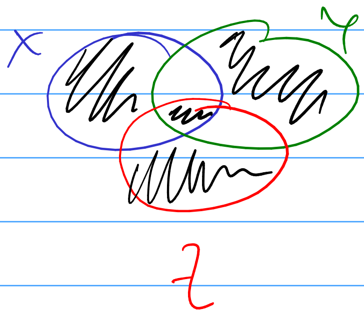
X+Y is



So $(X+Y)+Z$ is 

$Y+Z$ is 

they're the same!

$X+(Y+Z)$ is 

what is 0?
is there a set with $0+X = X \quad \forall X$

$0 =$ empty set $\emptyset$

$$(X \setminus \emptyset) \cup (\emptyset \setminus X)$$

$$= X \cup \emptyset = X.$$

what is $-X$? given X, find $-X$
with $X + (-X) = 0$

Might guess $-X =$ complement

complement

actually $X + X^c = 1$

in fact $-X = X$

$X+X = X \setminus X \cup X \setminus X = \phi \cup \phi = \phi$

distributive prop: on worksheet

Def: $a \in R$ is a unit if

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

Example: in $\mathbb{Z}$, units are ± 1

in $\mathbb{R}$, units are any nonzero #.

Def $a \in R$ is a zero-divisor

if $a \neq 0$, and
$\exists\, c \in R$ $c \neq 0$
with $ac = 0$ or $ca = 0$

Example: in $\mathbb{Z}$ and $\mathbb{Q}$, there are no zero-divisors.

in $M_2(\mathbb{Z})$ or $M_2(\mathbb{R})$,

A is a zero-div. iff $\det A = 0$
(HW).

next time: $\mathbb{Z}_m$.