Week 6

We have lectures next week!

Assessed coursework deadline

11 am next Monday!

Last week

A ring is a set R

with $+$ (addition)

$\times$ (multiplication)

(R+0) If $a, b \in R$, $a+b \in R$

(R+1) If $a, b, c \in R$,

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

(R+2) $\exists\, 0 \in R$ s.t. $0+a = a+0 = a$ $\forall\, a \in R$

(R+3) $\forall\, a \in R$, there exists $b \in R$

s.t. $a+b = b+a = 0$

(R+4) If $a, b \in R$,

$$a+b = b+a$$

(R+0) — (R+4) tells you that

$(R, +)$ is an abelian group.

(A ring, by definition, is an abelian group)

(R×0) If $a, b \in R$,

$$a \times b \in R$$
$$\parallel$$
$$ab$$

(R×1) If $a, b, c \in R$

then $a \times (b \times c) = (a \times b) \times c$

$(R \times +)$ If $a, b, c \in R$,

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

$(R + \times)$

$$(b + c) \times a = b \times a + c \times a.$$

Remark $(R, \times)$ is NOT a group!

because there is no identity element w.r.t. $\times$.

Def If $\forall a, b \in R$

& $ab = ba$, then R is called a commutative ring.

Examples

- $\{0\}$ with addition $0+0=0$
  multiplication $0 \times 0 = 0$

- $(\mathbb{Z}, +, \times)$ is a commutative ring.

- $(\mathbb{Z}_n, +, \times)$ —"—
  $\mathbb{Z}_n = \{[0]_n, [1]_n, \cdots [n-1]_n\}$

- If $(G, *)$ is an abelian group,
  then $(G, *, \times)$ is a ring
  $\underbrace{*}_{\text{this is my choice of "+"}}$

where $\forall a, b \in G$,

$$a \times b = e$$

the identity element of G.

$(R \times +)$ $a \times (b+c) = a \times b + a \times c$

LHS $a \times (b+c) = e$

RHS $a \times b = e$

$a \times c = e$

$$a \times b + a \times c = e + e$$

$$= e$$

because $(G, *)$ is a group.

- $\mathbb{Z}[i] := \{a+bi \mid a, b \in \mathbb{Z}\}$

  $i = \sqrt{-1}$

- $M_2(\mathbb{R}) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| \ a, b, c, d \in \mathbb{R} \right\}$

  is a non-commutative ring.

- $\mathbb{R}[X]$ = the set of polynomials in one variable X with coeffs in $\mathbb{R}$.

I'll come back to this example

more in details in week 8

- If $(R, +_R, \times_R)$

$(S, +_S, \times_S)$

the Cartesian product of R & S

(i.e. the set of ordered pairs of elements in R & S),

$$R \times S = \{ (r, s) \mid r \in R, \; s \in S \}$$

is a ring with respect to

$$(r, s) + (r', s') = (r +_R r', \; s +_S s')$$

$r, r' \in R$

$s, s' \in S$

$$(r,s) \times (r', s') = (r \times_R r', s \times_S s')$$

$$\mathbb{R}^2 = \{(r,s) \mid r, s \in \mathbb{R}\}$$

- The set of all functions

$$\mathbb{R} \to \mathbb{R}$$

defines a ring

$$f, g : \mathbb{R} \to \mathbb{R}$$

$$(f+g) : \mathbb{R} \to \mathbb{R}$$

$$x \mapsto f(x) + g(x)$$

$$fg : \mathbb{R} \to \mathbb{R}$$

$$x \mapsto f(x)g(x)$$

The "0", i.e. the identity element w.r.t. addition $(R+2)$

is

$$\begin{array}{ccc} \mathbb{R} & \to & \mathbb{R} \\ \cup\!\!\shortmid & & \cup\!\!\shortmid \\ x & \mapsto & 0 \end{array}$$

I gave you a couple of non-examples!

Recall that $(R, +)$

is an abelian group.

Prop 15 Let $(R, +, \times)$ be a ring.

- The zero element, i.e. the identity element w.r.t. $+$ in $(R,+)$, is unique.

- Any element in R has a unique inverse w.r.t. $+$

If $a \in R$, $\exists!\, b \in R$

there exists a unique element

s.t. $a+b=b+a=0$

- If $a+b=a+c$,

then $b=c$.

Prop 16 For every element a in R,

$$a \times 0 = 0 \times a = 0$$

Hint: Use R+2!

$\Downarrow$ $\exists\, 0$ s.t. $a+0=0+a$

$=a$

$\forall a \in R$

Letting $a=0$ itself,

we get $0+0=0$

Multiplying both sides by $a \in R$,

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

$$\overset{\parallel\,(R\times +)}{} \qquad \overset{\parallel\,(R+2)}{}$$

$$a \cdot 0 + a \cdot 0 \qquad\qquad a \cdot 0 + 0$$

R+2 $(a \cdot 0) + 0 = 0 + (a \cdot 0)$

$$\parallel$$

$$a \cdot 0$$

Last assertion of Prop 15 says

$$a \cdot 0 = 0$$

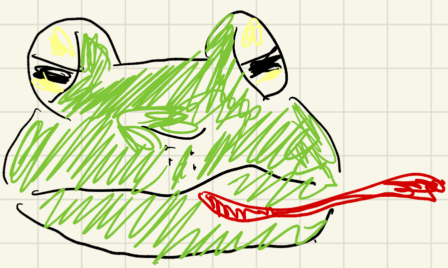
Similar for $0 \cdot a = 0$

(Exercise).

(R+2)

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

$$= (a\cdot 0)$$



Up until now, we've only looked at "additive" structures.

We'll now look at "multiplicative" structures.

Def Let $(R, +, \times)$ be a ring.

If R has an element "1" s.t. $a \times 1 = 1 \times a = a$ $\forall a \in R$

then we say that R is a ring

with identity element

By this "identity", we mean the multiplicative identity (rather than the additive identity "0" in R+2)

Examples

- $(\mathbb{Z}, +, \times)$ is a commutative ring with identity "1".
- $(\mathbb{Q}, +, \times)$ — " —

- $(\mathbb{R}, +, \times)$ — " —

- $\{0\}$ is a ring with identity 0

  because it is *defined* that

  $$0 \times 0 = 0.$$

- If R is a ring with identity,

then the set $M_2(R)$ of 2-by-2 matrices with entries in R is a ring

with identity $\begin{pmatrix} 1_R & 0 \\ 0 & 1_R \end{pmatrix}$

the identity element of R prescribed by the assumption

Theorem 17

$\mathbb{Z}_n :=$ the set of equivalence classes $[a]_n$ w.r.t ($\equiv$ mod n) is a (commutative) ring with identity $[1]$.

Pf

$$[1][a] \overset{\text{def.}}{=} [1 \cdot a] = [a]$$

$$[a][1] = [a \cdot 1] = [a].$$

Find rings without identity element !

- The set $2\mathbb{Z} := \{2z \mid z \in \mathbb{Z}\}$ of even integers is a ring without identity.

(because 1 is <u>NOT</u> an even integer)

- $R = \{ \underset{\text{continuous}}{f : \mathbb{R} \to \mathbb{R}} \mid \int_0^\infty f(x)\,dx < \infty \}$

with addition & multiplication
as defined earlier.

is a ring without identity

because the identity function

$$\begin{array}{ccc} \mathbb{R} & \to & \mathbb{R} \\ \in & & \in \\ x & \mapsto & 1 \end{array}$$

$$\int_0^\infty 1 = \infty$$

so this function does NOT

belongs to R.

<u>Def</u> Let $(R, +, \times)$ be a ring <u>with identity</u> 1.

An element a in R is called a <u>unit</u> if $\exists\, b \in R$ s.t. $ab = ba = 1$.

In other words,

$$\{\text{units in } R\} = \left\{\begin{array}{l}\text{elements in } R \\ \text{with multiplicative}\end{array}\right\}$$

inverses!

Def Let $R^\times$ denote the set of units in $(R, +, \times)$ with identity.

Exercise

- $\mathbb{Z}^\times$
- $M_2(\mathbb{R})^\times$

I'm looking for an integer $a \in \mathbb{Z}$ s.t. $\exists\, b$ $\boxed{ab = ba = 1}$

This says!

a & b are integers that divide 1.

- $\mathbb{Z}[i]^\times = \{ a+bi \quad i^2=-1 \quad a,b \in \mathbb{Z} \}$

They are $\{\pm 1\}$.

$M_2(\mathbb{R})^\times$

$M_2(\mathbb{R})$ a ring with identity

$$1_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

The units are $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{R})$

s.t. $\exists \; B \in M_2(\mathbb{R})$

s.t. $AB = BA = I_2$

These matrices are called

invertible matrices, i.e.

$$\begin{array}{ccc} A & \text{with} & \det A \neq 0 \\ \| & & \| \\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} & & ad-bc \end{array}$$

In fact, if $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with $ad-bc \neq 0$

then $B = \dfrac{1}{ad-bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$

works!

Need to check

$$AB = BA = 1$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \frac{1}{ad-bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

$$= \frac{1}{ad-bc} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

$$= \frac{1}{ad-bc} \begin{pmatrix} ad-bc & \overset{0}{\overset{\shortparallel}{-ab+ab}} \\ \underset{0}{\underset{\shortparallel}{dc-dc}} & -bc+ad \end{pmatrix}$$

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

- $\mathbb{Z}[i]^\times$?

I'm looking for

$a+bi$ s.t. $\exists$ $c+di$

$a,b \in \mathbb{Z}$ $c,d \in \mathbb{Z}$

$$(a+bi)(c+di) = \underset{\substack{1+0i \\ \shortparallel}}{1}$$

$$|r+si| = \sqrt{r^2+s^2}$$

$\downarrow$ Taking the absolute values on both sides

$$(a^2+b^2)(c^2+d^2) = 1.$$

i.e. $a^2+b^2 = 1$,

$\Rightarrow$ (a,b) is either $(1,0)$, $(0,1)$, $(-1,0)$, $(0,-1)$

$\Rightarrow$ Therefore

$$\mathbb{Z}[i]^{\times} = \{1, -1, i, -i\}$$

Homework untill Friday

Read up to Theorem 21

$$a * e = a$$

$$e * a = a$$