Last Monday.

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

If R has an element "1"

which statisfies the property :

$$1 \times a = a \times 1 = a \quad \forall a \in R$$

then we say that R has identity.

"0" the identity element w.r.t "$+$" in $R+2$

is often called the additive identity

"1" is often called the multiplicative identity.

<u>Example</u> $\mathbb{Z}_n$

$[1]$ is the identity

<u>Def</u> If $(R, +, \times)$ is a ring with identity 1

an element a in R is called a unit in R

if $\exists\, b \in R$ s.t.

$$a \times b = b \times a = 1.$$

<u>Def</u> $R^{\times} :=$ the set of units in R.

Examples

$$\mathbb{Z}^\times = \{\pm 1\}.$$

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

$$i^2 = -1$$

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

GOAL $(R, +, \times)$ is a ring with identity.

$(R^\times, \times)$ is a group.

Proposition 19 $(R, +, \times)$ a ring

with identity 1.

- The identity 1 is unique.

- If 1 is distinct from the additive identity 0, then 0 is not a unit.

- 1 is a unit & its inverse w.r.t. $\times$ is 1 itself

Pf Look at Prop 14 for inspiration.

Suppose r & s are elements in R

(1) s.t. $ra = ar = a \quad \forall a \in R$

$sa = as = a \quad \forall a \in R$

GOAL $r = s$.

Letting $a = s$ in the former, I get

$$rs = s$$

Similarly, $a = r$ in the latter, I get

$$rs = r$$

Combining those two, $s = r$.

(2) Suppose that 0 is a unit

(GOAL: find contradiction)

By definition, there exists $a \in R$

s.t. $$a \cdot 0 = 0 \cdot a = 1.$$

OTOH, Prop 16 says

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

Combining these two,

we get $0 = 1$

This contradicts the assumption $0 \neq 1$.

(3) Since 1 is the identity,

$$1 \times a = a \times 1 = a \quad \forall a \in R.$$

In particular:

$$1 \times 1 = 1.$$

This equality says that 1 is the inverse of 1 w.r.t. $\times$.

Prop 20 $(R, +, \times)$ is a ring with identity 1.

- If a is a unit, then its inverse is unique.

The inverse is written as

a^{-1}.

- If a is a unit,

  then so is a^{-1}.

The inverse of the inverse a^{-1} of a

is a.

$$(a^{-1})^{-1} = a.$$

- If a & b are units, then

so is $ab = a \times b$ & the inverse of

ab is $b^{-1} a^{-1}$.

Pf: See notes!

They all follow from Prop 14.

Theorem 21.

If $(R, +, \times)$ is a ring with identity,

then $(R^\times, \times)$ is a group.

If, in particular, R is a commutative ring,

then $(R^\times, \times)$ is an abelian group.

Exercise $(\mathbb{Z}, +, \times)$

is a ring of integers.

Define new addition

$$a \boxplus b = a + b + 1$$

old addition "+"

$$a \boxtimes b = a + b + ab$$

$\forall\, a, b \in \mathbb{Z}$

old addition "+"

old "×"

$(\mathbb{Z}, \boxplus, \boxtimes)$ is a commutative ring with identity.

(R+0) $a \boxplus b \in \mathbb{Z}$

$=$

$a+b+1$

(R+1)

$a \boxplus (b \boxplus c) = a \boxplus (b+c+1)$

$= a+(b+c+1)+1$

$= ?$

$(a \boxplus b) \boxplus c = (a+b+1) \boxplus c$

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

$= (a+b+1)+c+1$

(R+2) I need to look for

b s.t. $a \boxplus b = a$

$\Leftrightarrow \quad a+b+1 = a$

$\Leftrightarrow \quad b = -1.$

-1 is the identity element w.r.t. $\boxplus$.

Indeed,

$$a \boxplus (-1) = a + (-1) + 1 = a$$

$$(-1) \boxplus a = (-1) + a + 1 = a$$

(R+3) Given a in $\mathbb{Z}$

I need to find b in $\mathbb{Z}$

s.t. $a \boxplus b = -1$.

This is the identity w.r.t. $\boxplus$.

i.e. $a + b + 1 = -1$

$\Leftrightarrow \quad b = -a-2$

Need to check

$$a \boxplus (-a-2) = (-1)$$

$$(-a-2) \boxplus a = (-1),$$

$(R \times 0)$

$(R \times 1)$ $\quad a \boxtimes (b \boxtimes c)$

$\boxtimes$

$$= a \boxtimes (b + c + bc)$$

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

$(a \boxtimes b) \boxtimes c$

$$= (a + b + ab) \boxtimes c$$

$$=$$

$(a+b+ab)+c$

$+ (a+b+ab)\cdot c$

The multiplicative identity w.r.t X

is 0 !