

Assessed coursework 1

hand in your work by

11 am, 4th of March

The problem set can be found in
the Week 5 tab of the MTH 4104
QMplus page.

Last week, I defined:

Def A group $(G, *)$

is a set G

with operation $*$

satisfying

(G0) if $a, b \in G,$

$$a * b \in G$$

(G1) if $a, b, c \in G.$

$$a * (b * c) = (a * b) * c$$

(G2) There is an element e of G

$$\text{s.t. } e * a = a * e = a$$

$$\forall a \in G$$

(G3) For every element a in G ,

there exists $b \in G$ s.t.

$$a * b = b * a = e.$$

If $(G, *)$ satisfies

$$(G4) \forall a, b \in G, \quad a * b = b * a,$$

we call it an abelian group.

Prop 14 $*$ the identity element in (G2) is unique.

* The inverse of a is unique.

$$\forall a \in G$$

and two more assertions.

Rings

Def A ring is a set R

which comes equipped with two operations

$+$ (addition)

\times (multiplication)

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

then $a+b \in R$.

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

then $a+(b+c) = (a+b)+c$
in R .

(R+2) There is an element 0 in R

satisfying $a+0 = 0+a = a$

$\forall a \in R$.

(R+3) For every element a in R

there exists b in R st.

$$a+b = b+a = 0$$

$$(R+4) \quad \forall a, b \in R,$$

$$a+b = b+a.$$

$$(R \times 0) \quad \forall a, b \in R$$

$$a \times b \in R.$$

(R x 1) If a, b, c are elements in R ,

$$\text{then } a \times (b \times c) = (a \times b) \times c$$

(R x +) If $a, b, c \in \mathbb{R}$, then

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

(R + x) If $a, b, c \in \mathbb{R}$, then

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

Note that

$a \times (b + c)$ is not necessarily
same as $(b + c) \times a$

PK By (R+0) - (R+4),

$$(G, *) = (R, +)$$

is a group

(A ring is a group)

Rk I shall write ab

for $a \times b$ from now
on

Def A ring $(R, +, \times)$

is a commutative ring

if $\forall a, b \in R, ab = ba$.

Examples

0, or the identity element

writes " $+$ ",

needs to be in a ring R .

- $\{0\}$ $0 + 0 = 0$
 $0 \times 0 = 0$

This is the smallest possible ring.

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

- The set $\mathbb{C}[X]$ of polynomials

in one variable X with coeffs in \mathbb{C} ,

$$C_n X^n + C_{n-1} X^{n-1} + \dots + C_1 X + C_0$$

$$C_i \in \mathbb{C}$$

$$(X^2 + X + 1) + (X^3 + 3X)$$

$$= X^3 + X^2 + 4X + 1 \quad \text{etc.}$$

$$(X + 1)X$$

$$= X^2 + X \quad \text{etc.}$$

• The set $M_2(\mathbb{C})$ of 2-by-2

matrices with entries in \mathbb{R}

is a ring:

$$+ : \begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} a+a' & b+b' \\ c+c' & d+d' \end{pmatrix}$$

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

\uparrow

$M_2(\mathbb{R})$

$$\times : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in M_2(\mathbb{R})$$

$$= \begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{pmatrix}$$

$$0 : \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in M_2(\mathbb{R})$$

X to be $\forall a, b \in G$

$$a \times b = e$$

where e is the identity element

in $(G, *)$.

Then $(G, \begin{matrix} + \\ \text{"} \\ * \end{matrix}, X)$ is a commutative ring.

because $ab = e$

$$ba = e$$

so $ab = ba = e$.

- $\mathbb{R} =$ the set of non-negative integers
 $0, 1, 2, \dots$
 $+$
 \times as we know for integers

Is $(\mathbb{R}, +, \times)$ a ring?

This is not a ring. It fails on $(\mathbb{R}+3)$

First of all, 0 is 0 in $(\mathbb{R}+2)$ but 2

- $\mathbb{R} =$ the set of positive integers does NOT
 $1, 2, 3, \dots$ but
 $+$
 \times as we know then $2+b=0$
 $\in \mathbb{R}$

Is this $(\mathbb{R}, +, \times)$ a ring? /

(-2) is NST

a non-negative
integer.

This is not a ring either

because 0 is NST in \mathbb{R}

& $(\mathbb{R}+2)$ does NST hold.

• $\mathbb{Z} = \sqrt{-1}$

$$\mathbb{Z}[i] := \left\{ a + bi \mid \begin{array}{l} a, b \\ \in \\ \mathbb{Z} \end{array} \right\}$$

$$+ : (a + bi) + (a' + b'i)$$

$$= \underbrace{(a + a')}_{\in \mathbb{Z}} + \underbrace{(b + b')}_{\in \mathbb{Z}} i$$

$$\times : (a + bi)(a' + b'i)$$

$$= \underbrace{(aa' - bb')}_{\in \mathbb{Z}} + \underbrace{(a'b + ab')}_{\in \mathbb{Z}} i$$

$$0 \text{ (as in } \mathbb{R}+2) : 0 + 0i \\ \parallel \\ 0$$

This is called the ring of
Gaussian integers \mathbb{Z}