Next Monday

Revision for Week 4 - Week 9

+

module trailer (MTH 5130 Number Theory)

<u>No lectures</u> on 29/03 (Next Friday)

01/04

§6 Matrices.

Let $(R, \underline{\underline{+}}, \times)$ be a ring.

<u>Def</u> Let

$M_2(R)$ be the set of matrices

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad a, b, c, d \in R$$

with addition $\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$

definition

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

$+$ in R

multiplication

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

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

$a \times a'$

wrt $\times$ of R

Theorem 34

$M_2(R)$ is a ring.

If R is a ring with identity,

(i.e. $\exists\, 1_R$ s.t.

$a \times 1 = 1 \times a = a$)

then $M_2(R)$ is a ring with identity.

RK.

The identity w.r.t. $+$ in $M_2(R)$

$$\begin{pmatrix} 0_R & 0_R \\ 0_R & 0_R \end{pmatrix}$$

where 0_R := the identity element w.r.t. $+$ of R.

$(R+2)$

If R is a ring with identity 1_R

then $M_2(R)$ has $\begin{pmatrix} 1_R & 0_R \\ 0_R & 1_R \end{pmatrix}$

as its (multiplicative) identity.

Indeed,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1_R & 0_R \\ 0_R & 1_R \end{pmatrix}$$

$$= \begin{pmatrix} a \cdot 1_R + b \cdot 0_R & a \cdot 0_R + b \cdot 1_R \\ c \cdot 1_R + d \cdot 0_R & c \cdot 0_R + d \cdot 1_R \end{pmatrix}$$

$a \cdot 1_R = a$

because 1_R is the identity

$$= \begin{pmatrix} a + 0_R & 0_R + b \\ c + 0_R & 0_R + d \end{pmatrix}$$

Prop 16

$b \cdot 0_R = 0_R \cdot b$

$= 0_R$

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

Ex Check $\begin{pmatrix} 1_R & 0_R \\ 0_R & 1_R \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}$

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

Rk Contrary to $R[x]$, (Compare this with Thm 25)

even if R is commutative

(i.e. $ab = ba$ $\forall a, b \in R$)

$M_2(R)$ is <u>never</u> commutative.

Let's see this in an example.

Let $R = \mathbb{F}_2 = \{ [0]_2 , [1]_2 \}$

$$A = \begin{pmatrix} [1] & [1] \\ [0] & [1] \end{pmatrix} \in M_2(\mathbb{F}_2)$$

$$B = \begin{pmatrix} [1] & [1] \\ [1] & [1] \end{pmatrix} \in M_2(\mathbb{F}_2)$$

$$AB = \begin{pmatrix} [1] & [1] \\ [0] & [1] \end{pmatrix} \begin{pmatrix} [1] & [1] \\ [1] & [1] \end{pmatrix}$$

$$= \Big(\; [1]\cdot[1] + [1][1] = [1] + [1] \qquad 0$$

$$0 \qquad\qquad = [2] = [0] \qquad 0$$

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

$$BA = \begin{pmatrix} [1] & [1] \\ [1] & [1] \end{pmatrix} \begin{pmatrix} [1] & [1] \\ [0] & [1] \end{pmatrix}$$

$$= \begin{pmatrix} \begin{array}{l} [1][1] + [1][0] \\ = [1] + [0] = [1] \end{array} & \begin{array}{l} [1][1] + [1][1] \\ = [1] + [1] \\ = [2] = [0] \end{array} \\ \begin{array}{l} [1][1] + [1][0] \\ = [1] + [0] = [1] \end{array} & \begin{array}{l} [1][1] + [1][1] \\ = [1] + [1] \\ = [2] = [0] \end{array} \end{pmatrix}$$

$$= \begin{pmatrix} [1] & [0] \\ [1] & [0] \end{pmatrix} \leftarrow$$

So $AB \neq BA$

Therefore $M_2(\mathbb{F}_2)$ is not a commutative ring.

Prop 35 $(R, +, \times)$ a ring.

If R is a ring with identity

but not a ring with the property

that $\forall a, b \in R$

$ab = 0_R$,

then $M_2(R)$ is neither commutative

nor a division ring.

a ring that satisfies all the axioms of a field needs to satisfy except

$ab = ba \quad \forall_{a,b} \in R.$

Rk An example of a ring excluded above

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

Define $(R, +, \times)$

by $a + b = a * b \quad \forall_{a,b} \in G$

$a \times b = e$

the identity of G

$(|G| \geq 2)$

Rk An example of a ring that is considered in Prop 35 is a field!

Since $\mathbb{F}_2$ is a field,
$(\mathbb{F}_p)$
Prop 35 is consistent with the example.

Pf The assumption amounts to: there exist $a, b \in R$

$ab \neq 0$

By Prop 16, neither a nor b is 0.

(If it were, then $ab = 0$)

To show that $M_2(R)$ is not commutative,

$$\underbrace{\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}}_{\substack{\shortparallel \\ A}} \underbrace{\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}}_{\substack{\shortparallel \\ B}} = \begin{pmatrix} 0 & ab \\ 0 & 0 \end{pmatrix}$$

$a \cdot 0 + 0 \cdot 0 = 0 + 0$

$$\underbrace{\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}}_{\substack{\shortparallel \\ B}} \underbrace{\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}}_{\substack{\shortparallel \\ A}} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = 0 \quad (R+2)$$

Since $ab \neq 0$, $AB \neq BA$.

Therefore $M_2(R)$ is not commutative

To show that $M_2(R)$ is not a division ring,

find an element in $M_2(R)$ that does NOT have multiplicative inverse in $M_2(R)$.

More precisely, the matrix

$$\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}$$

does NOT have a multiplicative inverse,

i.e. no matrix $B \in M_2(R)$

satisfies $\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} B = \begin{pmatrix} 1_R & 0_R \\ 0_R & 1_R \end{pmatrix}$

$\nearrow$

$\rightarrow B \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1_R & 0_R \\ 0_R & 1_R \end{pmatrix}$

To prove this, suppose for a contradiction that such a matrix B exists.

(If this leads to a contradiction, we win)

$$B\left(\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}\right) = B\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

(RX1)

$$\| $$

$$\left(B\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}\right)\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$$

$$\| $$

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \quad \#$$

Since $a \neq 0$,

we have a contradiction $\square$