18.10.2021

Seminar W3 – 916

Def: $(R, +, \cdot)$ ring

- $(R, +)$ abelian group
- $(R, \cdot)$ semigroup
  (if $(R,\cdot)$ monoid $\Rightarrow$ unital ring)
- distributivity: $\forall x,y,z \in R$: $x\cdot(y+z) = x\cdot y + x\cdot z$
  $(x+y)\cdot z = xz + yz$
- if $\cdot$ commutative $\Rightarrow$ commutative ring
- if $\forall x \in R\setminus\{0\}$: $\exists x^{-1}$: $x\cdot x^{-1} = x^{-1}\cdot x = 1$
  $\Rightarrow$ division ring (= "corp")
  (skew field)
- if $(R,+,\cdot)$ unital, commutative, division ring
  $\Rightarrow$ field (= "corp comutativ")

Ex.: $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{C}$, $\mathcal{C}([0,1])$

Def/Th. $(G,\cdot)$ group, $H \subseteq G$

$H \leq G$ (subgroup of) $\iff$ (i) $H \neq \emptyset$
(ii) $\forall x,y \in H$: $xy^{-1} \in H$
$\forall x,y \in H$: $xy \in H$
$\forall x \in H$: $x^{-1} \in H$

$(R,+,\cdot)$ ring, $S \subseteq R$

$S \leq R$ (subring of) $\iff$
(i) $S \neq \emptyset$
(ii) $(S,+) \leq (R,+)$: $\forall x,y \in S$: $x - y \in S$ ($\underset{||}{x+(-y)}$)
$\forall x,y \in S$: $x+y \in S$
$\forall x \in S$: $-x \in S$
(iii) $(S,\cdot)$ stable part of $(R,\cdot)$: $\forall x,y \in S$: $xy \in S$

5. Let $n \in \mathbb{N}$, $n \geq 2$. Prove that:
(*i*) $GL_n(\mathbb{C}) = \{A \in M_n(\mathbb{C}) \mid det(A) \neq 0\}$ is a stable subset of the monoid $(M_n(\mathbb{C}), \cdot)$;
(*ii*) $(GL_n(\mathbb{C}), \cdot)$ is a group, called the *general linear group of rank n*;
(*iii*) $SL_n(\mathbb{C}) = \{A \in M_n(\mathbb{C}) \mid det(A) = 1\}$ is a subgroup of the group $(GL_n(\mathbb{C}), \cdot)$.

(you can use the fact that $\det(AB) = \det A \cdot \det B$)

Sol.: (i) $A, B \in GL_n(\mathbb{C}) \Rightarrow \det(AB) = \underbrace{\det A}_{\neq 0} \cdot \underbrace{\det B}_{\neq 0} \neq 0$

$\Rightarrow AB \in GL_n(\mathbb{C}) \Rightarrow GL_n(\mathbb{C})$ stable subset of $(M_n(\mathbb{C}), \cdot)$

(ii) We've already shown that $\cdot$ is an operation on $GL_n(\mathbb{C})$

The associativity of $\cdot$ is inherited from $(M_n(\mathbb{C}), \cdot)$

Remark: To show associativity of $\cdot$ in $M_n(\mathbb{C})$, we need the following result:

$$A = (a_{ij})_{\substack{i=\overline{1,m} \\ j=\overline{1,n}}} \qquad B = (b_{kl})_{\substack{k=\overline{1,n} \\ l=\overline{1,p}}}$$

$$\Rightarrow AB = (c_{\alpha\beta})_{\substack{\alpha=\overline{1,m} \\ \beta=\overline{1,p}}}$$

$$c_{\alpha\beta} = \sum_{h=1}^{n} a_{\alpha h} \cdot b_{h\beta}$$

$I_n \in GL_n(\mathbb{C})$, because $\det(I_n) = 1 \neq 0$

$\forall A \in GL_n(\mathbb{C}) : \exists A^{-1} = A^* \cdot \frac{1}{\det A} \in GL_n(\mathbb{C})$
(because: $A \cdot A^{-1} = I_n \Rightarrow \det A^{-1} = \frac{1}{\det A} \neq 0$)

$\left(R \text{ ring} : \quad GL_n(R) = \{ A \in M_n(R) \mid \det A \text{ is invertible in } R \} \right)$

$\Rightarrow (GL_n(\mathbb{C}), \cdot)$ group

(ii) $SL_n(\mathbb{C}) \overset{?}{\leq} GL_n(\mathbb{C})$

$SL_n(\mathbb{C}) \neq \emptyset$, because $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in SL_n(\mathbb{C})$

Let $A, B \in SL_n(\mathbb{C}) \overset{?}{\Rightarrow} AB^{-1} \in SL_n(\mathbb{C})$

It's the same as proving:

$\forall A, B \in SL_n(\mathbb{C}) \overset{?}{\Rightarrow} AB, B^{-1} \in SL_n(\mathbb{C})$

$\det(AB) = \underbrace{\det A}_{1} \cdot \underbrace{\det B}_{1} = 1 \Rightarrow AB \in SL_n(\mathbb{C})$

$\det(B^{-1}) = \dfrac{1}{\det B} = 1 \Rightarrow B^{-1} \in SL_n(\mathbb{C})$

6. Show that the following sets are subrings of the corresponding rings:
(*i*) $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ in $(\mathbb{C}, +, \cdot)$.
(*ii*) $\mathcal{M} = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \middle| a, b, c \in \mathbb{R} \right\}$ in $(M_2(\mathbb{R}), +, \cdot)$.

Sol.: 6.(ii) $\begin{pmatrix} 1 & 4 \\ 0 & 6 \end{pmatrix} \in \mathcal{M} \Rightarrow \mathcal{M} \neq \emptyset$

$(\mathcal{M}, +) \overset{?}{\leq} (M_2(\mathbb{R}), +)$

Let $A, B \in \mathcal{M}$: $A - B \in \mathcal{M}$?

$A = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$, $\quad B = \begin{pmatrix} d & e \\ 0 & f \end{pmatrix}$

$$\left.\begin{array}{l} A - B = \begin{pmatrix} a-d & b-e \\ 0 & c-f \end{pmatrix} \\ a-d,\ b-e,\ c-f \in \mathbb{R} \end{array}\right\} \Rightarrow A - B \in \mathcal{M}$$

$(\mathcal{M}, \cdot)$ stable part of $(\mathcal{M}_2(\mathbb{R}), \cdot)$

$\forall A, B \in \mathcal{M} : A \cdot B \in \mathcal{M}$?

$$\left.\begin{array}{l} A \cdot B = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \cdot \begin{pmatrix} d & e \\ 0 & f \end{pmatrix} = \begin{pmatrix} ad & ae+bf \\ 0 & cf \end{pmatrix} \\ ad,\ ae+bf,\ cf \in \mathbb{R} \end{array}\right\} \Rightarrow$$

$\Rightarrow AB \in \mathcal{M}$

$\Rightarrow \quad \mathcal{M} \leq \mathcal{M}_2(\mathbb{R})$

Def.: $(G_1, \oplus)$, $(G_2, \boxplus)$ groups, $f: G_1 \to G_2$ is a <u>group (homo)morphism</u> if:

$$\forall x, y \in G_1 : \quad f(x \oplus y) = f(x) \boxplus f(y)$$

$(R_1, \oplus, \odot)$, $(R_2, \boxplus, \boxdot)$ rings, $f: R_1 \to R_2$ is a <u>ring homomorphism</u> if: $\forall x, y \in R_1 : \begin{cases} f(x \oplus y) = f(x) \boxplus f(y) \\ f(x \odot y) = f(x) \boxdot f(y) \end{cases}$

(if R_1 and R_2 are unital rings and $f(1_{R_1}) = 1_{R_2} \to$ "unital homomorphism")

morphisms of fields have to be unital!

7. (*i*) Let $f : \mathbb{C}^* \to \mathbb{R}^*$ be defined by $f(z) = |z|$. Show that f is a group homomorphism between $(\mathbb{C}^*, \cdot)$ and $(\mathbb{R}^*, \cdot)$.

(*ii*) Let $g : \mathbb{C}^* \to GL_2(\mathbb{R})$ be defined by $g(a + bi) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$. Show that g is a group

Sol. : (i) We need to show that $\forall z_1, z_2 \in \mathbb{C}^*$:

$$f(z_1 z_2) = f(z_1) \cdot f(z_2)$$

i.e. $|z_1 z_2| = |z_1| \cdot |z_2|$

Let $z_1 = a_1 + b_1 i \qquad z_2 = a_2 + b_2 i$

$|z_1 z_2| = |(a_1 + b_1 i)(a_2 + b_2 i)| = |a_1 a_2 + a_1 b_2 i + a_2 b_1 i - b_1 b_2| =$

$= |a_1 a_2 - b_1 b_2 + (a_1 b_2 + a_2 b_1) \cdot i| = \sqrt{(a_1 a_2 - b_1 b_2)^2 + (a_1 b_2 + a_2 b_1)^2} =$

$= \sqrt{a_1^2 a_2^2 - 2a_1 a_2 b_1 b_2 + b_1^2 b_2^2 + a_1^2 b_2^2 + 2a_1 b_1 a_2 b_2 + a_2^2 b_1^2} =$

$= \sqrt{a_1^2 a_2^2 + b_1^2 b_2^2 + a_1^2 b_2^2 + a_2^2 b_1^2}$

$|z_1| \cdot |z_2| = \sqrt{a_1^2 + b_1^2} \cdot \sqrt{a_2^2 + b_2^2} = \sqrt{a_1^2 a_2^2 + a_1^2 b_2^2 + a_2^2 b_1^2 + b_1^2 b_2^2}$

$\Rightarrow \quad |z_1 z_2| = |z_1| \cdot |z_2|$

homomorphism = morphism $f : A \to B$
endomorphism = morphism $f : A \to A$
isomorphism = morphism $f : A \to B$ that is bijective
automorphism = morphism $f : A \to A$ that is bijective

10. Let $\mathcal{M} = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \middle| a, b \in \mathbb{R} \right\} \subseteq M_2(\mathbb{R})$. Show that $(\mathcal{M}, +, \cdot)$ is a field isomorphic to $(\mathbb{C}, +, \cdot)$.

<u>Sol.</u>: Let $f : \mathcal{M} \to \mathbb{C}$

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \longmapsto a+bi$$

Let $A_1 = \begin{pmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{pmatrix}$, $A_2 = \begin{pmatrix} a_2 & b_2 \\ -b_2 & a_2 \end{pmatrix}$

We will prove that
- $f(A_1 + A_2) = f(A_1) + f(A_2)$
- $f(A_1 \cdot A_2) = f(A_1) \cdot f(A_2)$
- $f(1_{\mathcal{M}}) = 1_{\mathbb{C}}$
- f bijective

$$f(A_1 + A_2) = f\left(\begin{pmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{pmatrix} + \begin{pmatrix} a_2 & b_2 \\ -b_2 & a_2 \end{pmatrix} \right) = f\left(\begin{pmatrix} a_1+a_2 & b_1+b_2 \\ -(b_1+b_2) & a_1+a_2 \end{pmatrix} \right) =$$

$$= (a_1+a_2) + (b_1+b_2) \cdot i = a_1 + b_1 i + a_2 + b_2 i = f(A_1) + f(A_2)$$

$$f(A_1 A_2) = f\left(\begin{pmatrix} a_1 & b_1 \\ -b_1 & a_2 \end{pmatrix} \cdot \begin{pmatrix} a_2 & b_2 \\ -b_2 & a_2 \end{pmatrix} \right) = f\left(\begin{pmatrix} a_1 a_2 - b_1 b_2 & a_1 b_2 + a_2 b_1 \\ -(a_1 b_2 + a_2 b_1) & a_1 a_2 - b_1 b_2 \end{pmatrix} \right)$$

$$= (a_1 a_2 - b_1 b_2) + (a_1 b_2 + a_2 b_1) \cdot i =$$

$$= a_1 a_2 + i^2 b_1 b_2 + (a_1 b_2 + a_2 b_1) \cdot i =$$

$$= (a_1 + i b_1) \cdot (a_2 + i b_2) = f(A_1) \cdot f(A_2)$$

$$1_{\mathcal{M}} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad f(I_2) = f\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 1 + 0 \cdot i = 1 = 1_{\mathbb{C}}$$

$\Rightarrow$ f morphism of fields

For any $z = a + bi \in \mathbb{C}$ $\exists$ $M = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ so that

$$f(M) = z$$

$\Rightarrow$ f surjective

For any $A_1, A_2 \in \mathcal{M}$ with $f(A_1) = f(A_2)$

$A_1 = \begin{pmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{pmatrix}, A_2 = \begin{pmatrix} a_2 & b_2 \\ -b_2 & a_2 \end{pmatrix}$

$\Rightarrow$ $a_1 + b_1 \cdot i = a_2 + b_2 \cdot i$ $\Rightarrow$ $\begin{matrix} a_1 = a_2 \\ b_1 = b_2 \end{matrix}$

$\Rightarrow A_1 = A_2$ $\Rightarrow$ f injective

$\Rightarrow$ f bij

$\Rightarrow$ f field isomorphism