12.10.2021

Seminar WZ - 911

- $(R, +, \cdot)$ ring

  set — operations

  → $(R, +)$ abelian group

  → $(R, \cdot)$ semigroup

  (if monoid $\Rightarrow$ unital ring or ring with unity)

  → distributivity:

  $\forall x, y, z \in R: \; x \cdot (y+z) = x \cdot y + x \cdot z$

  $(y+z) \cdot x = y \cdot x + z \cdot x$

  if commutativity of $\cdot$ $\Rightarrow$ commutative ring

- $(K, +, \cdot)$ field

  → $(K, +, \cdot)$ unital ring

  → $\forall x \in K \setminus \{0\} \; \exists x' : x x' = x' x = 1$

  → $\cdot$ commutative (if not, then division ring)

<u>Def</u>: $(G, \cdot)$ group, $S \subseteq G$, then:

$S \leq G \iff$ (i) $S \neq \emptyset$

(S is a subgroup of G) (ii) $\forall x, y \in S: \; x y^{-1} \in S$

$\underline{\text{Def}}$: $(R, +, \cdot)$ ring, $S \subseteq R$, then:

$S \leq R \iff$ (i) $S \neq \emptyset$

(S is a subring of R) (ii) $\forall x, y \in S: x - y \in S$

(iii) $\forall x, y \in S: x \cdot y \in S$

3.5. **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 don't have to show that $\det(AB) = \det(A)\det(B)$, it can be assumed)

$\underline{\text{Sol}}$: (i) We need to show that $\forall A, B \in GL_n(\mathbb{C}): AB \in GL_n(\mathbb{C})$

$A, B \in GL_n(\mathbb{C}) \Rightarrow \det A, \det B \neq 0 \Rightarrow \det(A)\det(B) \neq 0 \Rightarrow$

$\Rightarrow \det(AB) \neq 0 \Rightarrow AB \in GL_n(\mathbb{C})$

(ii) $GL_n(\mathbb{C}) \subseteq M_n(\mathbb{C}) \Rightarrow \cdot$ is associative

$\det(I_n) = 1 \Rightarrow I_n \in GL_n(\mathbb{C}) \Rightarrow I_n$ is the neutral element for $\cdot$ in $GL_n(\mathbb{C})$

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

$\Rightarrow$ the element (α, β) in AB is:

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

$\forall A \in GL_n(\mathbb{C}) \quad \exists A^{-1} = \frac{1}{\det(A)} \cdot A^* \in GL_n(\mathbb{C})$

$AA^{-1} = A^{-1}A = I_n$

(ii) $SL_n(\mathbb{C}) = \{A \in GL_n(\mathbb{C}) \mid \det A = 1\}$

$\det(I_n) = 1 \Rightarrow I_n \in SL_n(\mathbb{C}) \Rightarrow SL_n(\mathbb{C}) \neq \emptyset$

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

$A, B \in SL_n(\mathbb{C}) \Rightarrow \det A = \det B = 1$

$\det(AB^{-1}) = \det A \cdot \underbrace{\det(B^{-1})}$

$\det(B) \cdot \det(B^{-1}) = \det(BB^{-1}) = \det(I_n) = 1$

$\det(AB^{-1}) = \det A \cdot \underbrace{\det(B^{-1})}_{\frac{1}{\det B}} = \frac{\det A}{\det B} = 1$

$\Rightarrow AB^{-1} \in SL_n(\mathbb{C})$

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: (i) $\mathbb{Z}[i] \neq \emptyset$, because $1 \in \mathbb{Z}[i]$

$\forall z_1, z_2 \in \mathbb{Z}[i] \overset{?}{:} z_1 - z_2 \in \mathbb{Z}[i]$

Let $z_1 = a + bi$, $z_2 = c + di$, $a, b, c, d \in \mathbb{Z}$

$$z_1 - z_2 = \underbrace{(a-c)}_{\in \mathbb{Z}} + \underbrace{(b-d)}_{\in \mathbb{Z}} \cdot i \in \mathbb{Z}[i]$$

$$\forall z_1, z_2 \in \mathbb{Z}[i] : z_1 z_2 \overset{?}{\in} \mathbb{Z}[i]$$

$$z_1 = a + bi, \quad z_2 = c + di$$

$$z_1 z_2 = ac + adi + cbi + bd i^2 =$$

$$= \underbrace{(ac - bd)}_{\in \mathbb{Z}} + \underbrace{(ad + bc)}_{\in \mathbb{Z}} \cdot i \in \mathbb{Z}[i]$$

$$\Rightarrow \mathbb{Z}[i] \leq \mathbb{C}$$

<u>Remark:</u> $\mathbb{C}$ is a field, but $\mathbb{Z}[i]$ isn't a field

$$1+i \in \mathbb{C} \quad (1+i)^{-1} = \frac{1}{1+i} = \frac{1-i}{2} = \frac{1}{2} - \frac{1}{2} \cdot i \notin \mathbb{Z}[i]$$

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 homomorphism between $(\mathbb{C}^*, \cdot)$ and $(GL_2(\mathbb{R}), \cdot)$.

<u>Def</u>: $(G_1, *)$, $(G_2, \square)$ groups

$f : G_1 \to G_2$ is a group homomorphism if:

$$\forall x, y \in G_1 : f(x * y) = f(x) \square f(y)$$

$$\left(\Rightarrow f(x^{-1}) = f(x)^{-1}, \quad e_{G_2} = f(e_{G_1}) \right)$$

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 homomorphism between $(\mathbb{C}^*, \cdot)$ and $(GL_2(\mathbb{R}), \cdot)$.

Sol: 7.(ii)

Let $x = a+bi$, $y = c+di$

We will show that $g(xy) = g(x) \cdot g(y)$

$g(xy) = g((a+bi)(c+di)) = g(ac-bd+(ad+bc)\cdot i) =$

$= \begin{pmatrix} ac-bd & bc+ad \\ -bc-ad & ac-bd \end{pmatrix}$

$g(x) \cdot g(y) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \cdot \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} ac-bd & ad+bc \\ -bc-ad & -bd+ac \end{pmatrix}$

$\Rightarrow g(xy) = g(x) \cdot g(y) \Rightarrow g$ group morphism

Terminology: homomorphism = morphism $f : A_1 \to A_2$
endomorphism = morphism $f : A \to A$
isomorphism = morphism $f : A_1 \to A_2$ + bijectivity
automorphism = endo + iso = morphism $f : A \to A$ + bijectivity

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 $(\mathbb{C}, +, \cdot)$.

Sol: $(\mathcal{M}, +, \cdot)$ is a ring ?

$\longrightarrow$ $+$ is an operation on $\mathcal{M}$:

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

$$A_1 + A_2 = \begin{pmatrix} a_1 + a_2 & b_1 + b_2 \\ -b_1 - b_2 & a_1 + a_2 \end{pmatrix} \in \mathcal{M}$$

$\longrightarrow$ assoc. of $+$ is inherited

$\longrightarrow$ the neutral element, $O_2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in \mathcal{M}$

$\longrightarrow$ invertibility of $+$:

$$A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \Rightarrow -A = \begin{pmatrix} -a & -b \\ b & -a \end{pmatrix} \in \mathcal{M}$$

$$A + (-A) = O_2$$

$\longrightarrow$ commutativity of $+$ is inherited

$\longrightarrow$ $\cdot$ is an operation on $\mathcal{M}$:

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

$$= \begin{pmatrix} a_1 a_2 - b_1 b_2 & a_1 b_2 + b_1 a_2 \\ -a_2 b_1 - b_2 a_1 & -b_1 b_2 + a_1 a_2 \end{pmatrix} \in \mathcal{M}$$

→ associativity of $\cdot$ is inherited

→ the neutral element of $\cdot$ is $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in \mathcal{M}$

→ distributivity is inherited

$\Rightarrow \mathcal{M} \leq \mathcal{M}_2(\mathbb{C})$
(subring)

We will now show that $\forall A \in \mathcal{M} \setminus \{0\} \; \exists A'$:

$$AA' = A'A = I_2$$

$$A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

Let $A' = \frac{1}{a^2+b^2} \cdot A^* = \frac{1}{a^2+b^2} \cdot \begin{pmatrix} a & -b \\ b & a \end{pmatrix} =$

$$= \begin{pmatrix} \frac{a}{a^2+b^2} & \frac{-b}{a^2+b^2} \\ \frac{b}{a^2+b^2} & \frac{a}{a^2+b^2} \end{pmatrix} \in \mathcal{M}$$

$\Rightarrow \mathcal{M}$ field

We use the function:

$$g : \mathcal{M} \to \mathbb{C}$$
$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \longmapsto a+ib$$

Show that g is a field isomorphism