13.10.2021

Seminar W3 - 917

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

→ $(R,+)$ abelian group

→ $(R,\cdot)$ semigroup

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

→ distributivity:

$$\forall x,y,z \in R: \quad (x+y)\cdot z = xz+yz$$
$$z\cdot(x+y) = zx+zy$$

- if $\cdot$ is commutative $\Rightarrow$ commutative ring

- if R is unital and $\forall x \in R\setminus\{0\}: \exists x': x\cdot x' = x'\cdot x = 1$
  $\Rightarrow$ division ring

field = commutative division ring

Def: G group, $H \subseteq G$, then:

$H \leq G$ (subgroup) $\Leftrightarrow$ (i) $H \neq \emptyset$

(ii) $\forall x,y \in H: xy^{-1} \in H$

(or, if denoted additively: $\forall x,y \in H: x-y \in H$)

Def: R ring, $S \subseteq R$, then:

$S \leq R$ (subring) $\Leftrightarrow$ (i) $S \neq \emptyset$

(ii) $(S,+) \leq (R,+) \Leftrightarrow \forall x,y \in S: x-y \in S$

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

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 $(GL_n(\mathbb{C}), \cdot)$.
(special linear group)
(you can assume that $\det(AB) = \det(A) \cdot \det(B)$)

Sol.:

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

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

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

(ii) - $GL_n(\mathbb{C})$ stable subset of $(M_n(\mathbb{C}), \cdot)$

- assoc. of $\cdot$ is inherited from $M_n(\mathbb{C})$

- the neutral element of $(M_n(\mathbb{C}), \cdot)$ is I_n and $I_n \in GL_n(\mathbb{C})$

- $\forall A \in GL_n(\mathbb{C})$ $\exists A' \in GL_n(\mathbb{C})$: $AA' = A'A = I_n$

$$A' = \frac{1}{\det A} \cdot A^*$$

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

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

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

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

$\Rightarrow SL_n(\mathbb{C}) \leq GL_n(\mathbb{C})$

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). $\mathcal{M} \neq \emptyset$, because $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in \mathcal{M}$

Let $A, B \in \mathcal{M}$, $A = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ $B = \begin{pmatrix} d & e \\ 0 & f \end{pmatrix}$

$$A - B = \begin{pmatrix} a-d & b-e \\ 0 & c-f \end{pmatrix} \in \mathcal{M}$$

$$AB = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \cdot \begin{pmatrix} d & e \\ 0 & f \end{pmatrix} = \begin{pmatrix} ad & ae+bf \\ 0 & cf \end{pmatrix} \in \mathcal{M}$$

$\Rightarrow \mathcal{M} \leq M_2(\mathbb{R})$

Def: $(G_1, *)$, $(G_2, \square)$ groups, $f: G_1 \to G_2$ is a function

f is a group homomorphism if:

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

$(R_1, +, \cdot)$, $(R_2, \oplus, \odot)$ rings, $g: R_1 \to R_2$

g is a ring homomorphism if:

$$\forall x, y \in R_1: \quad f(x+y) = f(x) \oplus f(y)$$
$$f(xy) = f(x) \odot f(y)$$

Remark: if R_1, R_2 unital, then if $f(1_{R_1}) = 1_{R_2}$, then the ring homomorphism is unital homomorphism $=$ morphism $f: A \to B$

endomorphism $=$ morphism $f: A \to A$

isomorphism $=$ bijective morphism $f: A \to B$

automorphism $=$ bijective morphism $f: A \to A$

$=$ endo $+$ iso.

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.(i) $z_1 = a+bi$, $z_2 = c+di$

$$f(z_1 z_2) \overset{?}{=} f(z_1) \cdot f(z_2)$$

$$z_1 z_2 = (a+bi)(c+di) = ac + adi + bci - bd = (ac-bd) + i(ad+bc)$$

$$f(z_1 z_2) = |(ac-bd) + i(ad+bc)| = \sqrt{(ac-bd)^2 + (ad+bc)^2} =$$

$$= \sqrt{a^2c^2 + b^2d^2 - 2abcd + a^2d^2 + b^2c^2 + 2abcd} = \sqrt{a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2}$$

$$f(z_1) \cdot f(z_2) = \sqrt{a^2+b^2} \cdot \sqrt{c^2+d^2} = \sqrt{(a^2+b^2)(c^2+d^2)} =$$

$$= \sqrt{a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2}$$

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

3. Prove that $H = \{z \in \mathbb{C} \mid |z| = 1\}$ is a subgroup of $(\mathbb{C}^*, \cdot)$, but not of $(\mathbb{C}, +)$.

Sol: $|1| = 1 \Rightarrow 1 \in H \Rightarrow H \neq \emptyset$

Let $z_1, z_2 \in H$: $z_1 z_2^{-1} \overset{?}{\in} H$

$z_1, z_2 \in H \Rightarrow |z_1| = |z_2| = 1$

$|z_1 \cdot z_2^{-1}| = |z_1| \cdot |z_2|^{-1} = 1 \cdot 1 \Rightarrow z_1 z_2^{-1} \in H \Rightarrow H \leq (\mathbb{C}^\times, \cdot)$

Let $z_1 = 1$, $z_2 = i$, $|z_1| = |z_2| = 1$,

but $z_1 - z_2 = 1 - i$ and $|z_1 - z_2| = \sqrt{2} \neq 1 \Rightarrow z_1 - z_2 \notin H$

$\Rightarrow H \not\leq (\mathbb{C}, +)$

1. Let M be a non-empty set and let $S_M = \{f : M \to M \mid f \text{ is bijective}\}$. Show that $(S_M, \circ)$ is a group, called the *symmetric group* of M.

(you can assume that function composition is associative)

Sol: • $\circ$ is an operation:

$\forall f, g : M \to M$ bijective $\overset{?}{\Rightarrow} f \circ g$ bijective

• associativity: $\forall f, g, h$, let $x \in M$:

$((f \circ g) \circ h)(x) = (f \circ g)(h(x)) = f(g(h(x)))$

$(f \circ (g \circ h))(x) = f((g \circ h)(x)) = f(g(h(x)))$

$\Rightarrow (f \circ g) \circ h = f \circ (g \circ h)$

- the neutral element: $id_M : M \to M$
  $x \mapsto x$

  $\forall f \in S_M: \quad f \circ id_M = id_M \circ f = f$

- invertibility: $\forall f \in S_M \Rightarrow f$ bijective $\Rightarrow \exists f^{-1}$:

  $f \circ f^{-1} = f^{-1} \circ f = id_M$

Remark: If M is a finite set with n elements, then

$S_M = S_n$, the permutations of n elements