18.10.2021

Seminar W3-914

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

- $(R,+)$ abelian group
- $(R,\cdot)$ semigroup

  (if monoid $\Rightarrow$ unital ring)

- distributivity: $\forall x,y,z \in R$: $x\cdot(y+z) = xy + xz$
  $(x+y)\cdot z = x\cdot z + y\cdot z$

· operation
· associative

semigroup +
· has a neutral element

(if $\cdot$ is commutative $\Rightarrow$ commutative ring)

- if $\forall x \in R\setminus\{0\}$ $\exists x'$: $xx' = 1 = x'x$, then $\Rightarrow$ division ring

- $(R,+,\cdot)$ field = commutative division ring

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

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

$\underbrace{(H,\cdot) \leq (G,\cdot)}_{\text{subgroup}} \iff$ (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, $S \subseteq R$

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

$x+(-y)$

multiplication | additive

$x \cdot x = x^2$ $\quad x \cdot x^{-1} = 1$ | $x + x = 2x$ $\quad x + (-x) = 0$

$(G, *)$ $\quad x * x * x = x^3$ | $(G, \oplus)$ $\quad x \oplus x = 2x$

$x * y * y * x = xy^2x$

$x * y^{-1} * z * t = xy^{-1}zt$ | $x \oplus (-y) \oplus z \oplus t = x - y + z + t$

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 assume $\det(AB) = \det A \det B$ and that $\cdot$ is associative on $M_n(\mathbb{C})$)

Sol: (i) $\forall A, B \in GL_n(\mathbb{C})$: $A \cdot B \overset{?}{\in} GL_n(\mathbb{C})$

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

(ii) Associativity of $\cdot$ is inherited from $M_n(\mathbb{C})$

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

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

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

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

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

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

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

$$1 = \det(A \cdot A^{-1}) = \det A \cdot \det A^{-1} \Rightarrow \det A^{-1} = \frac{1}{\det A} = 1 \Rightarrow$$

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

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) $\quad 1 + 2i \in \mathbb{Z}[i] \Rightarrow \mathbb{Z}[i] \neq \emptyset$

Let $x = a + bi,\ y = c + di \in \mathbb{Z}[i] \Rightarrow a, b, c, d \in \mathbb{Z}$

$$x - y = (a + bi) - (c + di) = \underbrace{a - c}_{\in \mathbb{Z}} + \underbrace{(b - d)}_{\in \mathbb{Z}} \cdot i \in \mathbb{Z}[i]$$

$$xy = (a + bi) \cdot (c + di) = ac + adi + bic - bd =$$

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

$$\Rightarrow \quad \mathbb{Z}[i] \leqslant \mathbb{C}$$

Def: $(G_1, *)$, $(G_2, \square)$ groups, $f: G_1 \to G_2$ is called a group (homo)morphism if:

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

$(R_1, +, \cdot)$, $(R_2, \oplus, \odot)$ rings, $f: R_1 \to R_2$ is a ring homomorphism if: $\forall x, y \in R_1$:

$$f(x + y) = f(x) \oplus f(y)$$

$$f(x \cdot y) = f(x) \odot f(y)$$

(if R_1, R_2 unital rings and $f(1_{R_1}) = 1_{R_2}$

$\to$ unital ring homomorphism)

$\to$ homomorphism = morphism $f: A \to B$

endomorphism = morphism $f: A \to A$

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

automorphism = 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 $(GL_2(\mathbb{R}), \cdot)$.

<u>Sol</u> : 7.(ii) Let $z_1 = a+bi$, $z_2 = c+di$:

$$g((a+bi)(c+di)) \overset{?}{=} g(a+bi) \cdot g(c+di)$$

$$g((a+bi)(c+di)) = g(ac-bd + i(bc+ad)) = \begin{pmatrix} ac-bd & bc+ad \\ -bc-ad & ac-bd \end{pmatrix}$$

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

$$\Rightarrow g(a+bi) \cdot g(c+di) = g((a+bi)(c+di))$$

$\Rightarrow$ g group homom.

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 $\forall f, g$ bijective : $f \circ g$ bijective)

<u>Sol</u> : <u>Remark</u> : If M is finite, $|M| = n \Rightarrow S_M = S_n$

(<u>Cayley</u>: Every group is a subgroup of a group of permutations)

We check associativity: $\forall f, g, h \in S_M$: $(f \circ g) \circ h = f \circ (g \circ h)$

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 is the function $id_M : M \to M$, $x \mapsto x$

Let $x \in M$: $(f \circ id_M)(x) = f(id_M(x)) = f(x)$

$(id_M \circ f)(x) = id_M(f(x)) = f(x)$

$\Rightarrow f \circ id_M = id_M \circ f = f$

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

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

$\Rightarrow (S_M, \circ)$ group