18. 10. 2021

Seminar W3 – 915

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

- $(R,+)$ 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 $\cdot$ is commutative $\Rightarrow$ commutative ring
- if $\forall x \in R \setminus \{0\}$ $\exists x^{-1} \in R$: $xx^{-1} = x^{-1}x = 1$
  $\Rightarrow$ division ring
- if R is a commutative unital division ring $\Rightarrow$ Field

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

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

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

(ii) a. $\forall x,y \in H$: $xy \in H$

(ii) b. $\forall x \in H$: $x^{-1} \in H$

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

$(S,+,\cdot) \leq (R,+,\cdot) \iff$ (i) $S \neq \emptyset$
(subrings)

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

(ii a) $\forall x,y \in S: x+y \in S$

(ii b) $\forall x \in S: -x \in S$

(iii) $(S,\cdot)$ stable part of $(R,\cdot)$: $\forall x,y \in S: x\cdot y \in S$

Notation: Multiplicative: $\odot$ Additive

Multiplicative	Additive
$x \odot x =: x^2$	$x \oplus x = 2x$
$x \odot x \odot x = x^3$	$x \oplus x \oplus x = 3x$
$x \odot x^{-1} = 1$	$x \oplus (-x) = 0$
$(x \odot y) \odot (z^{-1} \odot t) = xyz^{-1}t$	$(x \oplus y) \oplus (-z \oplus t) = x+y-z+t$

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

(we can assume that $\det(AB) = \det A \cdot \det(B)$)

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

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

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

(ii) $(GL_n(\mathbb{C}), \cdot)$ is a group ?

$\cdot$ is an operation on $GL_n(\mathbb{C})$ (we showed this at (i))

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

if you really want to show associativity of matrix multiplication, then:

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

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

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

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

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

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

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

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

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

$\det(A) = \det B = 1$

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

$\Rightarrow \det B^{-1} = \dfrac{1}{\det B}$

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

"one-to-one"

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.

injective surjective

(you can assume that $\forall f, g \in S_M : f \circ g \in S_M$)

Sol:

Remark: If M is finite, $|M| = n$, then $S_M = S_n$

Cayley's theorem: Any finite group is a subgroup of a group of permutations.

$\forall f, g, z \in S_M : (f \circ g) \circ z = f \circ (g \circ z)$

We have to show that $\forall m \in M$:

$$((f \circ g) \circ z)(m) = (f \circ (g \circ z))(m)$$

$((f \circ g) \circ z)(m) = (f \circ g)(z(m)) = f(g(z(m)))$

$(f \circ (g \circ z))(m) = f((g \circ z)(m)) = f(g(z(m)))$

The neutral element is the identical function

$$id_M : M \to M$$
$$x \mapsto x$$

$\forall f \in S_M \Rightarrow f$ bijective $\Rightarrow f$ invertible $\Rightarrow \exists f^{-1} : f \circ f^{-1} = f^{-1} \circ f = id_M$

Remark:

$$f : \mathbb{R} \to \mathbb{R}_+$$
$$x \mapsto e^x$$

$$f(x)^{-1} = \frac{1}{e^x} \qquad f^{-1}(x) = \ln x$$

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) $\begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix} \in \mathcal{M} \Rightarrow \mathcal{M} \neq \emptyset$

Let $A_1 = \begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix} \in \mathcal{M}$, $A_2 = \begin{pmatrix} a_2 & b_2 \\ 0 & c_2 \end{pmatrix} \in \mathcal{M}$

$$A_1 - A_2 = \begin{pmatrix} a_1 - a_2 & b_1 - b_2 \\ 0 & c_1 - c_2 \end{pmatrix} \in \mathcal{M}$$

$$A_1 A_2 = \begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix} \cdot \begin{pmatrix} a_2 & b_2 \\ 0 & c_2 \end{pmatrix} = \begin{pmatrix} a_1 a_2 & a_1 b_2 + b_1 c_2 \\ 0 & c_1 c_2 \end{pmatrix} \in \mathcal{M}$$

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

Def: $(G_1, \odot)$, $(G_2, \boxdot)$ groups, $f: G_1 \to G_2$ is a group (homo)morphism if:

$$\forall x, y \in G_1: \quad f(x \odot y) = f(x) \boxdot f(y)$$

$(R_1, \oplus, \odot)$, $(R_2, \boxplus, \boxdot)$ rings $f: R_1 \to R_2$ is a ring homomorphism if

$$\forall x, y \in R_1: \quad f(x \oplus y) = f(x) \boxplus f(y)$$

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

Ex. 7