19.10.2023
Algebra - Seminar 3

1. $M \neq \emptyset$, $S_M = \{f : M \to M \mid f \text{ - bijective}\}$

$(S_M, \circ)$ - group?

- „$\circ$" - operation $\rightsquigarrow \forall f_a, f_b \in S$, $f_a \circ f_b \in S_M$

$(f_a \circ f_b)(x) = f_a(f_b(x))$
$f_b \in S \to f_b(x) \in M$
$f_a \in S \to f_a(f_b(x)) \in M$
$\Big\} \to f_a \circ f_b \in S_M$

- asociativity: $\forall f_a, f_b, f_c \in S_M$, $f_a \circ (f_b \circ f_c) = (f_a \circ f_b) \circ f_c$

$(f_a \circ (f_b \circ f_c))(x) = f_a \circ (f_b(f_c(x))) = f_a(f_b(f_c(x)))$
$((f_a \circ f_b) \circ f_c)(x) = f_a(f_b(x)) \circ f_c = f_a(f_b(f_c(x)))$
$\Big\} \to$

$\to$ „$\circ$" - asociative

- identity element: $\exists f_e \in S, \forall f \in S$, $f_e \circ f = f \circ f_e = f$

$(f_e \circ f)(x) = f_e(f(x)) = f(x)$
$(f \circ f_e)(x) = f(f_e(x)) = f(x)$
$\Big\} \to f_e(x) = x$

- inverse element

$\forall f \in S$, f - bijective $\to \exists f' \in S$ s.t. $(f \circ f')(x) = (f' \circ f)(x) = x$

2. $M \neq \emptyset$, $(R, +, \cdot)$ - ring

$R^M = \{f \mid f : M \to R\}$, $\forall f, g \in R^M$

$f + g : M \to R$, $(f+g)(x) = f(x) + g(x)$, $\forall x \in M$

$f \cdot g : M \to R$, $(f \cdot g)(x) = f(x) \cdot g(x)$, $\forall x \in M$

$(R^M, +, \cdot)$ - ring?

If R - commutative or has identity, does R^M have the same property?

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

1. $(R, +)$ - abelian group
2. $(R, \cdot)$ - semigroup
3. The distributive law holds:
   a) $x(y+z) = xy + xz$
   b) $(y+z)x = y \cdot x + z \cdot x$

- $(R^{\mathbb{N}}, +)$ - abelian group?

* commutativity: $\forall f, g \in R^{\mathbb{N}}$, $f+g = g+f$

$(g+f)(x) = g(x) + f(x) = f(x) + g(x)$ „T" ①

* asociativity: $\forall f, g, h \in R^{\mathbb{N}}$, $(f+(g+h))(x) = ((f+g)+h)(x)$

$(f + (g+h))(x) = (f + (g(x) + h(x)))(x) = f(x) + g(x) + h(x)$ } →

$((f+g)+h)(x) = ((f(x) + g(x)) + h) = f(x) + g(x) + h(x)$ }

→ „+" - asoc ②

* identity element: $\exists e \in R^{\mathbb{N}}$, $\forall f \in R^{\mathbb{N}}$, $(f+e)(x) = (e+f)(x) = f(x)$

„+" - com → $(e+f)(x) = (f+e)(x)$, $\forall e, f \in R^{\mathbb{N}}$

$(f+e)(x) = f(x) + e(x) = f(x) \rightarrow e(x) = 0$ ③

* inverse element: $\forall f \in R^{\mathbb{N}}$, $\exists f' \in R^{\mathbb{N}}$ s.t $(f+f')(x) = (f'+f)(x) = e$

„+" - comut → $(f+f')(x) = (f'+f)(x)$, $\forall f, f' \in R^{\mathbb{N}}$

$(f+f')(x) = f(x) + f'(x) = 0 \rightarrow f'(x) = -f(x) \in R^{\mathbb{N}}$ ④

From ①, ②, ③, ④ → $(R^{\mathbb{N}}, +)$ - abelian group I

- $(R^{\mathbb{N}}, \cdot)$ - semigroup

* asoc: $\forall f, g, h \in R^{\mathbb{N}}$, $(f \cdot (g \cdot h))(x) = ((f \cdot g) \cdot h)(x)$

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

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

→ $(R^{\mathbb{N}}, \cdot)$ - semigroup II

- distributivity law III

* $(f(g+h))(x) = (f(g(x)+h(x))) = f(x)\cdot(g(x)+h(x)) =$

$= f(x)\cdot g(x) + f(x)\cdot h(x)$

* $((g+h)f)(x) = (g(x)+h(x)\cdot f(x) = g(x)\cdot f(x) + h(x)\cdot f(x)$

From I, II, III, $\rightarrow (R^M, +, \cdot)$ - ring

- R^M - stable subset $\rightsquigarrow \forall f, g \in R^M,\ f\cdot g \in R^M$

$(f\cdot g)(x) = f(x)\cdot g(x)$

$f, g \in R^M \rightarrow \begin{matrix} f(x)\in R \\ g(x)\in R \end{matrix} \Big\} \rightarrow f(x)\ g(x) \in R,\ \forall x \in M \rightarrow$

$\rightarrow (f\cdot g)(x) \in R^M \rightarrow R^M$ - stable subset

$\left.\begin{matrix} R^M \text{ - stable subset} \\ R \text{ - commutative} \end{matrix}\right\} \rightarrow R^M$ - commutative (the commutative law holds to all the subsets of R)

Let 1_R be the identity element of R. Then $f: M \to R$, $f(x) = 1_R,\ \forall x \in M$ is the identity element of R^M.

3. $H = \{z \in \mathbb{C} \mid |z| = 1\}$

H - subgroup of $(\mathbb{C}^*, \cdot)$, but not of $(\mathbb{C}, +)$

H - subgroup of $(\mathbb{C}^*, \cdot)$ if:

1. $H \neq \emptyset$ ($1 \in H$ the identity element of "$\cdot$")
2. $\forall x, y \in H : x\cdot y \in H$
3. $\forall x \in H : x^{-1} \in H$

$\Big\} \rightsquigarrow \forall x, y \in H,\ x\cdot y^{-1} \in H$

The identity element of "$\cdot$" is $1 \in H$ because $|1| = 1$

Let $z_1, z_2 \in H \rightarrow |z_1| = |z_2| = 1$

$|z_2^{-1}| = \frac{1}{|z_2|} = \frac{1}{1} = 1$ $\Big\} \rightarrow$

$\rightarrow |z_1|\cdot|z_2^{-1}| = |z_1|\cdot\frac{1}{|z_2|} = 1\cdot\frac{1}{1} = 1\cdot 1 = 1 \in H \rightarrow z_1\cdot z_2^{-1} \in H$ $\Big\} \rightarrow$

$\rightarrow$ H - subgroup of $(\mathbb{C}^*, \cdot)$

H - subgroup of $(\mathbb{C}, +)$?

The identity elem for "+" is 0 and $|0| = 0 \notin H \rightarrow$

$\rightarrow$ H - is not a subgroup of $(\mathbb{C}, +)$

Hw: 4. $U_n = \{ z \in \mathbb{C} \mid z^n = 1 \}$

U_n - subgroup of $(\mathbb{C}^*, \cdot)$?

$U_n = \{ z_k \mid k = \overline{0, n-1} \}$

$z_k = \cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n}$

The identity el of "$\cdot$" $= 1 = \cos \frac{2 \cdot 0\pi}{n} + i \cdot \sin \frac{2 \cdot 0\pi}{n} \in U_n \rightarrow$

$\rightarrow U_n \neq \emptyset$

Let $z_x, z_y \in U_n$

$z_x \cdot z_y^{-1} = \left(\cos \frac{2x\pi}{n} + i \cdot \sin \frac{2x\pi}{n} \right) \cdot \frac{1}{\cos \frac{2y\pi}{n} + i \cdot \sin \frac{2y\pi}{n}}$

Hw: 5. $n \in \mathbb{N}$, $n \geq 2$

(i) $GL_n(\mathbb{C}) = \{ A \in M_n(\mathbb{C}) \mid \det(A) \neq 0 \}$ - stabel subset of $(M_n(\mathbb{C}), \cdot)$?

$GL_n(\mathbb{C})$ - stabel subset $\rightarrow \forall A, B \in GL_n$, $A \cdot B \in GL_n$

$A \in GL_n \rightarrow \det(A) \neq 0$

$B \in GL_n \rightarrow \det(B) \neq 0$ $\Big\} \rightarrow \det(A) \det(B) = \det(A \cdot B) \neq 0 \rightarrow$

$\rightarrow A \cdot B \in GL_n(\mathbb{C})$, $\forall A, B \in GL_n \rightarrow GL_n(\mathbb{C})$ - stabel subset

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

(i) - stabel subset

* asociativity: $\forall A, B, C \in GL_n(\mathbb{C})$, $A \cdot (B \cdot C) = (A \cdot B) \cdot C$

The multiplication of matrix is asociative (V)

* identity element: $\exists I_n \in GL_n(\mathbb{C})$, $\forall A \in GL_n(\mathbb{C})$, $I_n \cdot A = A \cdot I_n = A$

$\det I_n = 1 \neq 0 \rightarrow I_n \in GL_n(\mathbb{C})$, $I_n = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \\ 0 & 0 & \dots & 1 \end{pmatrix}$ ②

* inverse element: $\forall A \in GL_n(\mathbb{C})$, $\exists A' \in GL_n(\mathbb{C})$ s.t. $A \cdot A' = A' \cdot A - I_n$

$A \in GL_n(\mathbb{C}) \rightarrow \det A \neq 0 \rightarrow \exists A' \in GL_n(\mathbb{C})$ s.t. $A \cdot A' = A' \cdot A = I_n$ ③

From ①, ② & ③ $\rightarrow$ $(GL_n(\mathbb{C}), \cdot)$ - group

(ii) $SL_n(\mathbb{C}) = \{A \in M_n(\mathbb{C}) \mid \det(A) = 1\}$ - subgroup of $(GL_n(\mathbb{C}), \cdot)$?

$SL_n(\mathbb{C})$ - subgrop if

1. $SL_n(\mathbb{C}) \neq \emptyset$ $(I_n \in SL_n(\mathbb{C}))$
2. $\forall A, B \in SL_n(\mathbb{C})$, $A \cdot B^{-1} \in SL_n(\mathbb{C})$

* $\det(I_n) = 1 \rightarrow I_n \in SL_n(\mathbb{C})$

* $A, B \in SL_n(\mathbb{C}) \rightarrow \det(A) = 1$, $\det(B) = 1 \rightarrow \det(B^{-1}) = \frac{1}{\det(B)} = \frac{1}{1} = 1$

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

$\rightarrow SL_n(\mathbb{C})$ - subgroup of $(GL_n(\mathbb{C}), \cdot)$

6. (i) $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ - subring in $(\mathbb{C}, +, \cdot)$?

$\mathbb{Z}[i]$ - subring in $(\mathbb{C}, +, \cdot) \leftrightarrow$

$\mathbb{Z}[i] \neq \emptyset$ $(0 \in \mathbb{Z}[i])$

$\forall x, y \in \mathbb{Z}[i]$, $x + y \in \mathbb{Z}[i]$

$\forall x, y \in \mathbb{Z}[i]$, $x \cdot y \in \mathbb{Z}[i]$

* $0 = 0 + i \cdot 0$, $0 \in \mathbb{Z} \rightarrow 0 \in \mathbb{Z}[i] \Rightarrow \mathbb{Z}[i] \neq \emptyset$ ①

* Let $x, y \in \mathbb{Z}[i] \rightarrow x = a + bi$; $y = c + di$

$x - y = (a + bi) - (c + di) = a - c + i(b - d) \in \mathbb{Z}[i]$ ②

$a, b, c, d \in \mathbb{Z} \rightarrow a - c \in \mathbb{Z}$, $b - d \in \mathbb{Z}$

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

$x \cdot y = (a + bi)(c + di) = ac + adi + bci - bd$

$= (ac - bd) + i(ad + bc) \in \mathbb{Z}[i]$ ③

$a, b, c, d \in \mathbb{Z} \rightarrow ac - bd \in \mathbb{Z}$

$ad + bc \in \mathbb{Z}$

From ①, ②, ③ $\rightarrow$ $\mathbb{Z}[i]$ - subring

(a) $M = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a,b,c \in \mathbb{R} \right\}$ - subring in $(M_2(\mathbb{R}), +, \cdot)$

M - subring in $(M_2(\mathbb{R}), +, \cdot) \hookrightarrow \begin{cases} M \neq \emptyset \quad (O_2 \in M) \\ \forall A, B \in M,\ A + B \in M \\ \forall A, B \in M,\ A \cdot B \in M \end{cases}$

* $O_2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ the identity elem of $(M_2(\mathbb{R}), +)$

$O_2 = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$, $a = b = c = 0 \in \mathbb{R} \rightarrow O_2 \in M \rightarrow M \neq \emptyset$

* Let $A, B \in M$, $A = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$, $B = \begin{pmatrix} x & y \\ 0 & z \end{pmatrix}$

$A + B = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} + \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} = \begin{pmatrix} a+x & b+y \\ 0 & c+z \end{pmatrix} \in M$

$a, b, c, x, y, z \in \mathbb{R} \rightarrow a+x,\ b+y,\ c+z \in \mathbb{R}$

* Let $A, B \in M$

$A \cdot B = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} = \begin{pmatrix} ax+0b & ay+bz \\ 0c+0x & 0y+cz \end{pmatrix} = \begin{pmatrix} ax & ay+bz \\ 0 & cz \end{pmatrix} \in M$

$\rightarrow$ M - subring in $(M_2(\mathbb{R}), +, \cdot)$

7. (c) $f: \mathbb{C}^* \rightarrow \mathbb{R}^*$, $f(z) = |z|$

f - homomorphism between $(\mathbb{C}^*, \cdot)$ & $(\mathbb{R}^*, \cdot)$

f - homomorphism $\hookrightarrow \forall z_1, z_2 \in \mathbb{C}^*$, $f(z_1 \cdot z_2) = f(z_1) \cdot f(z_2)$

$f(z_1 \cdot z_2) = |z_1 \cdot z_2| = |z_1| \cdot |z_2| = f(z_1) \cdot f(z_2)$ „T"

(u) $g: \mathbb{C}^* \rightarrow GL_2(\mathbb{R})$, $g(a+bi) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$

g - homomorphism between $(\mathbb{C}^*, \cdot)$ & $(GL_2(\mathbb{R}), \cdot)$?

g - homomorphism $\hookrightarrow \forall a+bi, c+di \in \mathbb{C}^*$, $g((a+bi)(c+di)) =$

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

$(a+bi)(c+di) = ac + adi + bci - bd$

$= ac - bd + i(ad+bc)$

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

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

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

8. $n \in \mathbb{N}$, $n \geq 2$

$(\mathbb{Z}_n, +)$ & $(U_n, \cdot)$ - izomorfic ?

$\exists f: \mathbb{Z}_n \to U_n$ s.t. $\forall \hat{x}, \hat{y} \in \mathbb{Z}_n$, $f(x_n + y_n) = f(x) \cdot f(y)$ and f - bijective

$U_n = \{ z_k \mid k = \overline{0, n-1} \}$

$z_k = \cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n}$

$z = r(\cos \alpha + i \sin \alpha) \to z^n = r^n (\cos \alpha n + i \sin \alpha n)$

$z^n = \alpha \to$

$\to z_k = \sqrt[n]{r} \left(\cos \frac{\alpha + 2k\pi}{n} + i \sin \frac{\alpha + 2k\pi}{n} \right)$

$z^n = 1 \to 1 = \cos 0 - i \sin 0 \to z_k = \cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n}$

$f: \mathbb{Z}_n \to U_n$, $f(\hat{k}) = z_1^k$

* homomorphism $\forall \hat{k_1}, \hat{k_2} \in \mathbb{Z}_n$, $f(\hat{k_1} + \hat{k_2}) = f(\hat{k_1}) \cdot f(\hat{k_2})$

$f(\hat{k_1} + \hat{k_2}) = z_1^{\hat{k_1} + \hat{k_2}} = z_1^{\hat{k_1}} \cdot z_1^{\hat{k_2}} = f(\hat{k_1}) \cdot f(\hat{k_2})$

* bijectivity

(the exponential function is bijective?) f injective

9. $n \in \mathbb{N}$, $n \geq 2$, $(\mathbb{Z}_n, +, \cdot)$ - ring, $\hat{a} \in \mathbb{Z}_n^*$

(i) $\hat{a}$ - invertable $\hookrightarrow (a, n) = 1$ (a si n sunt prime intre ele)

$(n, m) = 1 \hookrightarrow \exists a, b \in \mathbb{Z}$ s.t. $a \cdot n + b \cdot m = 1$

$\hat{a}$ - inv. $\hookrightarrow \exists \hat{b} \in \mathbb{Z}_n$ s.t. $\hat{a} \cdot \hat{b} = 1 \to \widehat{a \cdot b} = 1 \hookrightarrow$

$\hookrightarrow a \cdot b \equiv 1 \pmod n \to n \mid (ab - 1) \hookrightarrow \exists k \in \mathbb{Z}$ s.t. $(ab - 1) = nk \hookrightarrow$

$\hookrightarrow \exists b, k \in \mathbb{Z}$ s.t. $ab - nk = 1 \hookrightarrow ab + (-k)n = 1 \hookrightarrow (a, n) = 1$

(ii) $(\mathbb{Z}_n, +, \cdot)$ - field $\hookrightarrow n$ - prime

$(\mathbb{Z}_n, +, \cdot)$ - field $\hookrightarrow (\mathbb{Z}_n^*, \cdot)$ - group $\hookrightarrow$

$\hookrightarrow$ every elem. is invertable $\overset{(i)}{\hookrightarrow} \forall \hat{a} \in \mathbb{Z}_n : (a, n) = 1 \to$

$\to (1, n) \neq (2, n) = \dots = (n-1, n) = 1 \to n$ - prime

Hw: 10 $M = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbb{R} \right\} \subseteq M_2(\mathbb{R})$

$(M, +, \cdot)$ - isomorphic to $(\mathbb{C}, +, \cdot)$

Let $f: M \to \mathbb{C}$, $f(A) = a + bi$, $A \in M$

* homomorphism

(i) $\forall A, B \in M$, $f(A+B) = f(A) + f(B)$

$A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, $B = \begin{pmatrix} c & d \\ -d & c \end{pmatrix}$

$A + B = \begin{pmatrix} a+c & b+d \\ -(b+d) & a+c \end{pmatrix}$

$f(A+B) = a + c + i(b+d) = a + bi + c + di = f(A) + f(B)$

(ii) $\forall A, B \in M$, $f(A \cdot B) = f(A) \cdot f(B)$

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

$f(A \cdot B) = (ac - bd) + i(bc + ad) =$

$= ac - bd + i \cdot bc + i \cdot ad$

$= a(c + id) + bi(c + id)$

$= (a + bi)(c + id) = f(A) \cdot f(B)$

* bijectivity (?)