Curs 1

Partial exams : Nov 26 (week 8)
↳ max grade: 4

Jan 21 (week 14)
↳ max grade : 5

Seminar 1

1.1 Which ones of the following symbols define an operation on $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$?

	$+$	$-$	$\cdot$	$\setminus$
$\mathbb{N}$	Yes	No	Yes	No
$\mathbb{Z}$	Yes	Yes	Yes	No
$\mathbb{Q}$	Yes	Yes	Yes	No
$\mathbb{R}$	Yes	Yes	Yes	No
$\mathbb{C}$	Yes	Yes	Yes	No

Def: G-set
operation on G $\Big\}$ $(G, \cdot)$ group

1. $\cdot$ is well defined (a stable part)
↳ $\forall\, x, y \in G$ a.î. $x \cdot y \in G$

2. $\cdot$ is associative

$(\forall)\ x, y, z \in G$ a.î. $(x \cdot y) \cdot z = x \cdot (y \cdot z)$

semigroup

3. neutral element

$\exists\ e \in G$ a.î. $x \cdot e = e \cdot x = x, \forall\ x \in G$

monoid

4. inversibility

$(\forall)\ x \in G, \exists\ x' \in G$ a.î. $x \cdot x' = x' \cdot x = e$

$\Rightarrow$ group

+5. commutativity

$(\forall)\ x, y \in G$ a.î. $xy = yx$

} abelian group

Ex: $(\mathbb{R}, \cdot), (\mathbb{Z}, +), (\mathbb{C}^*, \cdot), (S_n, \circ), (\mathbb{Z}_p^*, \cdot)$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

ex 4) $x * y = xy + x + y$

Prove that $(\mathbb{R}, *)$ is a commutative monoid and $[-1, +\infty)$ is a stable subset of $\mathbb{R}$

a) $(\mathbb{R}, *)$ commutative monoid $\Leftrightarrow$
- „$*$" - well defined (trivial)
- „$*$" - associative
- „$*$" has neutral elem
- „$*$" commutative

· „$*$" - commutative $\Leftrightarrow (\forall)\ x, y \in \mathbb{R} \Rightarrow x * y \overset{?}{=} y * x$

$x * y = y * x \Rightarrow x + y + xy = y + x + yx \Rightarrow$ „$*$" - commutative (1)

· „$*$" - associative - .... (2)

"$*$" has neutral element $\Leftrightarrow \exists\, e \in \mathbb{R}$ s.t. $x * e \stackrel{?}{=} e * x \stackrel{?}{=} x$, $(\forall)\, x \in \mathbb{R}$

$x * e = x \Leftrightarrow x + e + xe = x \,|-x \Rightarrow e + xe = 0 \Rightarrow e(x+1) = 0 \Rightarrow$

$\Rightarrow e = 0 \in \mathbb{R}$

Therefore, "$*$" has neutral element $e=0$ (3)

(1), (2), (3) $\Rightarrow$ $(\mathbb{R}, *)$ - commutative monoid

b) $[-1, +\infty)$ is a stable subset of $\mathbb{R} \Leftrightarrow (\forall)\, x, y \in [-1, +\infty) \Rightarrow$

$\Rightarrow x * y \in [-1, +\infty)$

$x \in [-1, +\infty) \Rightarrow x \geq -1 \,/ +1 \Rightarrow x + 1 \geq 0$ (1)

$y \in [-1, +\infty) \Rightarrow y \geq -1 \,| +1 \Rightarrow y + 1 \geq 0$ (2)

(1)$\cdot$(2) $\Rightarrow (x+1)(y+1) \geq 0 \Leftrightarrow xy + x + y + 1 \geq 0 \,|-1 \Rightarrow x + y + xy \geq -1$

$\Rightarrow x * y \geq -1 \Rightarrow x * y \in [-1, +\infty)$. Therefore, conclusion

ex 5) $x * y = \gcd(x, y)$, "$*$" - operation on $\mathbb{N}$

b) $D_n = \{ x \in \mathbb{N} \mid x | n \}$ stable subset of $(\mathbb{N}, *)$

$x \in D_n \Leftrightarrow x | n$

$y \in D_n \Leftrightarrow y | n$

$x * y = \gcd(x, y) = d \Rightarrow d | x$
$d | y$

$$\left.\begin{array}{l} d | x \\ x | n \end{array}\right| \Rightarrow d | n \Leftrightarrow \gcd(x, y) | n \Leftrightarrow \gcd(x, y) \in D_n$$

Seminar 2

Relations

$\mathcal{R} = (\underset{\text{domain}}{A}, \underset{\text{codomain}}{B}, \underset{\text{graph } (\subseteq A \times B)}{R})$

Equivalence relation : $\mathcal{R} = (A, A, R)$, so that :

- reflexivity : $(\forall) x \in A$: $\underline{x \mathcal{R} x}$ (in other words $(x,x) \in R$)
- simetry : $(\forall) x, y \in A$, if $x \mathcal{R} y$, then $y \mathcal{R} x$
- transitivity : $(\forall) x, y, z \in A$, if $x \mathcal{R} y$ and $y \mathcal{R} z$, then $x \mathcal{R} z$

2.1. : $\mathcal{r}, \mathcal{s}, \mathcal{t}, \mathcal{v}$ - homogeneous relations on the set

$M = \{2, 3, 4, 5, 6\}$ defined by
$$\begin{cases} x \mathcal{r} y \Leftrightarrow x < y \\ x \mathcal{s} y \Leftrightarrow x \mid y \\ x \mathcal{t} y \Leftrightarrow \gcd(x,y) = 1 \\ x \mathcal{v} y \Leftrightarrow x \equiv y \pmod 3 \end{cases}$$

Write the graphs of R, S, T, V of these relation

$R = \{(2,3), (2,4), (2,5), (2,6), (3,4), (3,5), (3,6), (4,5), (4,6), (5,6)\}$

$S = \{(2,4), (2,6), (3,6), (2,2), (3,3), (4,4), (5,5), (6,6)\}$

$T = \{(2,3), (2,5), (3,4), (3,5), (4,5), (3,2), (5,2), (4,3), (5,3), (5,4), (5,6), (6,5)\}$

$V = \{(2,5), (5,2), (3,6), (6,3), (2,2), (3,3), (4,4), (5,5), (6,6)\}$

2.3.: Give examples of relations having each one of the properties of reflexivity, simetry, transitivity but not the others 2

- $M = \{$ vertices of a directed graph G, $x \, r \, y \Leftrightarrow \exists$ a path from x to y - transitive, NOT reflexiv + simetrical

- $M = \{1, 2, 3\}$

  $\hookrightarrow$ $R = \{(1,2), (2,1)\}$ - s, $\cancel{r}$, $\cancel{t}$

  $R = \{(1,1), (2,2), (3,3), (1,2), (2,3)\}$ - r, $\cancel{s}$, $\cancel{t}$

  $R = \{(1,2), (2,3), (1,3)\}$ - t, $\cancel{r}$, $\cancel{s}$

Equivalence relations & partitions

Let A - set.

- $E(A)$ = the set of equivalences on A (r, s, t)
- $P(A)$ = the set of partitions of A

$P \in P(A)$; $P = \{U_i \mid U_i \subseteq A, \ i \in I\}$

$A = \bigcup U_i$ (→ union), $(\forall)\, i \neq j : U_i \cap U_j = \emptyset$

$E(A) \xleftrightarrow{\ \exists\ } P(A)$ → partition (a set of boxes that rep a set of eq. rel)

$E(A)$ ↓ equivalence relations; $\exists$ ↓ bijective; associate

$r \longmapsto A/r$

r ↓ relation; A/r quotient set

$r_P \longmapsto P$ → partition

r_P ↓ equiv. relation

$A/r = \{ r\langle x \rangle \mid x \in A \}$

$r\langle x \rangle = \{ y \in A \mid y \, r \, x \}$

(x,y)

$x\, r_S\, y \iff \exists\, U \in \mathcal{P} : U \ni x, y$ 2 equivalent if they come from the same box

2.5. $M = \{1, 2, 3, 4\}$

r_1, r_2 - homogeneous relat. on M

$\pi_1, \pi_2 \subseteq \mathcal{P}(M) \rightarrow$ sets of subsets of M

$R_1 = \Delta_M \cup \{(1,2), (2,1), (1,3), (3,1), (2,3), (3,2)\}$

$\downarrow$

pair of identical elements $(1,1), (2,2) \ldots$

$R_2 = \Delta_M \cup \{(1,2), (1,3)\}$

$\pi_1 = \{\{1\}, \{2\}, \{3\}\}$

$\pi_2 = \{\{1\}, \{1,2\}, \{3,4\}\}$

(i) are r_1, r_2 equivalent on M? If so, write their equiv. set

(ii) are π_1, π_2 partitions of M? If so, write the graphs of their associated relations

i) r_1 is an equiv. on M
$\downarrow$
t, r, s

r_2 is r and t, but is not s because $(1,2) \in R_2$ but $(2,1) \notin R_2$

?? $M / r_1 = \{\{1, 2, 3\}, \{4\}\} \rightarrow$ the quotient set

ii) π_1 is a partition because the elem are disjointed and every elem of M can be found in an elem of π_1 r.

π_2 is not partition because $\{1\} \cap \{1,2\} \neq \emptyset$

$R_{\pi_1}2 = \Delta_M \cup \{(3,4), (4,3)\}$

ex: $M = \{1, 2, 3, 4, 5, 6, 7\}$

$\mathcal{P} = \{\{1\}, \{2,3\}, \{4\}, \{5,6,7\}\}$

$R_{\mathcal{P}} = \{(1,1), (2,2), (3,3), (2,3), (3,2), (4,4), (5,5), (5,6), (6,5),$
$(6,6), (6,7), (7,7)\}$

Seminar 3

Def: $(\underset{\text{set}}{G}, \underset{\text{operation}}{*})$ is a group if:

semigroup $\begin{cases} - * \text{ is well defined}: (\forall)\, x,y \in G : x*y \in G \\ - * \text{ associative}: (\forall)\, x,y,z \in G : (x*y)*z = x*(y*z) \end{cases}$

- $*$ has neutral element: $\exists\, e \in G : x*e = e*x = x, (\forall)\, x \in G$

- every elem of G is invertible $(\forall)\, x \in G, \exists\, x' \in G : x*x' = x'*x = e$

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

Prove that $(S_M, \circ)$ is a group

- „$\circ$" is well define : $(\forall)\, f,g \in S_M : f\circ g \overset{?}{\in} S_M$

$(f\circ g) : M \to M$
f,g - bijective $\Rightarrow f \circ g$ is bijective

$\Rightarrow$ "$\circ$" is well defined

- „$\circ$" is associative : $(\forall) f,g,h \in S_M : (f\circ g)\circ h = f\circ(g\circ h), (\forall)\, x \in M$

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

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

$\Rightarrow (f\circ g)\circ h = f\circ(g\circ h), (\forall)\, f,g,h \in S_M \Rightarrow$ „$\circ$" is associative

- „$\circ$" has neutral elem

id_M (identity function) $: M \to M$ – the neutral eleme

$id_M(x) = x$

$(\forall) f \in S_M : (f \circ id_M)_{(x)} = (id_M \circ f)_{(x)} = f(x)$; $(\forall) x \in M$ – proove this:

$(f \circ id_M)(x) = f(id_M(x)) = f(x)$
$(id_M \circ f)(x) = id_M(f(x)) = f(x)$ $\Big/ \Rightarrow$ „$\circ$" has neutral eleme

– every eleme of S_M is invertible

f-bijective $\Rightarrow f$ invertible $\Rightarrow \exists f^{-1}$ s.t. $f \circ f^{-1} = f^{-1} \circ f = id_M$

$\Rightarrow S_M$ – group

Def / theorem: $(G, \cdot)$ is a group, $H \subseteq G$. Then G is a subgroup of G ($H \leq G$) if (i) $H \neq \emptyset$

(ii) $(\forall) x, y \in H : x \cdot y^{-1} \in H$
or
$(\forall) x, y \in H : \begin{cases} x \cdot y \in H \\ x^{-1} \in G \end{cases}$ $\Big\}$ the same

3.5 (i) $GL_n(\mathbb{C}) = \{ A \in \mathcal{M}_n(\mathbb{C}) \mid \det A \neq 0)$ – stable subset of the monoid $(\mathcal{M}_n(\mathbb{C}), \cdot)$

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

(iii) $SL_n(\mathbb{C}) = \; A \in \mathcal{M}_n(\mathbb{C}) / \det A = 1 \}$ – subgroup of the group $(GL_n(\mathbb{C}), \cdot)$

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

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

$A, B \in GL_n(\mathbb{C}) \Rightarrow \det A, \det B \neq 0 \Rightarrow \det(A \cdot B) \neq 0 \Rightarrow GL_n(\mathbb{C})$ is a stable part of $\mathcal{M}_n(\mathbb{C})$

(ii) – „$\cdot$" – well defined (at (i))

- "·" - associative: $\forall A_1, A_2, A_3 \in \mathcal{M}_n(\mathbb{C})$,

$(A_1 \cdot A_2) \cdot A_3 = A_1 \cdot (A_2 \cdot A_3)$ - the multiplication of matrices is always associative

- "·" has neutral element: $\exists\, i_n \in GL_n(\mathbb{C})$, $(\forall)\, A \in GL_n(\mathbb{C})$

$A \cdot i_n = i_n \cdot A = A$

- every elem of GL_n is invertible: $(\forall)\, A \in GL_n(\mathbb{C})$,

$\exists\, A' \in GL_n(\mathbb{C})$ s.t. $A' = \dfrac{1}{\underbrace{\det A}_{\neq 0}} \cdot A^*$

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

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

(1) $i_n \in SL_n(\mathbb{C})$

(2) $(\forall)\, A, B \in SL_n(\mathbb{C}): A \cdot B \in \mathcal{M}_n(\mathbb{C})$ (1)

$\det(A \cdot B) = \det A \cdot \det B = 1$ (2)

$\xrightarrow[(2)]{(1)} A \cdot B \in SL_n(\mathbb{C})$, $(\forall)\, A, B \in SL_n(\mathbb{C})$

(3) $(\forall)\, A \in SL_n(\mathbb{C})$, $\exists\, A^{-1}$ $(\det A \neq 0)$ s.t. $A \cdot A^{-1} = A^{-1} \cdot A = i_n$

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

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

Rings

Def: $(A, +, \cdot)$ is a ring if:

- $(A, +)$ - abelian group
- $(A, \cdot)$ - semigroup
- distributivity: $(\forall)\, x, y, z \in A$: $x \cdot (y + z) = xy + x \cdot z$

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

- $\rightarrow$ if $(A,\cdot)$ is a monoid, we have a ring with unity (unital ring)
- $\rightarrow$ if $\cdot$ is commutative $\Rightarrow$ commutative ring

Def/Th: If $(A,+,\cdot)$ is a ring, $B \subseteq A$. then B is a subring $(B \leq A)$ of A is:

(i) $B \neq 0$

(ii) $\underbrace{(B,+) \leq (A,+)}_{\text{subgroup}} \Leftrightarrow (\forall)\ x,y \in B:\ x-y \in B$

(iii) $\underbrace{(B,\cdot) \leq (A,\cdot)}_{\text{sub semi group}} \Leftrightarrow (\forall)\ x,y \in B:\ xy \in B$

3.6 Show that the following sets are subrings of the respective ring:

1) $\mathbb{Z}(i) = \{a+bi \in \mathbb{C} \mid a,b \in \mathbb{Z}\}$ in $(\mathbb{C},+,\cdot)$

2) $\mathcal{U} = \left\{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a,b,c \in \mathbb{R}\right\}$ in $(\mathcal{M}_2(\mathbb{R}),+,\cdot)$

1) (i) $1 \in \mathbb{Z}(i) \Rightarrow \mathbb{Z}(i) \neq \emptyset$

(ii) $(\forall)\ z_1, z_2 \in \mathbb{Z}(i) \Rightarrow z_1 - z_2 \in \mathbb{Z}(i)$

$z_1 = a+bi$

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

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

(iii) $(\forall)\ z_1, z_2 \in \mathbb{Z}(i) \Rightarrow z_1 \cdot z_2 \overset{?}{\in} \mathbb{Z}(i)$

$z_1 \cdot z_2 = (a+bi)(c+di) = ac-bd + i(ad+bc) \in \mathbb{Z}(i)$

$I_2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in M \Rightarrow M \neq \emptyset$

(ii) $(\forall)\ A, B \in M,\ A - B \overset{?}{\in} M$

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

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

(iii) $(\forall)\ A, B \in M,\ A \cdot B \overset{?}{\in} M$

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

$\Rightarrow A \cdot B \in M$

Def: $(G_1, *)$ and $(G_2, \#)$ groups.

$f: G_1 \to G_2$ is a group (homo)morphism if $(\forall)\ x, y \in G_1$:

$f(x * y) = f(x) \# f(y)$

Def: $(A_1, \boxplus, \boxdot)$, $(A_2, \oplus, \odot)$ rings. $f: A_1 \to A_2$ is ring homo-morphism if $(\forall)\ x, y \in A$: $f(x \boxplus y) = f(x) \oplus f(y)$

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

$\to$ unital: $f(1_{A_1}) = 1_{A_2}$

3.7 $f: \mathbb{C}^* \to \mathbb{R}^*,\ f(z) = |z|$.

(i) f - group homomorphism

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

g group homomorphism

$z_1, z_2 \in \mathbb{C}^*$: $f(z_1 \cdot z_2) = f(z_1) \cdot f(z_2)$

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

Let $z_1 = a + bi$

$z_2 = c + di$, $a, b, c, d \in \mathbb{R}$

$$z_1 \cdot z_2 = (ac - bd) + i(ad + bc)$$

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

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

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