Seminar 3
24.11.2022 00:24

R1 $(R, \cdot)$
(i) semigroup: if associative
(ii) monoid: if identity element exists
(iii) group: if inverse exists
(iv) abelian: commutative
$GL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid \det(A) \neq 0\}$ → general linear group of rank n
Klein's group $K = \{e, a, b, c\}$

·	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

R2 R-set
$(R, +, \cdot)$
1) ring, if $(R, +)$ abelian group
$(R, \cdot)$ semigroup
the distributive law holds: $x \cdot (y+z) = xy + xz$, $\forall x, y, z \in R$
$(y+z) \cdot x = yx + zx$, $\forall x, y, z \in R$
2) unitary ring: if ring and $\exists\, e$ with respects to $\cdot$
3) division ring (skew field): if $(R, \cdot)$ abelian group, $(R^*, \cdot)$ is a group and the distributive law holds
4) field: is a commutative division ring
$(R, +, \cdot)$ commutative if $\cdot$ is commutative
5) $\{e\}$
$e + e = e$
$e \cdot e = e$
$(\{e\}, +, \cdot)$ commutative ring, called the trivial ring

R3 $(G, \cdot)$ group
$H \subset G$
H-subgroup $\Rightarrow \forall x, y \in H,\ x \cdot y^{-1} \in H$
$H \leq G$ $\quad H \neq \emptyset$
$(R, +, \cdot)$ ring
$A \subseteq R$
$A \leq R$ (subring) $\Leftrightarrow$ $\begin{cases} A \neq \emptyset \\ \forall x, y \in A,\ x - y \in A \\ \forall x \in R, \forall a \in A,\ x \cdot a \in A \end{cases}$
$(k, +, \cdot)$ field
$A \subseteq k$
$A \subseteq k$ (subfield) $\Leftrightarrow$ $\begin{cases} |A| \geq 2 \ (0, 1 \in A) \\ \forall x, y \in A,\ x - y \in A \\ \forall x, y \in A,\ y \neq 0,\ x \cdot y^{-1} \in A \end{cases}$
$(G, \cdot)$ and $(G', \cdot)$
$f: G \to G'$
f group homomorphism $\Leftrightarrow f(x \cdot y) = f(x) \cdot f(y)$, $\forall x, y \in G$
$G \simeq G'$ isomorphic
$(R, +, \cdot)$ and $(R', +, \cdot)$ rings
$f: R \to R'$
f ring homomorphism if $\forall x, y \in R$ $\Leftrightarrow$ $\begin{cases} f(x+y) = f(x) + f(y), \\ f(xy) = f(x) \cdot f(y) \end{cases} \forall x, y \in R$
$R \simeq R'$

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.

$\forall f_1, f_2, f_3 \in S_n \Rightarrow (f_1 \circ f_2) \circ f_3 = f_1 \circ (f_2 \circ f_3)$
$((f_1 \circ f_2) \circ f_3)(x) = (f_1 \circ f_2)(f_3(x)) = f_1(f_2(f_3(x)))$
$(f_1 \circ (f_2 \circ f_3))(x) = (f_1 \circ f_2)(f_3(x)) = f_1(f_2(f_3(x)))$ $\Big\} \Rightarrow ((f_1 \circ f_2) \circ f_3 = f_1 \circ (f_2 \circ f_3)) \Rightarrow (S_n, \circ)$ is associative
Identity law: $\exists\, e \in S_n$, $(f \circ e)(x) = (e \circ f)(x) = f(x)$
$(f \circ \varphi)(x) = f(e(x)) = f(x) \Rightarrow e(x) = x$
$\varphi \in S_n$, f is bijective
Inverse
$\forall f \in S_n$, $\exists f^{-1} \in S_n$ such that $(f \circ f^{-1})(x) = f(f^{-1}(x)) = x$
f is bijective $\Rightarrow \exists\, f^{-1} \in S_n$, that is also bijective $\Rightarrow \forall f \in S_n, \exists f^{-1} \in S_n$
$\Rightarrow (S_n, \circ)$ is a group.

2. Let M be a non-empty set and let $(R, +, \cdot)$ be a ring. Define on $R^M = \{f \mid f : M \to R\}$ two operations by: $\forall f, g \in R^M$,

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

Show that $(R^M, +, \cdot)$ is a ring. If R is commutative or has identity, does R^M have the same property?

$(R^M, +)$ ring $\Rightarrow$ $(R^M, +)$ abelian group
$(R, \cdot)$ semigroup
distributivity holds: $\forall f, g, h \in R^X$, $((f+g) \cdot h)(x) = (f \cdot g)(x) + (f \cdot h)(x) = f(x)\, g(x) + f(x) \cdot h(x)$ (?)
If R is commutative, R^M is commutative
If R has an identity element, R^M also has an identity element, but it is different from the one of R

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

$(H, \cdot)$ subgroup $\Rightarrow$ $\begin{cases} H \neq \emptyset \\ \forall x, y \in H,\ x \cdot y^{-1} \in H \end{cases}$
$z = 1 \Rightarrow |z| = 1 \Rightarrow H \neq \emptyset$
$z_1 = a_1 + ib_1$
$z_2 = a_2 + ib_2$
$z_2^{-1} = \frac{1}{a_2 + ib_2} = \frac{1}{z_2}$
$|z_2^{-1}| = \frac{1}{|z_2|} = 1$
$z_1 \cdot z_2^{-1} = \frac{z_1}{z_2}$
$\frac{z_1}{z_2} \in H \ \forall\ |\frac{z_1}{z_2}| = 1$
$|\frac{z_1}{z_2}| = \frac{|z_1|}{|z_2|} = 1 \in H \Rightarrow H$ is a subgroup

$1 \in H$
$i \in H$
$1 - i \notin H$

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

i) $\mathbb{Z}[i] \leq \mathbb{C}$ $\Leftrightarrow$ $\begin{cases} \mathbb{Z}[i] \neq \emptyset \\ \forall x, y \in \mathbb{Z}[i],\ x - y \in \mathbb{Z}[i] \\ \forall\ x, y \in \mathbb{Z}[i],\ x \cdot y \in \mathbb{Z}[i] \end{cases}$
$x \cdot y = (a_1 + b_1 i)(a_2 + b_2 i) = \underbrace{a_1 a_2 - b_1 b_2}_{\in \mathbb{Z}} + \underbrace{a_1 b_2 + a_2 b_1}_{\in \mathbb{Z}} i$
ii) $M \leq M_2(\mathbb{R})$ $\Leftrightarrow$ $\begin{cases} M \neq \emptyset \\ \forall A_1, A_2 \in M,\ A_1 - A_2 \in M \\ \forall B_1, A_2 \in M,\ B_1 \cdot A_2 \in M \end{cases}$
$A_1 = \begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix}$
$A_2 = \begin{pmatrix} a_2 & b_2 \\ 0 & c_2 \end{pmatrix}$
$A_1 \cdot A_2 = \begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ 0 & c_2 \end{pmatrix} = \begin{pmatrix} a_1 a_2 & a_1 b_2 + b_1 c_2 \\ 0 & c_1 c_2 \end{pmatrix} \in M$

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 $g(a + bi) = \begin{pmatrix} a & b \\ -b & b \end{pmatrix}$. Show that g is a group homomorphism between $(\mathbb{C}^*, \cdot)$ and $(GL_2(\mathbb{R}), \cdot)$.

i) $f(z) = |z|$
$\mathbb{C}^* \simeq \mathbb{R}^+$ $\Leftrightarrow$ $f : \mathbb{C}^* \to \mathbb{R}^+$, $f(z_1 \cdot z_2) = f(z_1) \cdot f(z_2)$
$f(z_1) = |z_1|$
$f(z_2) = |z_2|$
$f(z_1 z_2) = |z_1 \cdot z_2| = |z_1| \cdot |z_2|$
ii) same.

8. Let $n \in \mathbb{N}$, $n \geq 2$. Prove that the groups $(\mathbb{Z}_n, +)$ of residue classes modulo n and $(U_n, \cdot)$ of n-th roots of unity are isomorphic.

$f : U_n \to \mathbb{Z}_n$, $f(\varepsilon^k) = k$, $\forall k \in \mathbb{Z}$
$f(\varepsilon^{k_1} \cdot \varepsilon^{k_2}) = f(\varepsilon^{k_1}) + f(\varepsilon^{k_2})$
$k = n,\ n \in \mathbb{Z}$
$f(\varepsilon^n) = f(1) = 0$

9. Let $n \in \mathbb{N}$, $n \geq 2$. Consider the ring $(\mathbb{Z}_n, +, \cdot)$ and let $\hat{a} \in \mathbb{Z}_n$.
(i) Prove that $\hat{a}$ is invertible $\Leftrightarrow (a, n) = 1$.
(ii) Deduce that $(\mathbb{Z}_n, +, \cdot)$ is a field $\Leftrightarrow n$ is prime.

i) $\hat{a}$ invertible $\Leftrightarrow \exists\, \hat{b} \in \mathbb{Z}_n^*$ $\exists \hat{a}^{-1} = \hat{b} \in \mathbb{Z}_n$ s.t. $\hat{a}\hat{b} = \hat{1} \Leftrightarrow n \mid ab - 1 \Leftrightarrow \exists k \in \mathbb{Z}$, $nk = ab - 1 \Rightarrow ab + nk(-k) = 1 \Rightarrow (a, n) = 1$
ii) $(\mathbb{Z}_n, +, \cdot)$ field $\Leftrightarrow \forall\, \hat{a} \in \mathbb{Z}_n$ is invertible $\Leftrightarrow \forall\, \hat{1}, \hat{2}, \ldots, \hat{n-1}$ are invertible $\Leftrightarrow$ $\begin{cases} (1, n) = 1 \\ \vdots \\ (n-1, n) = 1 \end{cases}$ $\Leftrightarrow n$ is prime

10. Let $\mathcal{M} = \left\{\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \middle| a, b \in \mathbb{R}\right\} \subseteq M_2(\mathbb{R})$. Show that $(\mathcal{M}, +, \cdot)$ is a field isomorphic to $(\mathbb{C}, +, \cdot)$.

$f : \mathbb{C} \to \mathcal{M}$, $f(a + ib) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$
Vrem un abelian group.
$(\mathcal{M}^*, \cdot)$ is a group.
For f to be isomorphism, f must be a bijective homomorphism.
$\forall\, a + bi,\ c + di \in \mathbb{C}$, $f((a+ib) + (c+id)) = f((a+c) + i(b+d)) = \begin{pmatrix} a+c & b+d \\ -b-d & a+c \end{pmatrix} = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = f(a+bi) + f(c+di)$
$\forall\, a + bi,\ c + di \in \mathbb{C}$, $f((a+ib)(c+id)) = f((ac - bd) + i(ad + bc)) = \begin{pmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{pmatrix}$
$f(a+bi) \cdot f(c+di) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} ac-bd & ad+bc \\ -bc-ad & ac-bd \end{pmatrix}$
$\Big\} \Rightarrow f((a+bi)(c+di)) = f(a+bi) \cdot f(c+di)$ $\Big\} \Rightarrow f$ is a homomorphism.
f is bijective, $\exists \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ s.t. $f(a+ib) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \Rightarrow f$ is a fielded isomorphism