17.10.2023

$(G, \cdot)$ group

- "$\cdot$" operation, associative
- "$\cdot$" has a neutral elem.
- $\forall$ elem. in G is invertible with respect to "$\cdot$"

+ "$\cdot$" commutative.

$H \subseteq G$, H subgroup of G if $(H, \cdot)$ is a group

Characterization theorem for subgroups

$(G, \cdot)$ group, $H \subseteq G$

$H \leq G \iff$ i) $H \neq \emptyset$ ← most of times we check if $1 \in H$

subgroup

ii) $\forall x, y \in H, x \cdot y \in H$

iii) $\forall x \in H, x^{-1} \in H$

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

3) Let $U_n = \{ z \in \mathbb{C} \mid z^n = 1 \}$

prove that U_n is a subgroup of $(\mathbb{C}^*, \cdot)$

and U_n is not a subgroup of $(\mathbb{C}, +)$

- $1 \in U_n \Rightarrow U_n \neq \emptyset$
- $\forall z_1, z_2 \in U_n \Rightarrow \begin{cases} z_1^n = 1 \\ z_2^n = 1 \end{cases} \Rightarrow (z_1 \cdot z_2)^n = 1 \Rightarrow$

$\Rightarrow (z_1 \cdot z_2) \in U_n, \; z_1, z_2 \in U_n$

- $\forall z_n \in U_n, \; z^{-1} \stackrel{?}{\in} U_n$

1 is the neutral elem.

$z \cdot z^{-1} = 1 \Rightarrow z^{-1} = \frac{1}{z} \Rightarrow (z^{-1})^n = \left(\frac{1}{z}\right)^n = 1 \Rightarrow$

$\Rightarrow z^{-1} \in U_n$

Therefore, $U_n \leq \mathbb{C}^*$

U_n is not a subgroup of $(\mathbb{C}, +)$ because $0 \notin U_n$

5) $n \in \mathbb{N}$, $n \geq 2$

prove that

i) $GL_n = \{A \in M_n(\mathbb{C}) \mid \det A \neq 0\}$ is a stable subset of $(M_n(\mathbb{C}), \cdot)$

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

iii) $SL_n(\mathbb{C}) = \{A \in M_n(\mathbb{C}) \mid \det A = 1\}$ is a subgroup of $(GL_n(\mathbb{C}), \cdot)$

---

i) and ii) $I_n \in GL_n(\mathbb{C})$ $(\det I_n = 1 \neq 0)$

$\forall A \in GL_n(\mathbb{C})$, $\det A \neq 0 \Rightarrow \exists A^{-1}$ for which $\det A = \det A^{-1} \neq 0 \Rightarrow A^{-1} \in GL_n(\mathbb{C})$

assoc. is inherited from $M_n(\mathbb{C})$

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

$\Rightarrow (A \cdot B) \in GL_n(\mathbb{C})$

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

$\Rightarrow SL_n(\mathbb{C}) \neq \emptyset$ (1)

$\forall A \in SL_n(\mathbb{C})$, $\det A = 1 \neq 0 \Rightarrow \exists A^{-1}$ and

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

$\forall A \in SL_n(\mathbb{C})$ (2)

$\forall A, B \in SL_n(\mathbb{C})$, $\det(A \cdot B) = \det A \cdot \det B =$

$= 1 \cdot 1 = 1 \Rightarrow (A \cdot B) \in SL_n(\mathbb{C})$, $\forall A, B \in SL_n(\mathbb{C})$ (3)

(1), (2), (3) $\Longrightarrow (SL_n, \cdot) \leq (GL_n(\mathbb{C}), \cdot)$

$(R, +, \cdot)$ is a ring

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

$S \subseteq R$

S is a subring of R if $(S, +, \cdot)$ ring

Caracterisation theorem I

$(R, +, \cdot)$ ring, $S \subseteq R$

$S \leq R \iff$ i) $S \neq \emptyset$ (subring $\leq$)

ii) $(S, +) \leq (R, +)$ (subgroup)

iii) $(S, \cdot) \leq (R, \cdot)$ (subsemigroup (depending on context, we have the same notation))

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

$\forall x \in S, x^{-1} \in S$

$\iff \forall x, y \in S, (x - y) \in S$

iii) $\forall x, y \in S, (x \cdot y) \in S$ (Stability only)

6) Show that the set $M = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a,b,c \in \mathbb{R} \right\}$ is a subring of $(M_2(\mathbb{R}), +, \cdot)$

Let $A = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in M \Rightarrow M \neq \emptyset$ (1)

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

$$A+B = \begin{pmatrix} a+d & b+e \\ 0+0 & c+f \end{pmatrix} = \begin{pmatrix} k & \ell \\ 0 & m \end{pmatrix} \in M \quad (2)$$

$a+d = k \in \mathbb{R}$
$b+e = \ell \in \mathbb{R}$
$c+f = m \in \mathbb{R}$

OBS: (2)+(3) $\Leftrightarrow$ prove that $\forall A, B \in M$, $A - B \in M$ (easier) !!!!

$\forall A \in M$, $A = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \Rightarrow -A = \begin{pmatrix} -a & -b \\ 0 & -c \end{pmatrix}$

$$A + (-A) = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} + \begin{pmatrix} -a & -b \\ 0 & -c \end{pmatrix} = O_2 \in M \quad (3)$$

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

$$= \begin{pmatrix} \underbrace{ad+b\cdot 0}_{\in \mathbb{R}} & \underbrace{ae+bf}_{\in \mathbb{R}} \\ \underbrace{0\cdot d + c\cdot 0}_{=0} & \underbrace{0\cdot e + cf}_{\in \mathbb{R}} \end{pmatrix} \in M \quad (4)$$

$(1),(2),(3),(4) \Rightarrow (M, +, \cdot) \leq (M_2(\mathbb{R}), +, \cdot)$

OBS: For fields and subfields, we need to also show that every element is invertible. (i.e. "operation)

$(G_1, \cdot)$, $(G_2, *)$ groups

$f: G_1 \to G_2$ is a group homomorphism if $\Longleftrightarrow$

$\Longleftrightarrow \forall x, y \in G_1, \; f(x \cdot y) = f(x) * f(y)$

$(R_1, +, \cdot)$, $(R_2, \oplus, \odot)$ rings

$f: R_1 \to R_2$ ring homo. $\Longleftrightarrow$ 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 and R_2 are unital rings (i.e. $\exists 1_{R_1}, 1_{R_2}$) then if $f(1_{R_1}) = 1_{R_2} \Rightarrow f$ is a unital homo.

$(R_1, +, \cdot)$, $(R_2, \oplus, \odot)$ fields

$f: R_1 \to R_2$ ring homo $\Leftrightarrow$ $f: R_1 \to R_2$ field homo.

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

Show that g is a group homo. between $(\mathbb{C}^*, \cdot)$ and $(GL_2(\mathbb{R}), \cdot)$

$\forall z_1, z_2 \in \mathbb{C}^*$, $g(z_1 z_2) \overset{?}{=} g(z_1) \cdot g(z_2)$

$z_1 = a_1 + b_1 i$
$z_2 = a_2 + b_2 i$

$z_1 \cdot z_2 = (a_1 + b_1 i)(a_2 + b_2 i) =$
$= a_1 a_2 + a_1 b_2 i + a_2 b_1 i - b_1 b_2 =$
$= a_1 a_2 - b_1 b_2 + i(a_1 b_2 + a_2 b_1)$

$$g(z_1 z_2) = \begin{pmatrix} a_1 a_2 - b_1 b_2 & a_1 b_2 + a_2 b_1 \\ -(a_1 b_2 + a_2 b_1) & a_1 a_2 - b_1 b_2 \end{pmatrix} \quad (*)$$

$$f(z_1)\cdot f(z_2)=\begin{pmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{pmatrix}\begin{pmatrix} a_2 & b_2 \\ -b_2 & a_2 \end{pmatrix}=$$

$$=\begin{pmatrix} a_1a_2-b_1b_2 & a_1b_2+a_2b_1 \\ -(a_1b_2+a_2b_1) & a_1a_2-b_1b_2 \end{pmatrix} \quad (2)$$

$\xrightarrow{(1),(2)}$ f - group homo.

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

Show that $(M,+,\cdot)$ field and that M is isomorphic to the field $(\mathbb{C},+,\cdot)$

Let $A_i=\begin{pmatrix} a_i & b_i \\ -b_i & a_i \end{pmatrix}$, $i=\overline{1,2}$

$$A_1-A_2=\begin{pmatrix} a_1-a_2 & b_1-b_2 \\ -b_1+b_2 & a_1-a_2 \end{pmatrix}\in M \Rightarrow (M,+)\leq$$

$\leq (M_2(\mathbb{R}),+)$

Also $O_2\in M \Rightarrow M\neq\emptyset$

$$A_1 \cdot A_2 = \begin{pmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ -b_2 & a_2 \end{pmatrix}$$

$$= \begin{pmatrix} a_1a_2 - b_1b_2 & a_1b_2 + a_2b_1 \\ -(a_1b_2 + a_2b_1) & a_1a_2 - b_1b_2 \end{pmatrix} \in M \Rightarrow$$

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

↳ submonoid

$I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in M$, for $a=1, b=0$

So far we know M is a unital ring

$$A_1A_2 = \begin{pmatrix} a_1a_2 - b_1b_2 & a_1b_2 + b_1a_2 \\ -(a_1b_2 + b_1a_2) & a_1a_2 - b_1b_2 \end{pmatrix}$$

$$A_2A_1 = \begin{pmatrix} a_2a_1 - b_2b_1 & a_1b_2 + b_2a_1 \\ -(a_2b_1 + b_2a_1) & a_2a_1 - b_2b_1 \end{pmatrix} = A_1A_2$$

So $\cdot$ is commutative in M but it is not in $M_2(\mathbb{R})$

Let $A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in M$

$A^t = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \Rightarrow A^* = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$

$A^{-1} = \frac{1}{\det A} \cdot A^* = \frac{1}{a^2+b^2} \cdot \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$

$A^{-1} = \begin{pmatrix} \frac{a}{a^2+b^2} & -\frac{b}{a^2+b^2} \\ \frac{b}{a^2+b^2} & \frac{a}{a^2+b^2} \end{pmatrix} \in M$

So, $(M, +, \cdot)$ field

define the function $f: M \to \mathbb{C}$

$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \to a+bi$

It's easy to show that f is a ring homo.

We have to show that f is bijective

(1) inj: if $f\begin{pmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{pmatrix} = f\begin{pmatrix} a_2 & b_2 \\ -b_2 & a_2 \end{pmatrix} \Rightarrow$

$\Rightarrow a_1 + b_1 i = a_2 + b_2 i \Rightarrow$

$\Rightarrow a_1 = a_2$ and $b_1 = b_2 \Rightarrow$

$\Rightarrow \begin{pmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{pmatrix} = \begin{pmatrix} a_2 & b_2 \\ -b_2 & a_2 \end{pmatrix}$

(2) surj: Let $a+bi \in \mathbb{C}$, then $f\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = a+bi$

(1), (2) $\Rightarrow$ f bijective
f ring homo
M, $\mathbb{C}$ fields
$\Rightarrow$ f field iso $\Rightarrow M \simeq \mathbb{C}$