$(G, \cdot)$ group

- $\cdot$ operation
- $\cdot$ associative
- $\cdot$ has a neutral number
- every element in G is invertable

$H \subseteq G$ is a subgroup ($H \subseteq G$)

if $(H, \cdot)$ is a group

Charact. Thm for subgroups: $(G, \cdot)$ group $H \subseteq G$

$H \subseteq G \iff$ (i) $H \neq \emptyset$

(ii) $\forall x, y \in H$: $xy \in H$ } stable part

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

$=$ $\forall x, y \in H \quad xy^{-1} \in H$

↑ you can use just this one for proof MOST of the time

Seminar 3

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.

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: $\forall f, g \in R^M$,

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

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

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

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

4. Let $U_n = \{z \in \mathbb{C} \mid z^n = 1\} \quad (n \in \mathbb{N}^*)$ be the *set of n-th roots of unity*. Prove that U_n is a subgroup of $(\mathbb{C}^*, \cdot)$.

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

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 $(M_2(\mathbb{R}), +, \cdot)$.

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

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.

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

3.4) Let $U_n = \{z \in \mathbb{C} \mid z^n = 1\}$, $n \in \mathbb{N}^*$, Prove that $(U_n, \cdot)$ is a subgroup of $(\mathbb{C}^*, \cdot)$ but $(U_n, +)$ is not a subgroup of $(\mathbb{C}, +)$

$H \subseteq G \iff$ (i) $H \neq \emptyset$

(ii) $\forall x, y \in H$, $xy \in H$ } stable part $=$ $\forall x, y \in H \quad xy^{-1} \in H$

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

↑ you can use just this one for proof MOST of the time

a) $(U_n, \cdot)$ (i) $1 \in U_n \Rightarrow U_n \neq \emptyset$

(ii) $\forall x, y \in U_n \Rightarrow xy \in U_n$

~~$(a+ib)(c+id) = ac + iad + i(bc) - bd = (ac - bd) + i(ad + bc)$~~

Let z_1 and $z_2 \in U_n$ s.t.

$\Rightarrow z_1^n = 1$, $z_2^n = 1$ } $\Rightarrow (z_1 z_2)^n = 1$

$z_1^n \cdot z_2^n = 1$ } $\Rightarrow z_1, z_2 \in U_n$

$1 \cdot 1 = 1$

(iii) $z_1 \in U_n$

$\left(z_1^{-1}\right)^n = z_1^{-n} = \frac{1}{z_1^n} = \frac{1}{1} = 1 \Rightarrow z_1^{-1} \in U_n$

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

b) $1 \in U_n$, but $1 + 1 = 2 \notin U_n \Rightarrow U_n \not\leq (\mathbb{C}, +)$

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

(i) (i) $GL_n(\mathbb{C}) = \{A \in M_n(\mathbb{C}) \mid \det(A) \neq 0\}$

$I_n \in GL_n(\mathbb{C}) \Rightarrow GL_n(\mathbb{C}) \neq \emptyset$

~~(ii)~~

Let A and $B \in GL_n(\mathbb{C}) \Rightarrow \begin{matrix} \det A \cdot \det B \neq 0 \\ \det(AB) \neq 0 \end{matrix} \Rightarrow A \cdot B \in GL_n(\mathbb{C}) \Rightarrow$ monoid

ii) Associativity is inherited from $M_n(\mathbb{C})$

$I_n \in GL_n(\mathbb{C}) \Rightarrow I_n$ is the neutral element

Let $A \in GL_n(\mathbb{C}) \Rightarrow \det A \neq 0 \Rightarrow \exists A^{-1}$ s.t. $A \cdot A^{-1} = I_n \Rightarrow \det A \cdot \det A^{-1} = 1 \Rightarrow$

$\Rightarrow \det A^{-1} \neq 0 \Rightarrow A^{-1} \in GL(\mathbb{C})$

iii) $SL_n(\mathbb{C}) = \{A \in M_n(\mathbb{C}) \mid \det A = 1\}$

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

(ii) $\forall A, B \in SL_n(\mathbb{C}) \overset{?}{\Rightarrow} A \cdot B \in SL_n(\mathbb{C})$

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

$\det A \cdot \det B = 1$

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

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

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

$\det I_n = \det A \cdot \det A^{-1}$

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

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

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

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

Char. thm. for subrings

$S \leq R \iff$ (i) $S \neq 0$
(ii) $(S, +) \leq (R, +)$
(iii) $(S, \cdot) \leq (R, \cdot)$

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

(iii) $\iff \forall x, y \in S : x \cdot y \in S$

if R is a field, for checking that S is a subfield you only need to add the condition:

$$\forall \underset{x \neq 0}{x \in S} : x^{-1} \in S$$

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 $(M_2(\mathbb{R}), +, \cdot)$.

$S \leq R \Leftrightarrow$ (i) $S \neq \emptyset$
(ii) $(S, +) \leq (R, +)$
(iii) $(S, \cdot) \leq (R, \cdot)$

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

(i) $I_2 \in \mathcal{M} \Rightarrow \mathcal{M} \neq \emptyset$

(ii) Let $X = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ $Y = \begin{pmatrix} d & e \\ 0 & f \end{pmatrix}$

$X - Y \stackrel{?}{\in} \mathcal{M}$

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

$a, b, \dots, e, f \in \mathbb{R} \Rightarrow \begin{matrix} a-d \in \mathbb{R} \\ b-e \in \mathbb{R} \\ c-f \in \mathbb{R} \end{matrix} \Rightarrow X - Y \in \mathbb{R}$

(iii) $X \cdot Y \in \mathcal{M}$

$$X \cdot Y = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} d & e \\ 0 & f \end{pmatrix} = \begin{pmatrix} ad & ae + bf \\ 0 & cf \end{pmatrix}$$

$a, b, \dots, e, f \in \mathbb{R} \Rightarrow \left.\begin{matrix} ad \in \mathbb{R} \\ ae + bf \in \mathbb{R} \\ cf \in \mathbb{R} \end{matrix}\right\} \Rightarrow X \cdot Y \in \mathbb{R}$

$\Rightarrow$ $\mathcal{M}$ - subring of $(\mathbb{R}, +, \cdot)$

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

$f : G_1 \to G_2$ is a **group homomorphism**

if $\forall x, y \in G_1$:

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

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

$f : R_1 \to R_2$ is a **ring homomorphism**

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, R_2 unital rings $(\exists 1_{R_1}, 1_{R_2})$ and $f(1_{R_1}) = 1_{R_2} \Rightarrow$ unital ring homomorphism

Remark If R_1, R_2 are fields, then:

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

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

if $\forall x, y \in \mathbb{C}^*$: $g(x \cdot y) = g(x) \cdot g(y)$

Let $z_1, z_1 \in \mathbb{C}^*$

$z_1 = a + ib$ $\quad$ $z_2 = c + id$

$g(z_1) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ $\quad$ $g(z_1) = \begin{pmatrix} c & d \\ -d & c \end{pmatrix}$

$g(z_1 \cdot z_2) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} c & d \\ -d & c \end{pmatrix}$

$g(ac - bd + (ad+bc)i) = \begin{pmatrix} ac-bd & ad+bc \\ -bc-ad & -bd+ac \end{pmatrix}$

$\begin{pmatrix} ac-bd & ad+bc \\ -ad-bc & ac-bd \end{pmatrix} =$ ✓ true

$\Rightarrow$ g is a group homo

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

→ morphism bijective function is bijective

Show that $\mathcal{M}$ is a field and it's isomorphic to $\mathbb{C}$

$(\mathcal{M}, +, \cdot)$ - field $\Leftrightarrow$ $(\mathcal{M}, +)$ - abelian group

$(\mathcal{M}, \cdot)$ - semigroup

$(\mathcal{M}, +)$ - abelian group

↳ associative enherike

↳ neutral element $O_2 \in \mathcal{M}$, $a = b = 0$

↳ invertable $\Rightarrow$ $A + A^{-1} = O_2$

$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} + A^{-1} = O_2$

$\Rightarrow A^{-1} = \begin{pmatrix} -a & -b \\ b & -a \end{pmatrix} = -A \in \mathcal{M}$ $\Rightarrow$ true

$(M, +, \cdot)$ - field $\Leftrightarrow$ $(M, +, \cdot)$ div. ring and "$\cdot$" commutative

Show that $(M, +, \cdot)$ is a subring of $(M_2(\mathbb{R}), +, \cdot)$

$M \neq \emptyset$ because $I_2 \in M$

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

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

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

$\Rightarrow (M, +, \cdot)$ is a subring of $M_2(R)$

$\Rightarrow M$ is a unital ring

* all elements invertable

$$A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \neq O_2$$

$\det A = a^2 + b^2 > 0 \quad \forall a, b \in \mathbb{R}$

$\Rightarrow \exists A^{-1}$

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

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

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

$\Rightarrow A \in M$, $A^{-1} \in M \Rightarrow M$ div. ring

* "$\cdot$" com $\Leftrightarrow \forall A, B \in M$, $A \cdot B = B \cdot A$

$$\begin{pmatrix} ac-bd & ad+bc \\ -bc-ad & ac-bd \end{pmatrix} = \begin{pmatrix} ca-db & cb+ad \\ -ad-bc & ac-bd \end{pmatrix} \Rightarrow \text{true}$$ commutative

$\Longrightarrow$ M - field

isomorphism

$f : \mathcal{H} \to \mathbb{C}$

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

To do

show that f is a homo rings

↳ + show bijective