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 $\Longleftrightarrow (a, n) = 1$.
(ii) Deduce that $(\mathbb{Z}_n, +, \cdot)$ is a field $\Longleftrightarrow n$ 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 $(\mathbb{C}, +, \cdot)$.