Seminar 1

1. Which ones of the usual symbols of addition, subtraction, multiplication and division define an operation (composition law) on the numerical sets $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$?

2. What algebraic structures with one operation (groupoid, semigroup, monoid or group) are the numerical sets $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ together with addition or multiplication?

3. Give examples of:
(i) a groupoid which is not a semigroup.
(ii) a semigroup which is not a monoid.
(iii) a monoid which is not a group.

4. Give example of a groupoid with identity element in which there exists an element having two different symmetric elements.

5. Let $A = \{a_1, a_2, a_3\}$ be a set. Determine the number of:
(i) operations on A;
(ii) commutative operations on A;
(iii) operations on A with identity element.
Generalization for a set A with n elements ($n \in \mathbb{N}^*$).

6. Let "$*$" be the operation on $\mathbb{R}$ defined by:

$$x * y = x + y + xy.$$

Show that:
(i) $(\mathbb{R}, *)$ is a commutative monoid.
(ii) The interval $[-1, \infty)$ is a stable subset of $(\mathbb{R}, *)$.

7. Let "$*$" be the operation on $\mathbb{N}$ defined by $x * y = \text{g.c.d.}(x, y)$.
(i) Prove that $(\mathbb{N}, *)$ is a commutative monoid.
(ii) Show that $D_n = \{x \in \mathbb{N} \mid x/n\}$ ($n \in \mathbb{N}^*$) is a stable subset of $(\mathbb{N}, *)$ and $(D_n, *)$ is a commutative monoid.
(iii) Fill in the table of the operation "$*$" on D_6.

8. Determine the finite stable subsets of $(\mathbb{Z}, \cdot)$.

9. Let A be a set and let $\mathcal{P}(A)$ be the power set of A (that is, the set of all subsets of A). What algebraic structure with one operation (groupoid, semigroup, monoid or group) is $\mathcal{P}(A)$ together with the operation "$\cup$" or "$\cap$"?

10. Let $(A, \cdot)$ be a groupoid and $X, Y \subseteq A$. Let "$\cdot$" be the operation on the power set $\mathcal{P}(A)$ defined by:

$$X \cdot Y = \{x \cdot y \mid x \in X, y \in Y\}.$$

Show that:
(i) If $(A, \cdot)$ is commutative, then $(\mathcal{P}(A), \cdot)$ is commutative.
(ii) If $(A, \cdot)$ is a semigroup, then $(\mathcal{P}(A), \cdot)$ is a semigroup.
(iii) If $(A, \cdot)$ is a monoid, then $(\mathcal{P}(A), \cdot)$ is a monoid.
(iv) If $(A, \cdot)$ is a group, then in general $(\mathcal{P}(A), \cdot)$ is not a group (for $A \neq \emptyset$).

Seminar 2

1. Let " $*$ " be the operation on $\mathbb{R}$ defined by:

$$x * y = xy - 5x - 5y + 30.$$

Is $(\mathbb{R}, *)$ a group? What about $(\mathbb{R} \setminus \{5\}, *)$?

2. Let $n \in \mathbb{N}$, $n \geq 2$. Show that the set

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

is a stable subset of the monoid $(M_n(\mathbb{R}), \cdot)$ and $(GL_n(\mathbb{R}), \cdot)$ is a group.

3. Let $n \in \mathbb{N}^*$. Show that the set

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

is a stable subset of the group $(\mathbb{C}^*, \cdot)$, $(U_n, \cdot)$ is an abelian group, and determine the elements of U_n.

4. Let $n \in \mathbb{N}$ and $\mathbb{Z}_n = \{\widehat{x} \mid x \in \mathbb{Z}\}$, where $\widehat{x} = x + n\mathbb{Z} = \{x + nk \mid k \in \mathbb{Z}\}$. Let "+" be the operation on $\mathbb{Z}_n$ defined by:

$$\widehat{x} + \widehat{y} = \widehat{x + y}, \quad \forall\, \widehat{x}, \widehat{y} \in \mathbb{Z}_n.$$

Show that $(\mathbb{Z}_n, +)$ is an abelian group and determine its cardinal (discussion on n).

5. Let $M \neq \emptyset$ be a set and

$$S_M = \{f : M \to M \mid f \text{ bijective}\}.$$

(i) Show that $(S_M, \circ)$ is a group.
(ii) If $|M| = n \in \mathbb{N}^*$, then we denote S_M by S_n. Determine the operation table for the group $(S_3, \circ)$.

6. Determine the operation table for the dihedral group $(D_3, \cdot)$ of rotations and symmetries of an equilateral triangle.

7. Determine the operation table for the dihedral group $(D_4, \cdot)$ of rotations and symmetries of a square.

8. Let $(G, \cdot)$ and $(G', \cdot)$ be groups with identity elements e and e' respectively. Let " $\cdot$ " be the operation on $G \times G'$ defined by:

$$(g_1, g_1') \cdot (g_2, g_2') = (g_1 \cdot g_2, g_1' \cdot g_2'), \quad \forall (g_1, g_1'), (g_2, g_2') \in G \times G'.$$

Show that $(G \times G', \cdot)$ is a group, called the *direct product* of the groups G and G'.

9. Determine the group of invertible elements of the monoids $(\mathbb{N}, +)$, $(\mathbb{N}, \cdot)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$, $(\mathbb{C}, \cdot)$, $(M_n(\mathbb{R}), \cdot)$ $(n \in \mathbb{N},\ n \geq 2)$ and $(M^M, \circ)$, where $M \neq \emptyset$ is a set and M^M denotes the set of all functions $f : M \to M$.

10. Let $(G, \cdot)$ be a group. Show that:
(i) G is abelian $\iff \forall x, y \in G,\ (xy)^2 = x^2 y^2$.
(ii) $\forall x \in G,\ x^2 = 1 \implies G$ is abelian.

Seminar 3

1. Which ones of the numerical sets $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are subgroups of the groups $(\mathbb{C}, +)$ and $(\mathbb{C}^*, \cdot)$?

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

3. Let $n \in \mathbb{N}$, $n \geq 2$. Show 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.
(iii) $SL_n(\mathbb{C}) = \{A \in M_n(\mathbb{C}) \mid \det(A) = 1\}$ is a subgroup of the group $(GL_n(\mathbb{C}), \cdot)$.

4. Let $n \in \mathbb{N}^*$. Show that $U_n = \{z \in \mathbb{C} \mid z^n = 1\}$ is a subgroup of the group $(\mathbb{C}^*, \cdot)$.

5. Consider the set $S(\mathbb{Z}, +) = \{n\mathbb{Z} \mid n \in \mathbb{N}\}$ of subgroups of the the group $(\mathbb{Z}, +)$ and $m, n \in \mathbb{N}$. Show that:
(i) $n\mathbb{Z} \subseteq m\mathbb{Z} \Longleftrightarrow m|n$.
(ii) $m\mathbb{Z} \cap n\mathbb{Z} = [m, n]\mathbb{Z}$, where $[m, n]$ denotes the least common multiple of m and n.
(iii) $m\mathbb{Z} + n\mathbb{Z} = (m, n)\mathbb{Z}$, where (m, n) denotes the greatest common divisor of m and n.

6. Let $(G, \cdot)$ be a group and $H, K \leq G$. Show that:

$$H \cup K \leq G \Longleftrightarrow H \subseteq K \text{ or } K \subseteq H\,.$$

7. Let $(G, \cdot)$ be a group and let $\emptyset \neq H \subseteq G$ be a finite set. Show that:

$$H \leq G \Longleftrightarrow H \text{ is a stable subset of } (G, \cdot).$$

8. Let $(G, \cdot)$ be a group. Prove that:

$$Z(G) = \{x \in G \mid x \cdot g = g \cdot x\,, \forall g \in G\}$$

is a subgroup of G, called *the center of* G. When does the equality $Z(G) = G$ hold?

9. Prove that:

$$Z(GL_2(\mathbb{R}), \cdot) = \{a \cdot I_2 \mid a \in \mathbb{R}^*\},$$

where I_2 is the identity matrix. Generalization for $GL_n(\mathbb{R})$ with $n \in \mathbb{N}$, $n \geq 2$.

10. Prove that $Z(S_3, \circ) = \{e\}$, where e is the identity permutation. Generalization for S_n with $n \in \mathbb{N}$, $n \geq 3$.

Seminar 4

1. (*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 $n \in \mathbb{N}$ and $g : \mathbb{Z} \to \mathbb{Z}_n$ be defined by $g(x) = \widehat{x}$. Prove that g is a group homomorphism between $(\mathbb{Z}, +)$ and $(\mathbb{Z}_n, +)$.

2. (*i*) Let $n \in \mathbb{N}$, $n \geq 2$ and let $\alpha : GL_n(\mathbb{R}) \to \mathbb{R}^*$ be defined by $\alpha(A) = \det(A)$. Show that α is a group homomorphism between $(GL_n(\mathbb{R}), \cdot)$ and $(\mathbb{R}^*, \cdot)$.
(*ii*) Let $n \in \mathbb{N}$, $n \geq 2$ and let $\beta : M_n(\mathbb{R}) \to \mathbb{R}$ be defined by $\beta(A) = \det(A)$. Show that β is not a group homomorphism between $(M_n(\mathbb{R}), +)$ and $(\mathbb{R}, +)$.

3. Determine the kernel and the image of the group homomorphisms from Ex. **1.** and **2.**

4. Let $f : \mathbb{C}^* \to GL_2(\mathbb{R})$ be defined by $f(a + bi) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$. Show that f is a group homomorphism between $(\mathbb{C}^*, \cdot)$ and $(GL_2(\mathbb{R}), \cdot)$.

5. Let $a, b \in \mathbb{N}$ and $f : \mathbb{C}^* \to \mathbb{R}^*$ be defined by $f(z) = a \cdot |z| + b$. Determine a, b such that f is a group homomorphism between $(\mathbb{C}^*, \cdot)$ and $(\mathbb{R}^*, \cdot)$.

6. Let $(G, \cdot)$ be a group and let $f : G \to G$ be defined by $f(x) = x^{-1}$. Show that $f \in \mathrm{End}(G) \iff G$ is abelian.

7. Show that the following groups are isomorphic: $(\mathbb{Z}_n, +)$ and $(U_n, \cdot)$ $(n \in \mathbb{N}^*)$.

8. Show that the following groups are isomorphic: Klein's group $(K, \cdot)$ and $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$.

9. Show that the following groups are isomorphic: $(\mathbb{R}, +)$ and $(\mathbb{R}^*_+, \cdot)$. $\to f(x) = a^x$, $a > 0$

10. Let $(G, \cdot)$ be a group with 3 elements. Determine $\mathrm{End}(G)$ and $\mathrm{Aut}(G)$.

11. Determine $\mathrm{Aut}(U_4, \cdot)$.

12. (*i*) Let $f \in \mathrm{End}(\mathbb{Z}, +)$. Show that $f(n) = f(1) \cdot n$, $\forall n \in \mathbb{Z}$.
(*ii*) $\forall a \in \mathbb{Z}$, let $t_a : \mathbb{Z} \to \mathbb{Z}$ be defined by $t_a(n) = a \cdot n$. Prove that:

$$\mathrm{End}(\mathbb{Z}, +) = \{t_a \mid a \in \mathbb{Z}\}$$

and determine $\mathrm{Aut}(\mathbb{Z}, +)$.

10.

$\cdot$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

$\Rightarrow a^{-1} = b$, $b^{-1} = a$ $\Rightarrow$

$\mathrm{End}(G)$: $f(x) = e$, $f(x) = x$, $f(x) = x^{-1}$

$\mathrm{Aut}(G)$: $f(x) = e$, $f(x) = x$

Seminar 5

1. Determine the order of each element and all generators of the cyclic groups $(\mathbb{Z}_8, +)$ and $(U_6, \cdot)$. Generators for $\mathbb{Z}_8$: $\hat{1}, \hat{3}, \hat{5}, \hat{7}$ | Generators for U_6: $\varepsilon_1, \varepsilon_5$

2. Determine the order of each element of Klein's group $(K, \cdot)$, permutation group $(S_3, \circ)$ and quaternion group $(Q, \cdot)$. Are they cyclic groups?

3. *(i)* Consider the matrices $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$ in the group $(GL_2(\mathbb{R}), \cdot)$. Determine $\operatorname{ord} A$, $\operatorname{ord} B$, $\operatorname{ord}(A \cdot B)$ and $\operatorname{ord}(B \cdot A)$.

(ii) Give an example of group in which there exist two elements of infinite order, whose product has finite order.

4. Let $(G, \cdot)$ be a group, and let $x, y \in G$ be such that $xy = yx$, $\operatorname{ord} x = m$ and $\operatorname{ord} y = n$ $(m, n \in \mathbb{N}^*)$. Then:

(i) $\operatorname{ord}(xy)$ is finite and divides $[m, n]$.

(ii) If $< x > \cap < y >= \{1\}$, then $\operatorname{ord}(xy) = [m, n]$.

(iii) If $(m, n) = 1$, then $\operatorname{ord}(xy) = m \cdot n$.

5. Let $(G, \cdot)$ be a group and $x, y \in G$. Show that:

$$\operatorname{ord}(xy) = \operatorname{ord}(yx).$$

6. Let $(G, \cdot)$ be an abelian group. Show that

$$t(G) = \{x \in G \mid \operatorname{ord} x \text{ is finite}\}$$

is a subgroup of G. Is the property still true if G is not abelian? ?

7. Let $(G, \cdot)$ and $(G', \cdot)$ be abelian groups. Show that if $G \simeq G'$, then $t(G) \simeq t(G')$.

8. Using **7.** show that the following groups are not isomorphic:

(i) $(\mathbb{Q}, +)$ and $(\mathbb{Q}^*, \cdot)$.

(ii) $(\mathbb{R}, +)$ and $(\mathbb{R}^*, \cdot)$.

9. Let $f : G \to G'$ be a group homomorphism and let $x \in G$ be an element of finite order. Prove that:

(i) $\operatorname{ord} f(x)$ is finite and $\operatorname{ord} f(x) | \operatorname{ord} x$.

(ii) If f is injective, then $\operatorname{ord} f(x) = \operatorname{ord} x$.

10. Using **9.** show that the groups $(\mathbb{Z}_4, +)$ and $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$ are not isomorphic.

Seminar 6

1. Let $n \in \mathbb{N}$, $n \geq 2$ and

$$SL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid \det(A) = 1\}\,,$$

$$GL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid \det(A) \neq 0\}\,.$$

Show that $SL_n(\mathbb{R})$ is a normal subgroup of the group $(GL_n(\mathbb{R}), \cdot)$.

2. For $a \in \mathbb{R}$, let $t_a : \mathbb{R} \to \mathbb{R}$ be defined by $t_a(x) = a \cdot x$. Is the set $H = \{t_a \mid a \in \mathbb{R}^*\}$ a normal subgroup of the symmetric group $(S_{\mathbb{R}}, \circ)$?

3. Show that the center

$$Z(G) = \{x \in G \mid x \cdot g = g \cdot x, \forall g \in G\}$$

of a group $(G, \cdot)$ is a normal subgroup.

4. Determine the (normal) subgroups and the factor groups of the group $(\mathbb{Z}, +)$.

5. Determine the (normal) subgroups and the factor groups of the group $(\mathbb{Z}_6, +)$. Fill in the operation table for one of the factor groups.

6. Determine the (normal) subgroups and the factor groups of Klein's group $(K, \cdot)$. Fill in the operation table for one of the factor groups.

7. Determine the normal subgroups of the group $(S_3, \circ)$ (compute S_3/r_H and S_3/r'_H for $H \leq S_3$). Determine the factor groups S_3/N, where N is a normal subgroup of S_3, and fill in the operation table for one of them.

8. Determine the normal subgroups of the quaternion group $(Q, \cdot)$. Determine the factor groups Q/N, where N is a normal subgroup of Q, and fill in the operation table for the group $(Q/N, \cdot)$, where $N = \{-1, 1\}$.

Seminar 7

1. Let $n \in \mathbb{N}$, $n \geq 2$. Prove the group isomorphism

$$(GL_n(\mathbb{R})/SL_n(\mathbb{R}), \cdot) \simeq (\mathbb{R}^*, \cdot)$$

by using the first isomorphism theorem.

2. Prove the group isomorphism

$$(\mathbb{C}/\mathbb{R}, +) \simeq (\mathbb{R}, +)$$

by using the first isomorphism theorem.

3. Let $m, n \in \mathbb{N}$ be such that $(m, n) = 1$. Prove the group isomorphism

$$(\mathbb{Z}_{mn}, +) \simeq (\mathbb{Z}_m \times \mathbb{Z}_n, +).$$

4. Consider the group $(\mathbb{Z}_{24}, +)$ and its cyclic subgroups $H =< \widehat{4} >$ and $N =< \widehat{6} >$. Determine $H \cap N$, $H + N$ and apply the second isomorphism theorem.

5. Determine the subgroups and the factor groups of the group $(\mathbb{Z}_{12}, +)$ by using the third isomorphism theorem.

6. Determine the subgroups of the groups $(\mathbb{Z}_n, +)$ for $n = 1, \ldots, 12$, and then draw the Hasse diagram of the subgroup lattice of each of them.

7. Determine the subgroups of the group $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$, and then draw the Hasse diagram of its subgroup lattice.

8. Determine the subgroups of the quaternion group $(Q, \cdot)$, and then draw the Hasse diagram of its subgroup lattice.

Seminar 8

1. Compute the composition (product) of the following permutations of 4 elements, and then determine the signature and the inverse of the result:

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

2. Determine the orbits of each element of the set $\{1, 2, 3, 4, 5\}$ relative to the permutation:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix}.$$

3. Decompose into products of disjoint cycles and into products of transpositions the following permutations:

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 4 & 6 & 1 & 5 & 7 & 3 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 4 & 7 & 2 & 5 & 1 & 8 & 9 & 3 \end{pmatrix}.$$

4. Write down all elements of the alternating groups A_3 and A_4, and then decompose these elements into products of disjoint cycles.

5. Let $H = \{\sigma \in S_5 \mid \sigma(1) = 1 \text{ or } \sigma(5) = 5\}$. Is H a subgroup of the group $(S_5, \circ)$?

6. Show the isomorphism $(D_3, \cdot) \simeq (S_3, \circ)$, where D_3 is the 3-rd dihedral group.

7. Determine the order of each element and the cyclic subgroups of the group $(S_3, \circ)$.

8. Determine the subgroups of the group $(S_3, \circ)$, and then draw the Hasse diagram of its subgroup lattice.

Seminar 9

1. Show that the sets $\mathbb{Z}_n$ (residue classes modulo n), $M_n(\mathbb{R})$ (matrices $n \times n$) and $\mathbb{R}[X]$ (polynomials) form rings together with the corresponding addition and multiplication. Are they commutative rings, integral domains, division rings or fields? Generalization.

2. Show that the set $\mathbb{R}^{\mathbb{R}}$ of functions $f : \mathbb{R} \to \mathbb{R}$ forms a ring together with the addition and the multiplication defined by: $\forall f, g \in \mathbb{R}^{\mathbb{R}}$, $(f+g)(x) = f(x) + g(x)$, $(f \cdot g)(x) = f(x) \cdot g(x)$, $\forall x \in \mathbb{R}$. Is it a commutative ring, integral domain, division ring or field? Generalization.

3. Let $(G, +)$ be an abelian group. Show that $(\mathrm{End}(G), +, \circ)$ is a ring with identity.

4. Let $(R, +, \cdot)$ be a ring. Consider on the set $\mathbb{Z} \times R$ the addition and the multiplication defined by:

$$\begin{aligned}(m,a) + (n,b) &= (m+n, a+b),\\ (m,a) \cdot (n,b) &= (mn, ab + na + mb),\end{aligned}$$

$\forall (m,a), (n,b) \in \mathbb{Z} \times R$. Show that $(\mathbb{Z} \times R, +, \cdot)$ is a ring with identity.

5. Let $n \in \mathbb{N}$, $n \geq 2$ and $\widehat{0} \neq \widehat{a} \in \mathbb{Z}_n$. Prove that:

$$\widehat{a} \text{ is invertible in the ring } (\mathbb{Z}_n, +, \cdot) \Longleftrightarrow (a, n) = 1.$$

When is $(\mathbb{Z}_n, +, \cdot)$ a field?

6. Solve the following equations in the ring $(\mathbb{Z}_{12}, +, \cdot)$: $\widehat{4}x + \widehat{5} = \widehat{9}$ and $\widehat{5}x + \widehat{5} = \widehat{9}$.

7. Solve the following system of equations in the ring $(\mathbb{Z}_{12}, +, \cdot)$:

$$\begin{cases}\widehat{3}x + \widehat{4}y = \widehat{11}\\ \widehat{4}x + \widehat{9}y = \widehat{10}\end{cases}.$$

8. Solve the equation $\begin{pmatrix}1 & 2\\ 1 & 2\end{pmatrix} X = \begin{pmatrix}1 & 2\\ 1 & 2\end{pmatrix}$ in the ring $(M_2(\mathbb{C}), +, \cdot)$.

9. Let $\mathcal{M} = \left\{ \begin{pmatrix} a & b\\ 2b & a\end{pmatrix} \middle| a, b \in \mathbb{Q} \right\} \subseteq M_2(\mathbb{Q})$. Show that $\mathcal{M}$ is a stable subset of the ring $(M_2(\mathbb{Q}), +, \cdot)$ and $(\mathcal{M}, +, \cdot)$ is a field.

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 $\mathcal{M}$ is a stable subset of the ring $(M_2(\mathbb{R}), +, \cdot)$ and $(\mathcal{M}, +, \cdot)$ is a field.

Seminar 10

1. Are the following sets subrings of the field $\mathbb{C}$:
(i) $A = \{b\mathrm{i} \mid b \in \mathbb{R}\}$;
(ii) $B = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}$;
(iii) $C = \{z \in \mathbb{C} \mid |z| \leq 1\}$?

2. Show that the set $\mathbb{Z}[\mathrm{i}] = \{a + b\mathrm{i} \mid a, b \in \mathbb{Z}\}$ is a subring of the field $\mathbb{C}$, called *the ring of Gauss integers*. Determine its invertible elements.

3. Are the following sets subrings of the ring $M_2(\mathbb{R})$:
(i) $\mathcal{A} = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \middle| a, b, c \in \mathbb{R} \right\}$;
(ii) $\mathcal{B} = \left\{ \begin{pmatrix} a & a \\ 0 & b \end{pmatrix} \middle| a, b \in \mathbb{R} \right\}$;
(iii) $\mathcal{C} = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \middle| a, b \in \mathbb{R} \right\}$?

4. Are the following sets subrings of the ring $\mathbb{R}[X]$:
(i) $A = \{f \in \mathbb{R}[X] \mid \text{the free term of } f \text{ is } 0\}$;
(ii) $B = \{f \in \mathbb{R}[X] \mid \text{the free term of } f \text{ is } 1\}$;
(iii) $C = \{f \in \mathbb{R}[X] \mid \text{the coefficient of the term of degree 1 of } f \text{ is } 0\}$?

5. Give examples of:
(i) subring without identity of a ring with identity.
(ii) subring with identity of a ring with identity, which have different identities.
(iii) non-commutative finite ring.

6. Show that the set $\mathbb{Q}(\sqrt{2}) = \{a+b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ is a subfield of the field $\mathbb{R}$. Generalization.

7. Is the set $A = \{a + b\sqrt[3]{2} \mid a, b \in \mathbb{Q}\}$ a subring of the field $\mathbb{R}$?

8. Let $m, n \in \mathbb{N}$. Show that $n\mathbb{Z}$ is a subring of the ring $m\mathbb{Z} \Leftrightarrow m|n$.

9. Let $(R, +, \cdot)$ be a ring. Show that:

$$Z(R) = \{a \in R \mid a \cdot r = r \cdot a \,, \forall r \in R\}$$

is a subring of R, called the *center of* R. When does the equality $Z(R) = R$ hold?

10. Show that:

$$Z(M_2(\mathbb{R}), +, \cdot) = \{a \cdot I_2 \mid a \in \mathbb{R}\},$$

where I_2 is the identity matrix. Generalization for $M_n(\mathbb{R})$ with $n \in \mathbb{N}$, $n \geq 2$.

Seminar 11

1. *Let R be a ring. An element $a \in R$ is called idempotent if $a^2 = a$.*
Determine the idempotents of the ring $\mathbb{Z}_{12}$, and write down 4 idempotents of the ring $M_2(\mathbb{Z})$.

2. *Let R be a ring. An element $a \in R$ is called nilpotent if there exists $n \in \mathbb{N}$ such that $a^n = 0$.*

Determine the nilpotent elements of the ring $\mathbb{Z}_{12}$, and write down 2 nilpotent elements of the ring $M_2(\mathbb{Z})$.

3. Are the following functions ring homomorphism between the corresponding rings:
(i) $f : \mathbb{Z} \to \mathbb{Z}_n$ defined by $f(x) = \widehat{x}$;
(ii) $f : \mathbb{R} \to M_2(\mathbb{R})$ defined by $f(x) = \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}$;
(iii) $g : M_2(\mathbb{R}) \to \mathbb{R}$ defined by $g(A) = \det(A)$?

4. Let $f : \mathbb{Z}_{12} \to \mathbb{Z}_4$ be defined by $f(\widehat{x}) = \overline{x}$. Prove that f is well defined (that is, f is a function) and f is a ring homomorphism.

5. Consider the fields $(\mathcal{M}, +, \cdot)$ and $(\mathbb{Q}(\sqrt{2}), +, \cdot)$, where $\mathcal{M} = \left\{ \begin{pmatrix} a & b \\ 2b & a \end{pmatrix} \middle| a, b \in \mathbb{Q} \right\}$ and $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. Show that the fields $(\mathcal{M}, +, \cdot)$ and $(\mathbb{Q}(\sqrt{2}), +, \cdot)$ are isomorphic.

6. Consider the field $(\mathcal{M}, +, \cdot)$, where $\mathcal{M} = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \middle| a, b \in \mathbb{R} \right\}$. Show that the fields $(\mathcal{M}, +, \cdot)$ and $(\mathbb{C}, +, \cdot)$ are isomorphic.

7. For $a \in \mathbb{Z}$, let $t_a : \mathbb{Z} \to \mathbb{Z}$ be defined by $t_a(x) = ax$. Using the result $\mathrm{End}(\mathbb{Z}, +) = \{t_a \mid a \in \mathbb{Z}\}$, show that $\mathrm{End}(\mathbb{Z}, +, \cdot) = \{t_0, t_1\}$ and $\mathrm{Aut}(\mathbb{Z}, +, \cdot) = \{t_1\}$.

8. Consider the field $(\mathbb{Q}(\sqrt{2}), +, \cdot)$, where $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. Determine $\mathrm{Aut}(\mathbb{Q}(\sqrt{2}), +, \cdot)$.

Seminar 12

1. Are the following sets (left, right, two-sided) ideals of the ring $M_2(\mathbb{R})$:
(i) $\mathcal{A} = \left\{ \begin{pmatrix} a & a \\ 0 & 0 \end{pmatrix} \middle| a \in \mathbb{R} \right\}$;
(ii) $\mathcal{B} = \left\{ \begin{pmatrix} a & a \\ 0 & b \end{pmatrix} \middle| a, b \in \mathbb{R} \right\}$;
(iii) $\mathcal{C} = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \middle| a, b \in \mathbb{R} \right\}$?

2. In an arbitrary ring, is the intersection of a left ideal and a right ideal a two-sided ideal?

3. Are the following sets ideals of the ring $\mathbb{R}[X]$:
(i) $A = \{f \in \mathbb{R}[X] \mid \text{the free term of } f \text{ is } 0\}$;
(ii) $B = \{f \in \mathbb{R}[X] \mid \text{the free term of } f \text{ is } 1\}$;
(iii) $C = \{f \in \mathbb{R}[X] \mid \text{the coefficient of the term of degree 1 of } f \text{ is } 0\}$?

4. Let $R = \{\frac{m}{n} \in \mathbb{Q} \mid n \text{ is odd}\}$ and $U = \{\frac{m}{n} \in R \mid m \text{ is even}\}$. Show that R is a subring of the field $\mathbb{Q}$ and U is an ideal of R.

5. Let R be a ring and $a \in R$. Show that $Ra = \{ra \mid r \in R\}$ is a left ideal of R and $aR = \{ar \mid r \in R\}$ is a right ideal of R.

6. Let R be a ring and

$$Ann(R) = \{a \in R \mid \forall x \in R, ax = 0 = xa\}.$$

Show that $Ann(R)$ is an ideal of R, called the *annihilator* of R.

7. Determine the ideals of the ring $\mathbb{Z}_8$, and draw the Hasse diagram of its ideal lattice.

8. Determine the ideals of the ring $\mathbb{Z}_{12}$ and draw the Hasse diagram of its ideal lattice.

Seminar 13

1. Let $n \in \mathbb{N}$, $n \geq 2$. Prove the ring isomorphism

$$\mathbb{Z}[X]/(n) \cong \mathbb{Z}_n[X]$$

by using the first isomorphism theorem.

?**2.** Prove the ring isomorphism

$$\mathbb{Q}[X]/(X+1) \cong \mathbb{Q}$$

by using the first isomorphism theorem.

?**3.** Prove the ring isomorphism

$$\mathbb{R}[X]/(X^2+1) \cong \mathbb{C}$$

by using the first isomorphism theorem.

4. Let

$$R = \left\{ \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix} \middle| a, b \in \mathbb{Q} \right\}, \quad I = \left\{ \begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix} \middle| a \in \mathbb{Q} \right\}.$$

Show that R is a subring of the ring $\mathbb{M}_2(\mathbb{Q})$, I is an ideal of R and $R/I \cong \mathbb{Q}$.

5. Determine the factor rings of the ring $\mathbb{Z}_{12}$ by using the third isomorphism theorem.

6. Determine the characteristic of the ring $\mathbb{Z}_4 \times \mathbb{Z}_6$. Generalization for the ring $\mathbb{Z}_m \times \mathbb{Z}_n$ ($m, n \in \mathbb{N}$, $m, n \geq 2$).

7. Give examples of:
(i) Infinite ring having finite characteristic.
(ii) Commutative ring with identity which is not a field but has a prime characteristic.

8. Let R be a unitary commutative ring with $1 \neq 0$ and $\mathrm{char}(R) = p$ for some prime p. Prove that:

$$(a+b)^p = a^p + b^p, \quad \forall a, b \in R.$$