Seminar 3

$(G, *)$ is a group, if $*$ is associative, has identity element and all elements have a symmetric.

$(R, +, \cdot)$ is a ring if $(R, +)$ is an Abelian group, $(R^*, \cdot)$ is a semigroup and distributivity holds.

$(H, +)$ is a subgroup of $(G, +)$ if H is a stable subset $(\forall x, y \in H : x + y \in H)$ of G and $(H, +)$ is also a group. Or, we may also say that $H \neq \emptyset$ and $\forall x, y \in H : x - y \in H$.

$(H, +, \cdot)$ is a subring of $(G, +, \cdot)$ if $\mid H \mid \geq 2$, $\forall x, y \in H : x - y \in H$ and $\forall x, y \in H : x \cdot y \in H$.

$f : (G_1, \circ) \to (G_2, *)$ is a group homomorphism if $\forall x, y \in G_1 \Rightarrow f(x \circ y) = f(x) * f(y)$.

$f : (G_1, \circ) \to (G_2, *)$ is a group isomorphism if f is a group homomorphism and f is also bijective (i.e. f is injective and surjective).

We can say that two groups are isomorphic if there exists a group isomorphism between them, i.e. we find a function between the two groups, which is a group isomorphism.

1. To be a group, we have to prove that the operation is associative, has identity element and all elements have a symmetric.

   Associativity: $\forall f_1, f_2, f_3 \in S_M \Rightarrow ((f_1 \circ f_2) \circ f_3)(x) = (f_1 \circ (f_2 \circ f_3))(x)$, for any $x \in M$.

   $((f_1 \circ f_2) \circ f_3)(x) = (f_1 \circ f_2)(f_3(x)) = f_1(f_2(f_3(x))) = (f_1(f_2 \circ f_3))(x) = (f_1 \circ (f_2 \circ f_3))(x)$ (true)

   Identity element: $\exists e \in S_M$ such that $\forall f \in S_M : (e \circ f)(x) = (f \circ e)(x) = f(x), \forall x \in M$. Remember that the elements of S_M are functions. So e also has to be a function. Take the second composition: $(f \circ e)(x) = f(e(x)) = f(x) \Rightarrow e(x) = x$. But this is the identity function $1_M \in S_M$, as 1_M is bijective.

   Symmetric: $\forall f \in S_M, \exists f^{-1} \in S_M$ such that $(f \circ f^{-1})(x) = (f^{-1} \circ f)(x) = 1_M(x)$. As f is a bijective function, i.e. f has an inverse, f^{-1}, which is also bijective. So, each function in S_M has an inverse.

   In the end, $(S_M, \circ)$ is a group.

2. For $(R, +, \cdot)$ to be a ring we have to prove that $(R, +)$ is an Abelian group, $(R^*, \cdot)$ is a semigroup and distributivity holds.

$(R, +)$ **group**: We can easily see that $+$ is associative and commutative. The identity element is $\theta(x) = 0 \in R^M$ and each function $f(x)$ has a symmetric $-f(x)$.

$(R, \cdot)$ **semigroup**: Here, $\cdot$ has to be associative, which can be easily proved.

Distributivity: $\forall f, g, h \in R^M : (f \cdot (g+h))(x) = (f \cdot g)(x) + (f \cdot h)(x)$. And it's true.

So, in the end, $(R^M, +, \cdot)$ is a ring. If R is commutative, then R^M is also commutative and if R has an identity element w.r.t. the second operation, then R^M has also an identity element w.r.t. the second operation, which is different from the one in R. ($\epsilon(x) = 1$ to be precise)

3. Remember: $z \in \mathbb{C} \Rightarrow z = a + bi, a, b \in \mathbb{R} \Rightarrow \mid z \mid = \sqrt{a^2 + b^2}$

   For $(H, \cdot)$ to be a subgroup of $(\mathbb{C}^*, \cdot)$, we have to prove that $H \neq \emptyset$ and $\forall x, y \in H : x \cdot y^{-1} \in H$. (Another way to prove this, is that H is a stable subset of $\mathbb{C}^*$ and $(H, \cdot)$ is a group).

   For $H \neq \emptyset$ we have to find a $z \in H$ such that $\mid z \mid = 1$ (in other words, give me an example of such an element). Take $z = 1 \in H \Rightarrow \mid 1 \mid = 1$ (true).

   Now, $\forall z_1, z_2 \in H : z_1 \cdot z_2^{-1} \in H$. If $z_1, z_2 \in H \Rightarrow \mid z_1 \mid = 1$ and $\mid z_2 \mid = 1$. First, we have to prove that our $z_2^{-1} \in H$,so $z_2^{-1} = \frac{1}{z_2} \Rightarrow \mid z_2^{-1} \mid = \frac{1}{|z_2|} = \frac{1}{1} = 1 \Rightarrow z_2^{-1} \in H$. Now, $z_1 \cdot z_2^{-1} = z_1 \cdot \frac{1}{z_2} = \frac{z_1}{z_2}$ and for it to be in H, its modulus has to be $1 \Rightarrow \mid z_1 \cdot z_2^{-1} \mid = \frac{|z_1|}{|z_2|} = 1 \Rightarrow z_1 \cdot z_2^{-1} \in H$.

   In the end, $(H, \cdot) \leq (\mathbb{C}^*, \cdot)$.

   To prove that $(H, +) \nleq (\mathbb{C}, +)$, we can find an example such that $(H, +)$ is not a stable subset. So, take $z_1 = 1$ and $z_2 = i \Rightarrow \mid z_1 \mid = 1$ and $\mid z_2 \mid = 1$, both in H. But $z_1 + z_2 = 1 + i \Rightarrow \mid z_1 + z_2 \mid = \sqrt{1+1} = \sqrt{2} \notin H$.

4. As before, we prove, first, that $U_n \neq \emptyset$. Take: $z = 1 \in U_n \Rightarrow z^n = 1^n = 1$ (true). Now, $\forall z_1, z_2 \in U_n \Rightarrow z_1^n = 1$ and $z_2^n = 1$, where $z_2^{-1} = \frac{1}{z_2} \in \mathbb{C} \Rightarrow (z_2^{-1})^n = \frac{1}{z_2^n} = \frac{1}{1} = 1$. So, $z_1 \cdot z_2^{-1} = \frac{z_1}{z_2} \Rightarrow (z_1 \cdot z_2^{-1})^n = \frac{z_1^n}{z_2^n} = \frac{1}{1} = 1 \in U_n$.

5. (i) $\forall A, B \in GLn(\mathbb{C}) \Rightarrow det(A) \neq 0$ and $det(B) \neq 0 \Rightarrow det(A) \cdot det(B) \neq 0 \Rightarrow det(A \cdot B) \neq 0 \Rightarrow A \cdot B \in GLn(\mathbb{C})$. So $GLn(\mathbb{C})$ stable subset of $(M_n(\mathbb{C}), \cdot)$.

   (ii) Associativity is easy to prove. The identity element for multiplication of matrices is I_n, with $det(I_n) \neq 0$. For the inverse of a matrix, we know that it exists if the determinant of the matrix is different from 0, which we have. We only need to prove that the inverse of each matrix is also in $GLn(\mathbb{C})$: $det(A \cdot A^{-1}) = det(I_n)$, as $A \cdot A^{-1} = I_n \Rightarrow det(A) \cdot det(A^{-1}) = 1$, but $det(A) \neq 0 \Rightarrow det(A^{-1}) \neq 0 \Rightarrow A^{-1} \in GLn(\mathbb{C})$.

   (iii) We use that $SLn(\mathbb{C})$ has to be a stable subset of $GLn(\mathbb{C})$ and $(SLn(\mathbb{C}), \cdot)$ is also a group. For the first part: $\forall A, B \in SLn(\mathbb{C}) \Rightarrow det(A) = 1$ and $det(B) = 1 \Rightarrow det(A) \cdot det(B) = det(A \cdot B) = 1 \Rightarrow A \cdot B \in SLn(\mathbb{C})$. For the second part, it is easy to prove that multiplication of matrices in $SLn(\mathbb{C})$ is associative, the identity element is I_n and the inverse of each matrix exists and it is also in $SLn(\mathbb{C})$.

6. (i) To show that $(\mathbb{Z}[i], +, \cdot)$ is a subring of $(\mathbb{C}, +, \cdot)$, we will prove that: $\mid \mathbb{Z}[i] \mid \geq 2$, $\forall x, y \in \mathbb{Z}[i] : x - y \in \mathbb{Z}[i]$ and $\forall x, y \in \mathbb{Z}[i] : x \cdot y \in \mathbb{Z}[i]$. To prove that we have at least two elements in $\mathbb{Z}[i]$, we have to give examples: $0 = 0 + 0i$ and $1 = 1 + 0i$ are both in $\mathbb{Z}[i]$.

   The second part: $\forall x, y \in \mathbb{Z}[i] \Rightarrow x = a_1 + b_1 i$ and $y = a_2 + b_2 i$, where $-y = -a_2 - b_2 i \in \mathbb{Z}[i] \Rightarrow x - y = (a_1 - a_2) + (b_1 - b_2)i \in \mathbb{Z}[i]$, as $a_1 - a_2 \in \mathbb{Z}$ and $b_1 - b_2 \in \mathbb{Z}$.

   Finally, we have: $x \cdot y = (a_1 a_2 - b_1 b_2) + (a_1 b_2 + b_1 a_2)i \in \mathbb{Z}[i]$, as $a_1 a_2 - b_1 b_2 \in \mathbb{Z}$ and $a_1 b_2 + b_1 a_2 \in \mathbb{Z}$.

   So $(\mathbb{Z}[i], +, \cdot)$ is a subring of $(\mathbb{C}, +, \cdot)$.

   (ii) Here, we use the same thing. So, for M to have at least two elements, we find the matrices $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ and $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in M$. Then $\forall A, B \in M \Rightarrow A = \begin{bmatrix} a_1 & b_1 \\ 0 & c_1 \end{bmatrix}$ and $B = \begin{bmatrix} a_2 & b_2 \\ 0 & c_2 \end{bmatrix} \Rightarrow A - B = \begin{bmatrix} a_1 - a_2 & b_1 - b_2 \\ 0 & c_1 - c_2 \end{bmatrix} \in M$, as $a_1 - a_2, b_1 - b_2, c_1 - c_2 \in \mathbb{R}$. And $A \cdot B = \begin{bmatrix} a_1 a_2 & a_1 b_2 + b_1 c_2 \\ 0 & c_1 c_2 \end{bmatrix} \in M$, as $a_1 a_2, a_1 b_2 + b_1 c_2, c_1 c_2 \in \mathbb{R}$. So, $(M, +, \cdot)$ is a subring of $(M_2(\mathbb{R}), +, \cdot)$.

7. (i) For f to be a group homomorphism, we have to prove that: $\forall z_1, z_2 \in \mathbb{C}^* \Rightarrow f(z_1 \cdot z_2) = f(z_1) \cdot f(z_2)$.
   So, $f(z_1 \cdot z_2) =| z_1 \cdot z_2 |=| z_1 | \cdot | z_2 |= f(z_1) \cdot f(z_2)$ (true).
   (ii) The same things go for g: $\forall z_1, z_2 \in \mathbb{C}^* \Rightarrow z_1 = a_1 + b_1 i$ and $z_2 = a_2 + b_2 i$.

$$g(z_1 \cdot z_2) = g(a_1a_2 - b_1b_2 + i(a_1b_2 + a_2b_1)) = \begin{bmatrix} a_1a_2 - b_1b_2 & a_1b_2 + a_2b_1 \\ -a_1b_2 - a_2b_1 & a_1a_2 - b_1b_2 \end{bmatrix}$$

$$g(z_1) \cdot g(z_2) = \begin{bmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{bmatrix} \cdot \begin{bmatrix} a_2 & b_2 \\ -b_2 & a_2 \end{bmatrix} = \begin{bmatrix} a_1a_2 - b_1b_2 & a_1b_2 + a_2b_1 \\ -a_1b_2 - a_2b_1 & a_1a_2 - b_1b_2 \end{bmatrix}$$

   So, $g(z_1 \cdot z_2) = g(z_1) \cdot g(z_2) \Rightarrow g$ is a group homomorphism.

8. For $(\mathbb{Z}_n, +)$ to be isomorphic with $(U_n, \cdot)$, we have to find a function between them, which is a group isomomorphism.

   Take, $f : U_n \to \mathbb{Z}_n$, such that $f(z^k) = k, \forall k \in \mathbb{Z}_n$. We can easily see that f is a group homomorphism, as $f(z^{k_1} \cdot z^{k_2}) = f(z^{k_1+k_2}) = k_1 + k_2 = f(z^{k_1}) + f(z^{k_2})$. And also, f is a bijetive function.

   Pay attention to the case: $k = n$, where $n \in \mathbb{Z}_n$ is $0 \Rightarrow f(z^n) = f(1) = 0 = n \in \mathbb{Z}_n$.