Seminar 9

1. (a) $(\mathbb{Z}_n, +, \cdot)$

   We know that $(\mathbb{Z}_n, +)$ is an abelian group and also, the operation of $(\mathbb{Z}_n, \cdot)$ is associative. So, to be a ring, we only have to see if distributivity holds: $\hat{x}(\hat{a}+\hat{b}) = \hat{x}\cdot\widehat{a+b} = \hat{x}(a+b+n(a'+b')) = (x+nx')(a+b+n(a'+b')) = xa+xb+nxa'+nxb'+nx'a+nx'b+nnx'a'+nnx'b' = (xa+nxa'+nx'a+nnx'a')+(xb+nxb'+nx'b+nnx'b') = (x+nx')(a+na')+(x+nx')(b+nb') = \widehat{xa}+\widehat{xb} \Rightarrow (\mathbb{Z}_n, +, \cdot)$ is a ring. We know that multiplication is commutative, the identity element is $\hat{1}$ and by it's properties, we immediately deduce that it is a division ring, also. So, $(\mathbb{Z}_n, +, \cdot)$ is an integral domain. But to be a field, every element has to be invertible, which is not true for any n.

   (b) $(M_n(\mathbb{R}), +, \cdot)$

   It is easy to prove that $(M_n(\mathbb{R}), +, \cdot)$ is a ring. Here, the multiplication is not commutative. The identity element is I_n. If it were a division ring, then it should not have zero divisors, hence it should satisfy the property $\forall A, B \in M_n(\mathbb{R}) : A \cdot B = O_n \Rightarrow A = O_n$ or $B = O_n$. If we take $A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$, by computing $A \cdot B$ we get the matrix O_2. So it is not a division ring, which means it is not an integral domain. We know that only matrices which have the determinant different from 0 are invertible, so $(M_n(\mathbb{R}), +, \cdot)$ is not a field.

   (c) $(\mathbb{R}[X], +, \cdot)$

   We can easily see that $(\mathbb{R}[X], +, \cdot)$ is a ring. The multiplication is commutative and the identity element is the polynomial 1. It is not a division ring and not a field, because not every element is invertible (take the polynomial $f = X$). As $(\mathbb{R}, +, \cdot)$ is an integral domain, so is the set of polynomials over $\mathbb{R}$.

2. We know that addition is associative, commutative, the identity element is $\theta(x) = 0, \forall x \in \mathbb{R}$, and for any function f, we find it's symmetric $-f$. Also, the multiplication is associative, as $(f \cdot (g \cdot h))(x) = f(x) \cdot (g \cdot h)(x) = f(x) \cdot g(x) \cdot h(X) = (f \cdot g)(x) \cdot h(x) = ((f \cdot g) \cdot h)(x)$. And distributivity holds, by using the same reasoning. So $(\mathbb{R}^{\mathbb{R}}, +, \cdot)$ is a ring, which is commutative. The identity element is the function

$f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = 1, \forall x \in \mathbb{R}$. It is not a division ring. To prove that, let's take the next functions:

$$f = \begin{cases} 1 - 3x & if\ x \in [0, \frac{1}{3}] \\ 0 & if\ x \in [\frac{1}{3}, 1] \end{cases}$$

$$g = \begin{cases} 0 & x \in [0, \frac{1}{3}] \\ 0 & if\ 3x - 1 \in [\frac{1}{3}, 1] \end{cases}$$

Then $f \cdot g = 0$, even if neither f nor g are everywhere 0. So it is not an integral domain, hence not a field.

3. Remember that: $f \in End(G) \iff f(x+y) = f(x) + f(y), \forall x, y \in G$.

   Now we have to see if the operations are well-defined. Take two functions $f, g \in End(G)$, which have the property above. Then for every $x, y \in G$, we have:

$$\begin{aligned}(f+g)(x+y) &= f(x+y) + g(x+y) \\ &= f(x) + f(y) + g(x) + g(y) \\ &= (f+g)(x) + (f+g)(y),\end{aligned}$$

$$\begin{aligned}(f \circ g)(x+y) &= f(g(x+y)) = f(g(x) + g(y)) \\ &= f(g(x)) + f(g(y)) = (f \circ g)(x) + (f \circ g)(y).\end{aligned}$$

   From exercise 2, we know that addition is associative, commutative, the identity element is $\theta(x) = 0$ and every function has an inverse.

   Composition is associative, because the composition of functions is associative.

   For every $f, g, h \in End(G)$ and every $x \in G$, we have:

$$\begin{aligned}(f \circ (g+h))(x) &= f((g+h)(x)) = f(g(x) + h(x)) \\ &= f(g(x)) + f(h(x)) = (f \circ g)(x) + (f \circ h)(x),\end{aligned}$$

   and similarly on the other side, so distributivity holds.

   Hence $(End(G), +, \circ)$ is a ring, with identity element 1_G.

4. Take (m,a), (n,b), $(p,c) \in \mathbb{Z} \times R$.

   $(m,a)+((n,b)+(p,c)) = (m,a)+(n+p,b+c) = (m+n+p,a+b+c) = (m+n,a+b)+(n,c) = ((m,a)+(n,b))+(p,c)$, so addition is associative.

   $(m,a)+(n,b) = (m+n,a+b) = (n+m,b+a) = (n,b)+(m,a)$, so addition is commutative.

   $(m,a)+(0,0') = (m,a)$, where 0 is the identity element in $\mathbb{Z}$ (ring) and $0'$ is the identity element in R (ring).

   $(m,a)+(-m,-a) = (0,0')$, where $-m$ is the inverse of m in $\mathbb{Z}$ (ring) and $-a$ is the inverse of a in R (ring).

   So $(\mathbb{Z} \times R, +)$ is an abelian group.

   By simple computations, we get that: $(m,a)\cdot((n,b)\cdot(p,c)) = (mnp, anp+mbc+mbp+mnc+abc+abp+anc) = ((m,a)\cdot(n,b))\cdot(p,c)$. So, the multiplication is associative. Also, it is clearly commutative.

   Also, we see that: $(m,a)\cdot((n,b)+(p,c)) = (mn+mp, ab+ac+bm+mc+an+ap) = (m,a)\cdot(n,b)+(m,a)\cdot(p,c)$. So, distributivity holds.

   In conclusion, $(\mathbb{Z} \times R, +, \cdot)$ is a ring. To find the identity element, we use the fact that $\mathbb{Z}$ has the identity element 1.

   $(m,a)\cdot(1,x) = (m,a) \Rightarrow (m, ax+mx+a) = (m,a) \Rightarrow a = a(x+1)+mx \Rightarrow x+1 = 1$ and $x = 0$. So, the identity element in $(\mathbb{Z} \times R, +, \cdot)$ is $(1,0)$.

5. We know that $(a,n) = 1 \iff \exists x,y \in \mathbb{Z}$ such that $ax+ny = 1$.

   $\boxed{\Rightarrow}$ $\hat{a}$ invertible $\Rightarrow \exists \hat{b} \in \mathbb{Z}_n$ such that $\hat{a}\cdot\hat{b} = \hat{1} \iff \widehat{ab} = \hat{1} \iff n \mid ab-1 \iff \exists k$ such that $ab-1 = nk \iff \exists k$ such that $ab+n(-k) = 1 \Rightarrow (a,n) = 1$.

   $\boxed{\Leftarrow}$ $(a,n) = 1 \Rightarrow \exists x,y \in \mathbb{Z}$ such that $ax+ny = 1 \iff \widehat{ax+ny} = \hat{1} \iff \widehat{ax}+\widehat{ny} = \hat{1} \iff \widehat{ax}+\hat{0} = \hat{1} \Rightarrow \hat{a}$ is invertible, with $\hat{x}$ its inverse.

   $\mathbb{Z}_n$ is a field $\iff (a,n) = 1, \forall \hat{0} \neq \hat{a} \in \mathbb{Z}_n \iff n$ is a prime number.

6. We solve the first equation. Add to both sides $\hat{7}$ so we can get rid of $\hat{5}$. Hence, we get:

   $$\hat{4}x = \hat{4} \pmod{12}.$$

   Since $(4,12) = 4$, $\hat{4}$ is not invertible in $\mathbb{Z}_{12}$, hence we cannot simplify with it. We get by "trial and error" 4 solutions, namely: $\hat{1}$, $\hat{4}$, $\hat{7}$, $\widehat{10}$.

Now we solve the second equation. Now we get:

$$\hat{5}x = \hat{4} \pmod{12}.$$

Since $(5, 12) = 1$, $\hat{5}$ is invertible in $\mathbb{Z}_{12}$, and we have a unique solution. We have to multiply by the inverse of $\hat{5}$, so that in the left side we have only x. By simple computations, we get that the inverse of $\hat{5}$ is itself $\Rightarrow$ the second equation becomes $x = \hat{8} \pmod{12}$, which is the solution.

7. We want to have a system in only one variable, so we can get rid of x, by multiplying first equation by $\hat{4}$ and the second one by $\hat{3}$. We get the next equations:

$$\hat{4}y = \hat{8}(mod 12)$$

$$\hat{3}y = \hat{6}(mod 12)$$

We can add the first equation to the second one $\Rightarrow \hat{7}y = \hat{2} \pmod{12}$. By the same reasoning as in the previous exercise, we find the inverse of $\hat{7}$ which is itself and we multiply the last equation by $\hat{7} \Rightarrow y = \hat{2}$ (mod 12).

Now, the system becomes:

$$\hat{3}x + \hat{8} = \widehat{11}(mod 12)$$

$$\hat{4}x + \hat{6} = \widehat{10}(mod 12)$$

We add to the first equation $\hat{4}$ to get rid of the free term, and we add $\hat{6}$ to the second one. Using the same method as above, we find that $x = \hat{1} \pmod{12}$.

In both cases, $(7, 12) = 1$, which means that the solutions we've got are unique.

8. The trivial solution is $X = I_2$. Now, we take a matrix $X = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$. By computing the product, we get the equations: $a+2c = 1$ and $b+2d = 2$. So, the solutions are of the form $X = \begin{bmatrix} 1-2c & 2-2d \\ c & d \end{bmatrix}$, where $c, d \in \mathbb{C}$.

9. For M to be a stable subset of $M_2(\mathbb{Q})$, we need to prove that $\forall A, B \in M \Rightarrow A + B, A \cdot B \in M$.(Easy)

   Using the transfer of properties like associativity, commutativity, distributivity in stble subsets, we can easily see that $(M, +, \cdot)$ is a commutative ring, with identity element I_2. So, to be a field, we only have to prove that any non-zero matrix has an inverse. We know that a matrix is invertible $\iff$ the determinant is not 0. Take a matrix of the form $0 \neq A = \begin{bmatrix} a & b \\ 2b & a \end{bmatrix} \Rightarrow detA = a^2 - 2b^2$. In other words, A is invertible $\iff a^2 \neq 2b^2$. Consider $a^2 = 2b^2 \Rightarrow a = b\sqrt{2}$, but $a, b \in \mathbb{Q} \Rightarrow$, impossible. Hence $\Rightarrow a^2 \neq 2b^2$. So every non-zero matrix from M is invertible. In conclusion, $(M, +, \cdot)$ is a field.

10. As in exercise 9, we can immediately find that $(M, +, \cdot)$ is a commutative ring, with identity element I_2. A matrix $A = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ is invertible $\iff detA \neq 0 \iff a^2 + b^2 \neq 0$. If $a^2 + b^2 = 0$, then $a = b = 0$. Hence all non-zero matrices from M are invertible. In conclusion, $(M, +, \cdot)$ is a field.