Seminar 10

1. (a) $A \neq \emptyset$ as $0 = 0 \cdot i \in A$. Take $x, y \in A$. Then $x = ai$ and $y = bi$ for some $a, b \in \mathbb{R}$. It follows that $x - y = ai - bi = (a-b)i \in A$, as $a - b \in \mathbb{R}$. But $x \cdot y = ai \cdot bi = -ab \notin A$ (for $a, b \neq 0$) $\Rightarrow A$ is not a subring of $\mathbb{C}$.

   (b) $B \neq \emptyset$, as $0 = 0 + 0 \cdot \sqrt[3]{2} + 0 \cdot \sqrt[3]{4} \in B$. Take $x = a_1 + b_1\sqrt[3]{2} + c_1\sqrt[3]{4}$, $y = a_2 + b_2\sqrt[3]{2} + c_2\sqrt[3]{4} \in B$. It follows that $x - y = a_1 + b_1\sqrt[3]{2} + c_1\sqrt[3]{4} - (a_2 + b_2\sqrt[3]{2} + c_2\sqrt[3]{4}) = (a_1 - a_2) + (b_1 - b_2)\sqrt[3]{2} + (c_1 - c_2)\sqrt[3]{4} \in B$, as $a_1 - a_2, b_1 - b_2, c_1 - c_2 \in \mathbb{Q}$. Also, if we multiply these numbers, we get $x \cdot y = (a_1a_2 + 2b_1c_2) + (a_1b_2 + a_2b_1 + 2c_1c_2)\sqrt[3]{2} + (a_1c_2 + b_1b_2 + c_1a_2)\sqrt[3]{4}$, which is in B, as each parenthesis is a number in $\mathbb{Q}$. Hence, B is a subring of $\mathbb{C}$.

   (c) $C \neq \emptyset$, as $0 \in C$. Take $z_1 = a_1 + b_1i, z_2 = a_2 + b_2i \in C \Rightarrow |z_1| \leq 1,\ |z_2| \leq 1 \Rightarrow z_1 - z_2 = (a_1 - a_2) + (b_1 - b_2)i$. For this to be in C, its modulus has to be smaller or equal to 1 $\iff \mid z_1 - z_2 \mid = \sqrt{(a_1 - a_2)^2 + (b_1 - b_2)^2} \leq \sqrt{a_1^2 + b_1^2} + \sqrt{a_2^2 + b_2^2} + \sqrt{-2(a_1a_2 + b_1b_2)} \leq 1 + 1 + \sqrt{-2(a_1a_2 + b_1b_2)} \nleq 1$ in general. So C is not a subring of $\mathbb{C}$.

2. $\mathbb{Z}[i] \neq \emptyset$, as $0 \in \mathbb{Z}[i]$.Take $x = a_1 + b_1i, y = a_2 + b_2i \in \mathbb{Z}[i] \Rightarrow x - y = (a_1 - a_2) + (b_1 - b_2)i \in \mathbb{Z}[i]$ and $x \cdot y = (a_1 + b_1i)(a_2 + b_2i) = (a_1a_2 - b_1b_2) + (a_1b_2 + a_2b_1)i \in \mathbb{Z}[i] \Rightarrow \mathbb{Z}[i]$ is a subring of $\mathbb{C}$.

   An element $z \in \mathbb{Z}[i]$ is invertible if $\exists z^{-1} \in \mathbb{Z}[i]$ such that $z \cdot z^{-1} = 1$. Let $z = a + bi \Rightarrow z^{-1} = \frac{1}{a+bi} \iff z^{-1} = \frac{a-bi}{a^2+b^2} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2} \cdot i \in \mathbb{Z}[i]$ if $a^2 + b^2 \neq 0$. Hence $(a^2 + b^2)|a$ and $(a^2 + b^2)|b$, whence it follows that the invertible elements are 1, -1, i, $-i$.

   [Another way to prove it is to work with the function $f(z) = \mid z \mid$ and discuss the cases $\mid z \mid = 0$, $\mid z \mid = 1$ and $\mid z \mid \geq 2$.]

3. (a) The hardest part is to see if multiplication holds, i.e. $\forall A = \begin{bmatrix} a_1 & b_1 \\ 0 & c_1 \end{bmatrix}$ and $B = \begin{bmatrix} a_2 & b_2 \\ 0 & c_2 \end{bmatrix} \in A \Rightarrow A \cdot B = \begin{bmatrix} a_1a_2 & a_1b_2 + b_1c_2 \\ 0 & c_1c_2 \end{bmatrix}$ which is in A. Hence, A is a subring of $M_2(\mathbb{R})$.

   (b) Same as above. $A \cdot B = \begin{bmatrix} a_1a_2 & a_1a_2 + a_1b_2 \\ 0 & b_1b_2 \end{bmatrix}$, which is not in B, as $a_1a_2 \neq a_1a_2 + a_1b_2$ in general. Hence B is not a subring of $M_2(\mathbb{R})$.

(c) Same as (i) $\Rightarrow C$ is a subring of $M_2(\mathbb{R})$.

4. (a) $A \neq \emptyset$, as $f = X \in A$. Take $f = a_1X + a_2X^2 + \dots$ and $g = b_1X + b_2X^2 + \dots \in A \Rightarrow f - g = (a_1 - b_1)X + (a_2 - b_2)X^2 + \dots \in A$ and $f \cdot g = a_1b_1X^2 + (a_1b_2 + a_2b_1)X^3 + \dots \in A$. Hence A is a subring of $\mathbb{R}[X]$.

   (b) $B \neq \emptyset$, as $f = 1 \in B$. Take $f = 1 + a_1X + a_2X^2 + \dots$ and $g = 1 + b_1X + b_2X^2 + \dots \in B \Rightarrow f - g = (a_1 - b_1)X + (a_2 - b_2)X^2 + \dots \notin B$. Hence B is not a subring in $\mathbb{R}[X]$.

   (c) $C \neq \emptyset$, as $f = X^2 \in C$. Take $f = a_0 + a_2X^2 + \dots$ ad $g = b_0 + b_2X^2 + \dots \in C \Rightarrow f - g = (a_0 - b_0) + (a_2 - b_2)X^2 + \dots \in C$ and $f \cdot g = a_0b_0 + (a_0b_2 + a_2b_0)X^2 + \dots \in C$. Hence C is a subring of $\mathbb{R}[X]$.

5. (a) $2\mathbb{Z}$ is a subring without identity of the unitary ring $(\mathbb{Z}, +, \cdot)$.

   (b) $A = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \mid a \in \mathbb{R} \right\}$ is a subring with identity $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ of the ring $(M_2(\mathbb{R}), +, \cdot)$ with identiy I_2.

   (c) A good example is the non-commutative ring of matrices. But it is not always finite. So we need to take it over a finite field. For example: $(M_2(\mathbb{Z}_3), +, \cdot)$ is a ring.

6. $a = b = 0 \Rightarrow 0 \in \mathbb{Q}(\sqrt{2})$ and $a = 1$, $b = 0 \Rightarrow 1 \in \mathbb{Q}(\sqrt{2})$. So, $\mid \mathbb{Q}(\sqrt{2}) \mid \geq 2$. Take $x = a_1 + b_1\sqrt{2}$, $y = a_2 + b_2\sqrt{2} \in \mathbb{Q}(\sqrt{2}) \Rightarrow x - y = (a_1 - a_2) + (b_1 - b_2)\sqrt{2} \in \mathbb{Q}(\sqrt{2})$.

   Also, $(a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2}) = (a_1a_2 + 2b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{2} \in \mathbb{Q}(\sqrt{2})$.

   Now we assume that $y \neq 0$ and we show that $x \cdot y^{-1} \in \mathbb{Q}(\sqrt{2})$. By the above, it is enough to show that for every $z = a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$, $z^{-1} \in \mathbb{Q}(\sqrt{2})$.

   We have $z^{-1} = (a + b\sqrt{2})^{-1} = \frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{a^2-2b^2} = \frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ if $a^2 - 2b^2 \neq 0$. It happens if $a + b\sqrt{2} \neq 0$. If $a + b\sqrt{2} = 0 \Rightarrow a = b = 0 \Rightarrow a^2 - 2b^2 = 0$. If $a^2 - 2b^2 = 0$. Suppose $b \neq 0 \Rightarrow 2 = \frac{a^2}{b^2} \Rightarrow \sqrt{2} = \frac{a}{b} \in \mathbb{Q}$, which is impossible. $\Rightarrow a = b = 0 \Rightarrow \exists (a + b\sqrt{2})^{-1} \in \mathbb{Q}(\sqrt{2}) \Rightarrow \mathbb{Q}(\sqrt{2})$ subfield of $\mathbb{R}$.

7. $A \neq \emptyset$, as $0 \in A$. Take $a_1 + b_1\sqrt[3]{2}$, $a_2 + b_2\sqrt[3]{2} \in A \Rightarrow (a_1 - a_2) + (b_1 - b_2)\sqrt[3]{2} \in A$.

   Take $0 + \sqrt[3]{2} \in A \Rightarrow \sqrt[3]{2} \cdot \sqrt[3]{2} = \sqrt[3]{4}$. Suppose $\sqrt[3]{4} \in A \Rightarrow \exists a, b \in A$ such that $\sqrt[3]{4} = a + b\sqrt[3]{2}$. Multiply by $\sqrt[3]{2} \Rightarrow 2 = a\sqrt[3]{2} + b\sqrt[3]{4} \iff 2 = a\sqrt[3]{2} + b(a + b\sqrt[3]{2}) \iff 2 = ab + (a + b^2)\sqrt[3]{2}$. If $a + b^2 \neq 0 \Rightarrow \sqrt[3]{2} = \frac{2-ab}{a+b^2} \in \mathbb{Q}$ impossible $\Rightarrow a + b^2 = 0$ and $ab = 2 \iff a = -b^2$ and $ab = 2 \Rightarrow -b^3 = 2 \Rightarrow -b = \sqrt[3]{2}$ impossible $\Rightarrow \sqrt[3]{4} \notin A \Rightarrow A$ not a subring in $\mathbb{R}$.

8. First, we suppose that $n\mathbb{Z}$ is a subring of $m\mathbb{Z}$. We have $n\mathbb{Z} \subseteq m\mathbb{Z} \iff m|n$ by Exercise 5 from Seminar 3.

   Now, suppose that $m \mid n$. Then $n\mathbb{Z} \subseteq m\mathbb{Z}$. Clearly, $n\mathbb{Z} \neq \emptyset$. $\forall x, y \in n\mathbb{Z} \Rightarrow \exists x', y' \in \mathbb{Z}$ such that $x = nx', y = ny' \in n\mathbb{Z} \Rightarrow x - y = n(x' - y') \in n\mathbb{Z}$ and $xy = n(nx'y') \in n\mathbb{Z}$. Hence $n\mathbb{Z}$ is a subring of $m\mathbb{Z}$.

9. $Z(R) \neq \emptyset$, as the zero element of R commutes with any element. Now, $\forall a, b \in Z(R) \Rightarrow ar = ra$ and $br = rb, \forall r \in R \Rightarrow (a - b)r = ar - br = ra - rb = r(a - b)$, using that R is a ring. Also, $abr = arb = rab$. Hence, $a - b \in Z(R)$ and $ab \in Z(R)$, and so $Z(R)$ is a subring of $(R, +, \cdot)$. The equality holds $\iff$ R is a commutative ring $\iff$ all elements commute with respect to multiplication.

10. $Z(M_2(\mathbb{R}), +, \cdot) = \{A \in M_2(\mathbb{R}) \mid AB = BA, \forall B \in M_2(\mathbb{R})\}$. Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in Z(M_2(\mathbb{R}), +, \cdot)$. Since the equality $AB = BA$ happens for any B, let's consider the case for $B = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}$ and $B' = \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix}$.

$$AB = \begin{bmatrix} a & a \\ c & c \end{bmatrix} = BA = \begin{bmatrix} a + c & b + d \\ 0 & 0 \end{bmatrix}$$

   From here, we get that $c = 0$ and $a = b + d$.

$$AB' = \begin{bmatrix} b & b \\ d & d \end{bmatrix} = B'A = \begin{bmatrix} 0 & 0 \\ c + a & d + b \end{bmatrix}$$

   So, $b = 0$ and $a = d$. Hence: $A = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} = a \cdot I_2$. One easily checks that $a \cdot I_2 \in Z(M_2(\mathbb{R}), +, \cdot)$, $\forall a \in \mathbb{R}$.