Seminar 13

1. We have to prove that $\mathbb{Z}[X]/(n) \simeq \mathbb{Z}_n[X]$. By the first isomorphism theorem, we see that $\mathbb{Z}[X]$ is one of our rings, (n) is actually $ker(f)$, for a function f and $\mathbb{Z}_n[X]$ is the image of our function, or the second ring we need. From here, we deduce that our function is $f : \mathbb{Z}[X] \to \mathbb{Z}_n[X]$. As $ker(f) = (n) = \{0 \cdot n, 1 \cdot n, 2 \cdot n, \dots\}$ and also $ker(f) = \{a_0 + a_1X + \dots \mid f(a_0+a_1X+\dots) = \hat{0}\}$, we deduce that our function works like this: $\forall a \in \mathbb{Z}, f(a) = \hat{a}$ and $f(X) = X$. So, $f(a_0+a_1X+\dots) = \hat{a_0}+\hat{a_1}X+\dots$ and $ker(f) = \{n(a_0+a_1X+\dots) \mid a_0+a_1X+\dots \in \mathbb{Z}[X]\}$. This function that we found has to be an homomorphism, i.e.:

   (a) $f(a_0 + a_1X + \dots + b_0 + b_1X + \dots) = f(a_0 + b_0 + (a_1 + b_1)X + \dots) = \widehat{a_0 + b_0} + \widehat{a_1 + b_1}X + \dots = \hat{a_0} + \hat{b_0} + \hat{a_1}X + \hat{b_1}X + \dots = f(a_0 + a_1X + \dots) + f(b_0 + b_1X + \dots)$

   (b) $f((a_0 + a_1X + \dots) \cdot (b_0 + b_1X + \dots)) = f(a_0b_0 + (a_1b_0 + a_0b_1)X + \dots) = \widehat{a_0b_0} + (\widehat{a_1b_0 + a_0b_1})X + \dots = \hat{a_0}\hat{b_0} + (\hat{a_1}\hat{b_0} + \hat{a_0}\hat{b_1})X + \dots = f(a_0 + a_1X + \dots) \cdot f(b_0 + b_1X + \dots)$

   In the end, $ker(f)$ has to be an ideal of $\mathbb{Z}[X]$, i.e.:

   (a) $ker(f) \neq \emptyset$, which is true, as the polynomial $n \in ker(f)$.

   (b) $\forall n(a_0 + a_1X + \dots), n(b_0 + b_1X + \dots) \in ker(f) \Rightarrow n(a_0 + a_1X + \dots) - n(b_0 + b_1X + \dots) = n(a_0 - b_0 + (a_1 - b_1)X + \dots) \in ker(f)$.

   Hence, our isomorphism holds.

2. With the same reasoning as above, we take $f : \mathbb{Q}[X] \to \mathbb{Q}$. As $ker(f) = (X+1) = \{(X+1)(a_0+a_1X+\dots) \mid a_0+a_1X+\dots \in \mathbb{Q}[X]\}$, we find our function from the equation: $x + 1 = 0 \Rightarrow x = -1 \Rightarrow f(X) = -1$ and $f(a) = a, \forall a \in \mathbb{Q}$. One can easily prove that f is an homomorphism and $ker(f)$ is an ideal of $\mathbb{Q}[X]$.

3. The same way, we find $f : \mathbb{R}[X] \to \mathbb{C}$, where $ker(f) = \{(X^2 + 1)(a_0 + a_1X + \dots) \mid a_0 + a_1X + \dots \in \mathbb{R}[X]\}$. So, we get the expression of our function by solving the equation: $x^2 + 1 = 0 \Rightarrow x = \pm i$. One can take $f(X) = i$ and $f(a) = a, \forall a \in \mathbb{R}$. Also, one can easily prove that f is an homomorphism and $ker(f)$ is an ideal of $\mathbb{R}[X]$.

4. First, we have to prove that R is a subring of $M_2(\mathbb{Q})$.

   (a) $R \neq \emptyset$, true as $O_2 \in R$.

   (b) $\forall A = \begin{bmatrix} 0 & a_1 \\ 0 & a_2 \end{bmatrix}, B = \begin{bmatrix} 0 & b_1 \\ 0 & b_2 \end{bmatrix} \in R \Rightarrow A - B = \begin{bmatrix} 0 & a_1 - b_1 \\ 0 & a_2 - b_2 \end{bmatrix} \in R.$

   (c) $\forall A, B \in R$ (as above) $\Rightarrow A \cdot B = \begin{bmatrix} 0 & a_1 b_2 \\ 0 & a_2 b_2 \end{bmatrix} \in R.$

   Secondly, we have to prove that I is an ideal of R.

   (a) $I \neq \emptyset$, true as $O_2 \in I$.

   (b) $\forall A = \begin{bmatrix} 0 & a \\ 0 & 0 \end{bmatrix}, B = \begin{bmatrix} 0 & b \\ 0 & 0 \end{bmatrix} \in I \Rightarrow A - B = \begin{bmatrix} 0 & a - b \\ 0 & 0 \end{bmatrix}.$

   Now, to prove that R/I is isomorphic to $\mathbb{Q}$, we use the first isomorphism theorem. Take the function $f : R \to \mathbb{Q}$ with $f(\begin{bmatrix} 0 & a \\ 0 & b \end{bmatrix}) = b \in \mathbb{Q}$, as $ker(f) = I$, which we know it is an ideal of R. It is easy to see that f is an homomorphism, so, in the end, the isomorphism holds.

5. We know that the ideals of $\mathbb{Z}_{12}$ are $(\hat{1}), (\hat{2}), (\hat{3}), (\hat{4}), (\hat{6}), (\widehat{12})$. For the third isomorphism theorem, we need two ideals of our ring $\mathbb{Z}_{12}$, let's say U, V, with $U \subseteq V$. For our ideals, we know that: $(\widehat{12}) \subseteq (\hat{4}) \subseteq (\hat{2}) \subseteq (\hat{1})$ and $(\widehat{12}) \subseteq (\hat{6}) \subseteq (\hat{3}) \subseteq (\hat{1})$. The two relations that we get from the third isomorphism theorem are:

   (a) V/U ideal in R/U

   (b) $(R/U)/(V/U)$ isomorphic to R/V.

   For example, if we take $U = (\hat{4})$ and $V = (\hat{2}) \Rightarrow (\hat{2})/(\hat{4})$ is an ideal of $\mathbb{Z}_{12}/(\hat{4})$ and $(Z_{12}/(\hat{4}))/((\hat{2})/(\hat{4}))$ is isomorphic to $\mathbb{Z}_{12}/(\hat{2})$, which is a factor ring. So, in the end, all factor rings are $\mathbb{Z}_{12}/(\hat{1}), \mathbb{Z}_{12}/(\hat{2}), \mathbb{Z}_{12}/(\hat{3}), \mathbb{Z}_{12}/(\hat{4}), \mathbb{Z}_{12}/(\hat{6})$.

6. We know that $char(\mathbb{Z}_n) = n$ and $\mathbb{Z}_4 \times \mathbb{Z}_6 = \{(\bar{x}, \hat{x}) \mid \bar{x} \in \mathbb{Z}_4, \hat{x} \in \mathbb{Z}_6\}$. Then, the characteristic of $\mathbb{Z}_4 \times \mathbb{Z}_6$ is the smallest positive number n such that $n \cdot (\bar{1}, \hat{1}) = (\bar{0}, \hat{0})$. It is easy to see that $n = lcm[4, 6]$, i.e. the least common multiple of $char(\mathbb{Z}_4) = 4$ and $char(\mathbb{Z}_6) = 6$. So, $n = 12$. The same goes for $\mathbb{Z}_m \times \mathbb{Z}_n$.

7. (i) $(\mathbb{Z}_n[X], +, \cdot)$ is an infinite ring with $char(\mathbb{Z}) = n$.

   (ii) A simple example of a commutative ring with identity and prime characteristic is $\mathbb{Z}_p$, with p prime. But this is actually a field. So, in order to have a ring, take it over the polynomials, as $\mathbb{Z}_p[X]$.

8. $(a+b)^p = C_p^0 \cdot a^p \cdot b^0 + C_p^1 \cdot a^{p-1} \cdot b^1 + \cdots + C_p^p \cdot a^0 \cdot b^p$. We know that $C_p^k = \frac{p!}{k!(p-k)!}$ has to be an integer $\Rightarrow k!(p-k)! \mid p!$. But p is prime $\Rightarrow k!(p-k)! \nmid p \Rightarrow C_p^k = p \cdot q, q \in \mathbb{Z}$. As $char(R) = p \Rightarrow p \cdot q = p \cdot 1 \cdot q = 0 \cdot q = 0 \Rightarrow C_p^k = 0 \Rightarrow (a+b)^p = a^p + b^p$.