D-MATH | Algebra II | FS 2014
Prof. Brent Doran

Solutions 1

Quotient rings, adjoining elements and product rings

1. Consider the homomorphism $\mathbb{Z}[x] \to \mathbb{Z}$ for which $x \mapsto 1$. Explain in this case what the Correspondence Theorem says about ideals of $\mathbb{Z}[x]$.

   Solution : We are considering the evaluation homomorphism

   $$\mathbb{Z}[x] \to \mathbb{Z}, \quad f(x) \mapsto f(1).$$

   This homomorphism is obviously surjective (for any $n \in \mathbb{Z}$, take f to be the constant polynomial n). Division with remainder yields two polynomials $q(x), r(x)$ such that

   $$f(x) = q(x)(x-1) + r(x)$$

   and $\deg r(x) < \deg(x-1) = 1$, hence $r(x)$ is a constant integer and is given by $f(1) = r(1)$. In particular, the kernel of the evaluation homomorphism above consists of all polynomials $f(x) \in \mathbb{Z}[x]$ such that

   $$f(x) = q(x)(x-1),$$

   i.e. it is exactly the ideal $(x-1)$ in $\mathbb{Z}[x]$.

   The ideals of $\mathbb{Z}$ are of the form $(n) = n\mathbb{Z}$ for $n \in \mathbb{N}$ (see your notes from the lecture or Chapter 11.3 in Artin). We consider the inverse image of (n) under the evaluation homomorphism above. This is the set of all polynomials $f(x) \in \mathbb{Z}[x]$ such that

   $$f(x) - q(x)(x-1) \in (n)$$

   and thus contained in the ideal $(n, x-1)$. We can conclude with the Correspondence Theorem that the ideals of $\mathbb{Z}[x]$ containing the ideal $(x-1)$ are the ideals of the form $(n, x-1)$, for $n \in \mathbb{N}$. Moreover, we have isomorphisms

   $$\mathbb{Z}[x]/(n, x-1) \to \mathbb{Z}/(n).$$

2. (a) Let $\mathfrak{I} \subset \mathbb{Z}[x]$ be the ideal generated by $x-3$ and 7. Show that for every $f(x) \in \mathbb{Z}[x]$, there is an integer $0 \leqslant \alpha \leqslant 6$ such that $f(x) - \alpha \in \mathfrak{I}$. Conclude that the quotient ring $\mathbb{Z}[x]/\mathfrak{I}$ is isomorphic to $\mathbb{Z}/(7)$.

Solution : Division with remainder gives two polynomials $q(x)$, $r(x) \in \mathbb{Z}[x]$ satisfying $f(x) = q(x)(x-3) + r(x)$ and $\deg r(x) < \deg(x-3)$. We set $r_f := r(x) = f(3) \in \mathbb{Z}$. Under the quotient map $\mathbb{Z}[x] \to \mathbb{Z}[x]/\mathfrak{I}$, the polynomial $f(x)$ is then mapped onto

$$f(x) + \mathfrak{I} = \alpha + \mathfrak{I},$$

where $0 \leqslant \alpha \leqslant 6$ satisfies $r_f \equiv \alpha \bmod 7$.

Alternatively, we can replace the evaluation map in Exercise 1 by $f(x) \mapsto f(3)$ and repeat the Correspondance Theorem discussion here to conclude that $\mathbb{Z}[x]/\mathfrak{I}$ and $\mathbb{Z}/(7)$ are isomorphic.

(b) Find α explicitly for $f(x) = x^{250} + 15x^{14} + x^2 + 5$ (**Hint** : you may want to use here Fermat's Little Theorem, see e.g. `http://www.math.ethz.ch/education/bachelor/lectures/hs2013/math/algebra1/Exercise6.pdf`).

Solution : We must determine $f(3) \bmod 7$. Using Fermat's Little Theorem, we reduce the computation to

$$\begin{aligned} f(3) &= 3^{7 \cdot 35} 3^5 + 15 \cdot 3^{2 \cdot 7} + 3^2 + 5 \\ &\equiv 3^{35} 3^5 + 16 \cdot 3^2 + 5 \bmod 7 \\ &\equiv 3^4 + 16 \cdot 9 + 5 \equiv 6 \bmod 7. \end{aligned}$$

(c) Describe the ring obtained from $\mathbb{Z}/(12)$ by adjoining an inverse of 2.

Solution : Let α be an inverse of 2, that is, α satisfies $2\alpha - 1 = 0$. The ring we consider is $\mathbb{Z}_{12}[\alpha] = \mathbb{Z}_{12}[x]/(2x-1)$, and this is isomorphic as a ring to $\mathbb{Z}[x]/\mathfrak{I}$, where $\mathfrak{I}$ is the ideal generated by 12 and $2x-1$ (compare to (a) above or Exercise 1).

We show that $\mathfrak{I} = (3, x-2)$. The inclusion '$\subseteq$' is immediate since

$$2x - 1 = 2(x-2) + 3$$

and 12 is a multiple of 3. We deduce the converse inclusion from :

$$2x - 1 = 0 \implies 12x - 6 = 0 \text{ and together with } 12 = 0 \implies 6 = 0.$$

Going through the same procedure once again yields $3 = 0$. Finally, we can write

$$x - 2 = 4x - 3x - 2 = 2(2x-1).$$

Hence, $\mathbb{Z}_{12}[\alpha]$ is isomorphic to $\mathbb{Z}_3[x]/(x-2)$ and thus to $\mathbb{Z}_3$.

3. Let $R = K[t]$ be a polynomial ring over a field K and consider the ring $R' = R[x]/(tx - 1)$ obtained by adjoining an inverse of t to R. Prove that R' can be identified as the ring of **Laurent polynomials**.

   Solution : We define the ring of Laurent polynomials over a field K to be the set of all finite linear combinations of the form

   $$\sum_{k=-m}^{n} a_k t^k$$

   for $m, n \geqslant 0$ and $a_k \in K$. Addition and multiplication are defined as for polynomials.

   Let t^{-1} be a solution to the equation

   $$tx - 1 = 0,$$

   and then consider the evaluation homomorphism

   $$R[x] \to R[t^{-1}], \quad f(x) \mapsto f(t^{-1}).$$

   The usual arguments (see e.g. Exercise 1) allow us to show that this is a surjective map with kernel the ideal $(tx-1)$ and conclude with the first Isomorphism Theorem for rings that R' and $R[t^{-1}]$ are isomorphic. It is immediate that the elements of $R[t^{-1}]$ are exactly the Laurent polynomials described above.

   Recall moreover that $R[x]$ and $R[t^{-1}]$ are isomorphic to, respectively, $K[t, x]$ and $K[t, t^{-1}]$.

4. Let $\mathfrak{I}$ and $\mathfrak{J}$ be ideals of a ring R such that $\mathfrak{I} + \mathfrak{J} = R$. Prove :

   (a) $\mathfrak{I}\mathfrak{J} = \mathfrak{I} \cap \mathfrak{J}$.

   Solution : First, we note that $\mathfrak{I}\mathfrak{J} = \{\sum_{k=1}^{n} a_k b_k : n > 0, a_k \in \mathfrak{I}, b_k \in \mathfrak{J}\}$ is an ideal.

   The inclusion $\mathfrak{I}\mathfrak{J} \subseteq \mathfrak{I} \cap \mathfrak{J}$ the follows from the definition of ideals. For the converse implication, we use that $\mathfrak{I} + \mathfrak{J} = R$. In particular, we can find two elements $a \in \mathfrak{I}$ and $b \in \mathfrak{J}$ such that $a + b = 1$. Then for any element x in the ideal $\mathfrak{I} \cap \mathfrak{J}$,

   $$x = ax + bx \in \mathfrak{I}\mathfrak{J} + \mathfrak{I}\mathfrak{J} = \mathfrak{I}\mathfrak{J}.$$

   (b) (the **Chinese Remainder Theorem**) For any $a, b \in R$, there is an element $x \in R$ such that $x \equiv a \bmod \mathfrak{I}$ and $x \equiv b \bmod \mathfrak{J}$.

Solution : Let $u \in \mathfrak{I}$ and $v \in \mathfrak{J}$ be such that $u + v = 1$. Then

$$x := av + bu \in R$$

satisfies the Chinese Remainder Theorem. In fact, $x - a = (b - a)u \in \mathfrak{I}$ and $x - b = (a - b)v \in \mathfrak{J}$.

(c) If $\mathfrak{I}\mathfrak{J} = 0$, then R is isomorphic to the product ring $R/\mathfrak{I} \times R/\mathfrak{J}$.

Solution : Consider the map $R \to R/\mathfrak{I} \times R/\mathfrak{J}$ that sends each $x = a + b \in R = \mathfrak{I} + \mathfrak{J}$ to (b, a). This is a ring homomorphism with kernel $\mathfrak{I} \cap \mathfrak{J}$. We conclude with the first Isomomorphism Theorem for rings.

(d) Describe the idempotent elements corresponding to the above product decomposition.

Solution : Let $e \in \mathfrak{I}$ and $e' \in \mathfrak{J}$ be such that $e + e' = 1$. We show that these are idempotent elements that correspond to the product decomposition in (c).
In fact,

$$e^2 = e(1 - e') = e - ee'$$

and by assumption $ee' \in \mathfrak{I}\mathfrak{J} = 0$. Consider next the surjective homomorpshim $R \to (e)$ given by multiplication $r \mapsto er$, for every $r \in R$. By the mapping property of quotient rings, there exists then a ring homomorphism $R/\mathfrak{J} \to (e)$. It is easily seen that the multiplication map $R \to (e)$ is onto. Its kernel consists of all R-elements r such that

$$er = (1 - e')r = r - e'r = 0,$$

so that any element r in the kernel is in fact element of the ideal $\mathfrak{J}$, as $r = e'r \in \mathfrak{J}$. Conversely, we show that any element $a \in \mathfrak{J}$ is in that kernel, thus yielding an isomorphism between $R/\mathfrak{J}$ and (e). In fact, for any $a \in R$, $ea \in \mathfrak{I}\mathfrak{J} = 0$ by assumption, and we are done. Hence, in the setting of (c),

$$R = R/\mathfrak{I} \times R/\mathfrak{J} = (e') \times (e).$$

5. Andy, Esther and Nick are flatmates in a WOKO and want to have pizza all together one night. However, they all have their quirks : Andy eats pizza every fifth day, Esther every 7th and Nick every 11th. Given that in 2014, Nick and Andy had their first pizza together on January 3 and Esther had pizza on January 4, on what day(s) of 2014 will they all manage to have pizza together ?

Solution : Let's set x to count the number of days after January 3. We want to solve the congruence equation system

$$\begin{cases} x \equiv 0 \bmod 5 \\ x \equiv 1 \bmod 7 \\ x \equiv 0 \bmod 11. \end{cases}$$

As a straightforward application of the Chinese Remainder Theorem, this system reduces to

$$\begin{cases} x \equiv 0 \bmod 55 \\ x \equiv 1 \bmod 7. \end{cases}$$

Then, by inspection, the only possible solution is $x = 330$. Hence Andy, Esther and Nick will all have pizza on the 333$^{\text{rd}}$ day of 2014, Saturday, November 29.

Note that exercise 4 holds more generally for a finite family of ideals $\mathfrak{I}_1, \dots, \mathfrak{I}_n$ with the property that $\mathfrak{I}_k + \mathfrak{I}_l = R$ for any two distinct ideals (i.e. $k \neq l$). Then (a) translates to $\mathfrak{I}_1 \cdot \dots \cdot \mathfrak{I}_n = \mathfrak{I}_1 \cap \dots \cap \mathfrak{I}_n$ and (b)+(c) to the fact that $R/\mathfrak{I}_1 \cdot \dots \cdot \mathfrak{I}_n$ is isomorphic to the finite product $R/\mathfrak{I}_1 \times \dots \times R/\mathfrak{I}_n$.

6. Is $\mathbb{Z}/(6)$ isomorphic to $\mathbb{Z}/(2) \times \mathbb{Z}/(3)$? What about $\mathbb{Z}/(8)$ and $\mathbb{Z}/(2) \times \mathbb{Z}/(4)$?

   Solution : In the first case, $\mathbb{Z}/(6)$ is isomorphic to $\mathbb{Z}/(2) \times \mathbb{Z}/(3)$; this is a direct application of the Chinese Remainder Theorem. In the second case, the two rings are not isomorphic. In fact, the additive group $\mathbb{Z}_2 \times \mathbb{Z}_4$ has no element of order 8, and hence can not be isomorphic to the cyclic group $\mathbb{Z}_8$.

   This translates the more general fact that the 'coprimality condition' expressed by $\mathfrak{I} + \mathfrak{J} = R$ is necessary for the Chinese Remainder Theorem to hold.