Abstract Algebra
Day 28 Class Work Solutions

1. Consider the polynomials $f(x) = 3x^4 - 7x^2 + 4$ and $g(x) = 4x^2 + 1$ in $\mathbb{Z}[x]$.

   (a) Find the sum $f(x) + g(x)$ and the product $f(x) \cdot g(x)$.

   Solution. We have $f(x)+g(x) = 3x^4 - 3x^2 + 5$ and $f(x) \cdot g(x) = 12x^6 - 25x^4 + 9x^2 + 4$. See Example 28.1 in the textbook for descriptions of how to obtain these results.

   (b) Verify that the sum and product that you found are also in $\mathbb{Z}[x]$.

   Solution. As seen in part (a), the sum $f(x) + g(x)$ is a polynomial whose coefficients are in $\mathbb{Z}$. The same is true for the product $f(x) \cdot g(x)$. Thus, both are in $\mathbb{Z}[x]$.

   (c) Convince yourself that $\mathbb{Z}[x]$ is closed under addition and multiplication.

   ← No proof required.

2. (a) Verify that $\mathbb{Z}[x]$ is a *commutative* ring, focusing on the following questions. You can "skim" through the other ring properties.

   - What are the additive and multiplicative identities of $\mathbb{Z}[x]$?
   - What's the additive inverse of, say, $f(x) = 3x^4 - 7x^2 + 4$?
   - Do $f(x) + g(x) = g(x) + f(x)$ and $f(x) \cdot g(x) = g(x) \cdot f(x)$?

   Ans: Still 0 and 1, which are *constant* polynomials.

   Solution. The additive and multiplicative identities of $\mathbb{Z}[x]$ are the constant polynomials 0 and 1, respectively. Every polynomial in $\mathbb{Z}[x]$ has an additive inverse in $\mathbb{Z}[x]$. With $f(x) = 3x^4 - 7x^2 + 4$, for example, we have $-f(x) = -3x^4 + 7x^2 - 4$, where $f(x) + (-f(x)) = 0$ and $-f(x) + f(x) = 0$.

   Although we won't provide a rigorous proof, it turns out that $\mathbb{Z}[x]$ is a ring. In fact, it's a *commutative* ring, since $\alpha(x) \cdot \beta(x) = \beta(x) \cdot \alpha(x)$ for all $\alpha(x)$, $\beta(x) \in \mathbb{Z}[x]$. As an exercise, try computing $g(x) \cdot f(x)$ using the polynomials in Problem #1 above and compare the product to $f(x) \cdot g(x)$.

   (b) Anita says, "$\mathbb{Z}$ is a subring of $\mathbb{Z}[x]$." Do you agree or disagree with her? Explain.

   Solution. Agree. The ring of integers $\mathbb{Z}$ is a subring of $\mathbb{Z}[x]$. Here, we're viewing the elements of $\mathbb{Z}$ (such as 0, 1, -3, and 6) as constant polynomials.

   (c) Explain why x does *not* have a multiplicative inverse in $\mathbb{Z}[x]$.

   Solution. There is no polynomial $q(x)$ such that $x \cdot q(x) = 1$. While it's true that $x \cdot \frac{1}{x} = 1$, we note that $\frac{1}{x}$ is *not* a polynomial. Therefore, x^{-1} does not exist in $\mathbb{Z}[x]$. (For a more rigorous argument, see Theorem 28.12 and its proof in the textbook.)

   (d) Elizabeth says, "$\mathbb{Z}[x]$ is *not* a field, and neither is $\mathbb{R}[x]$." What do you think?

   Recall: In a *field*, every nonzero element is a unit.

   Solution. Agree. The nonzero polynomial $x \in \mathbb{Z}[x]$ is *not* a unit, i.e., it doesn't have a multiplicative inverse, as shown in part (c). Thus, $\mathbb{Z}[x]$ is *not* a field. The same argument shows that $\mathbb{R}[x]$ is not a field either.

3. Consider the polynomials $f(x) = 3x^{15} + 4x^3 + 2$ and $g(x) = 6x^8 + 5x + 3$.

   (a) In $\mathbb{Z}[x]$, compute the degrees of $f(x)$, $g(x)$, and $f(x) \cdot g(x)$. How are they related?

   ← You don't actually have to compute $f(x) \cdot g(x)$.

   Solution. In $\mathbb{Z}[x]$, we have $\deg f(x) = 15$ and $\deg g(x) = 8$. Moreover,

$$\begin{aligned} f(x) \cdot g(x) &= (3x^{15})(6x^8) + \text{(lower degree terms)} \\ &= (3 \cdot 6)x^{15+8} + \text{(lower degree terms)} \\ &= 18x^{23} + \text{(lower degree terms)} \end{aligned}$$

   so that the degree of $f(x) \cdot g(x)$ is 23, which is the sum of 15 and 8.

(b) Same question, but in $\mathbb{Z}_7[x]$.

Solution. In $\mathbb{Z}_7[x]$, we have the same results as in $\mathbb{Z}[x]$. The only difference is that the highest degree term of $f(x) \cdot g(x)$ is $4x^{23}$ instead of $18x^{23}$, because $18 = 4$ in $\mathbb{Z}_7$.

(c) Same question, but in $\mathbb{Z}_9[x]$.

Ans to (c): $\deg f(x) \cdot g(x) = 16$.

Solution. In $\mathbb{Z}_9[x]$, we still have $\deg f(x) = 15$ and $\deg g(x) = 8$. But

$$\begin{aligned} f(x) \cdot g(x) &= (\mathbf{3}x^{15} + 4x^3 + 2)(\mathbf{6}x^8 + 5x + 3) \\ &= \mathbf{18}x^{23} + 15x^{16} + \text{(lower degree terms)} \\ &= \mathbf{0}x^{23} + 15x^{16} + \text{(lower degree terms)} \\ &= 15x^{16} + \text{(lower degree terms)} \end{aligned}$$

so that the degree of $f(x) \cdot g(x)$ is 16. This occurs, because 3 and 6 are zero divisors in $\mathbb{Z}_9$. Since $3 \cdot 6 = 0$ in $\mathbb{Z}_9$, the leading term $f(x) \cdot g(x)$ vanishes when its coefficient is reduced modulo 9.

(d) What's going on here? Can you *justify* it?

Solution. See Problem #4.

4. Consider the following theorem:

Theorem. Let $f(x)$, $g(x) \in R[x]$ where R is an integral domain, with $f(x)$, $g(x) \neq 0$. Then $\deg f(x) \cdot g(x) = \deg f(x) + \deg g(x)$.

Recall: An *integral domain* doesn't contain zero divisors.

(a) Give an example that illustrates the theorem.

Hint: See Problem #3.

Solution. See Problem #3, parts (a) and (b).

(b) Explain why the theorem is true. In particular, why must R be an integral domain?

Proof. Suppose $f(x)$ and $g(x)$ have degrees m and n, respectively. Then

$$f(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0 \quad \text{and} \quad g(x) = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0,$$

where the coefficients a_i and b_i are in R, and a_m, $b_n \neq 0$. Then,

$$\begin{aligned} f(x) \cdot g(x) &= (a_m x^m)(b_n x^n) + \text{(lower degree terms)} \\ &= a_m b_n x^{m+n} + \text{(lower degree terms)}. \end{aligned}$$

Since R is an integral domain and a_m, $b_n \neq 0$, we have $a_m b_n \neq 0$ as well. Thus, $\deg f(x) \cdot g(x) = m + n$, which equals $\deg f(x) + \deg g(x)$ as desired. ■

5. (a) Find all units in $\mathbb{Z}_7[x]$, i.e., $f(x)$, $g(x) \in \mathbb{Z}_7[x]$ such that $f(x) \cdot g(x) = 1$.

Ans: 1, 2, 3, 4, 5, 6.

Solution. The only units in $\mathbb{Z}_7[x]$ are 1, 2, 3, 4, 5, 6, where we view these as constant polynomials. Note that these are precisely the units of the coefficient ring $\mathbb{Z}_7$.

(b) Find all units in $\mathbb{Z}[x]$; in $\mathbb{R}[x]$.

Solution. The only units in $\mathbb{Z}[x]$ are 1 and -1; again, these are units of $\mathbb{Z}$. The only units in $\mathbb{R}[x]$ are the nonzero real numbers, i.e., the units of $\mathbb{R}$.

(c) **Prove:** If R is an integral domain, then the only units in $R[x]$ are the units of R.

← Thus, non-constant polynomials are *not* units.

Hint: Suppose $f(x) \cdot g(x) = 1$. Then $\deg f(x)$ and $\deg g(x)$ must be...

PROOF. Suppose $f(x) \in R[x]$ is a unit. We will show that $f(x)$ is a constant polynomial so that it is an element of R. Since $f(x)$ is a unit, there exists $g(x) \in R[x]$ such that $f(x) \cdot g(x) = 1$. Thus,

$$\deg f(x) + \deg g(x) = \deg f(x) \cdot g(x) = \deg(1) = 0.$$

Since $\deg f(x)$ and $\deg g(x)$ are non-negative integers whose sum is 0, they must both be 0. This implies that $f(x)$ is a constant polynomial, as desired. ■

6. (a) Find all zero divisors in $\mathbb{Z}_7[x]$; in $\mathbb{Z}[x]$; in $\mathbb{R}[x]$. ← Are there any?

   Solution. $\mathbb{Z}_7[x]$, $\mathbb{Z}[x]$, and $\mathbb{R}[x]$ have no zero divisors. For instance, we cannot find a pair of nonzero polynomials $f(x)$, $g(x) \in \mathbb{Z}_7[x]$ such that $f(x) \cdot g(x) = 0$.

   (b) **Prove:** If R is an integral domain, then $R[x]$ is an integral domain.

   Hint: Let $f(x)$, $g(x) \in R[x]$ be nonzero. Why must $f(x) \cdot g(x)$ also be nonzero?

   Solution. The proof in Problem #4(b) shows that the product of two nonzero polynomials in $R[x]$ is also nonzero. This confirms that $R[x]$ is an integral domain.

7. Our friends are discussing the degree of the constant 0.

   Anita: "Why can't we say $\deg(0) = 0$? The zero polynomial is a constant, right?"

   Elizabeth: "But the theorem from Problem #4 fails if $\deg(0) = 0$."

   Hint: We have $x^2 \cdot 0 = 0$. Take the degree of both sides.

   What might Elizabeth mean?

8. (a) In $\mathbb{Z}_9[x]$, find $f(x)$ such that $(1 + 3x) \cdot f(x) = 1$.

   Solution. We have

$$(1 + 3x) \cdot (1 + 6x) = 1 = 9x + 18x^2 = 1 + 0x + 0x^2 = 1,$$

   where we reduced the coefficients 9 and 18 in $\mathbb{Z}_9$. Thus, $f(x) = 1 + 6x$.

   (b) In $\mathbb{Z}_6[x]$, find a nonzero $f(x)$ such that $(2 + 4x) \cdot f(x) = 0$.

   Solution. We have

$$(2 + 4x) \cdot 3x = 6x + 12x^2 = 0,$$

   so that $2 + 4x$ and $3x$ are zero divisors in $\mathbb{Z}_6[x]$.

   (c) How are $\mathbb{Z}_9[x]$ and $\mathbb{Z}_6[x]$ different from $\mathbb{Z}_7[x]$, $\mathbb{Z}[x]$, and $\mathbb{R}[x]$? Explain.

   Solution. $\mathbb{Z}_9[x]$ has a unit that is *not* a constant polynomial. $\mathbb{Z}_6[x]$ has zero divisors. Neither of these is possible in $\mathbb{Z}_7[x]$, $\mathbb{Z}[x]$, and $\mathbb{R}[x]$

9. **(Some Food for Thought)**

   (a) Find *all* units in $\mathbb{Z}_9[x]$.

   (b) Find *all* zero divisors in $\mathbb{Z}_6[x]$.

10. **(More Food for Thought)**

   (a) In $\mathbb{Z}_9[x]$, find $f(x)$ such that $(1 - 3x) \cdot f(x) = 1$.

   (b) Same question, but in $\mathbb{Z}_{27}[x]$; in $\mathbb{Z}_{81}[x]$; in $\mathbb{Z}_{3^n}[x]$.