Abstract Algebra
Day 35 Class Work Solutions

1. Consider the element $8 \in \mathbb{Z}_{29}$. Since 8 and 29 are relatively prime, the GCD theorem says there exist x, $y \in \mathbb{Z}$ such that $8x + 29y = 1$. ← i.e., $\gcd(8, 29) = 1$.

   (a) Find integers x and y such that $8x + 29y = 1$. **Hint:** $88 + (-87) = 1$.

   Solution. Answer will vary. A possible solution is $x = 11$ and $y = -3$, since

   $$8 \cdot 11 + 29 \cdot (-3) = 88 + (-87) = 1.$$

   (b) Using your answer in part (a), find the multiplicative inverse of 8 in $\mathbb{Z}_{29}$.

   Solution. We have $8 \cdot 11 + 29 \cdot (-3) = 1 \implies 8 \cdot 11 - 1 = 29 \cdot 3 \implies 29 \mid (8 \cdot 11 - 1)$. Then $8 \cdot 11 = 1$ in $\mathbb{Z}_{29}$, so that 11 is the multiplicative inverse of 8 in $\mathbb{Z}_{29}$.

2. Consider the element $8 + \langle 29 \rangle$ in the quotient ring $\mathbb{Z}/\langle 29 \rangle$.

   (a) Using your result in Problem #1(a), complete the following:

   $$(8 + \langle 29 \rangle) \cdot (\_\_ + \langle 29 \rangle) = 8 \cdot \_\_ + \langle 29 \rangle = 1 + \langle 29 \rangle, \text{ because } \_\_\_\_\_ \in \langle 29 \rangle.$$ **Ans:** $8 \cdot 11 - 1 \in \langle 29 \rangle$.

   Recall: In $\mathbb{Z}/\langle 29 \rangle$, $\alpha + \langle 29 \rangle = \beta + \langle 29 \rangle$ if and only if...

   Solution. We have $(8 + \langle 29 \rangle) \cdot (11 + \langle 29 \rangle) = 8 \cdot 11 + \langle 29 \rangle$. Also, $8 \cdot 11 + \langle 29 \rangle = 1 + \langle 29 \rangle$, because $8 \cdot 11 - 1 = 29 \cdot 3 \in \langle 29 \rangle$. Thus, $(8 + \langle 29 \rangle) \cdot (11 + \langle 29 \rangle) = 1 + \langle 29 \rangle$.

   (b) Let $a + \langle 29 \rangle$ be a *nonzero* element of $\mathbb{Z}/\langle 29 \rangle$, so that $a \notin \langle 29 \rangle$. Explain why a and 29 are relatively prime, so that there exist x, $y \in \mathbb{Z}$ such that $ax + 29y = 1$. ← $a \notin \langle 29 \rangle$ means a is *not* a multiple of 29.

   Solution. Since $a \notin \langle 29 \rangle$, the integer a is *not* a multiple of 29. As 29 is prime, we have $\gcd(a, 29) = 1$. By the GCD theorem, there exist x, $y \in \mathbb{Z}$ such that $ax + 29y = 1$.

   (c) Using your result in part (b), complete the following:

   $$(a + \langle 29 \rangle) \cdot (\_\_ + \langle 29 \rangle) = a \cdot \_\_ + \langle 29 \rangle = 1 + \langle 29 \rangle, \text{ because } \_\_\_\_\_ \in \langle 29 \rangle.$$ **Ans:** $a \cdot x - 1 \in \langle 29 \rangle$.

   Solution.

   $$(a + \langle 29 \rangle) \cdot (x + \langle 29 \rangle) = ax + \langle 29 \rangle = 1 + \langle 29 \rangle, \text{ because } ax - 1 = 29 \cdot (-y) \in \langle 29 \rangle.$$

   (d) Anita says, "In (b) and (c), we proved that $\mathbb{Z}/\langle 29 \rangle$ is a field." What might she mean?

   Solution. We showed that any non-zero element $a + \langle 29 \rangle$ in $\mathbb{Z}/\langle 29 \rangle$ is a unit, i.e., it has a multiplicative inverse, namely $x + \langle 29 \rangle$.

   (e) Elizabeth wonders, "But how did we use the fact that 29 is prime?"

   Solution. In part (b), 29 being prime allowed us to conclude that $\gcd(a, 29) = 1$.

Here is the GCD theorem *for polynomials*.

> Let $f(x)$, $g(x) \in F[x]$. If $f(x)$ and $g(x)$ are relatively prime, then there exist $p(x)$, $q(x) \in F[x]$ such that $f(x) \cdot p(x) + g(x) \cdot q(x) = 1$.

Note: $f(x)$ and $g(x)$ are *relatively prime* if they don't share a non-constant common factor.

---

3. Fix $g(x) = x^2 + 1 \in \mathbb{Z}_7[x]$.

   (a) Compute $g(0)$, $g(1)$, $g(2)$, …, $g(6)$ in $\mathbb{Z}_7$.

   Solution. $g(0) = 1,\ g(1) = 2,\ g(2) = 5,\ g(3) = 3,\ g(4) = 3,\ g(5) = 5,\ g(6) = 2.$

   (b) Using your work in part (a), explain why $g(x)$ is unfactorable in $\mathbb{Z}_7[x]$.

   Solution. Part (a) shows that $g(x)$ has no root in $\mathbb{Z}_7$. Then, since $\deg g(x) = 2$, Theorem 30.19 implies that $g(x)$ is unfactorable in $\mathbb{Z}_7[x]$.

   (c) Based on our conjectures thus far, is $\mathbb{Z}_7[x]/\langle g(x)\rangle$ a field? ← It should be!

   Solution. Yes, because $g(x)$ is unfactorable in $\mathbb{Z}_7[x]$.

4. Let $f(x) = 3x + 5$ and $g(x) = x^2 + 1$ in $\mathbb{Z}_7[x]$.

   (a) Explain why $f(x)$ and $g(x)$ are relatively prime. Problem #3 should help. ← i.e., $g(x)$ is unfactorable.

   Solution. In Problem #3, we saw that $g(x)$ is unfactorable in $\mathbb{Z}_7[x]$. Also, $f(x)$ is *not* a multiple of $g(x)$, because $\deg f(x) < \deg g(x)$. Therefore, $f(x)$ and $g(x)$ are relatively prime.

   (b) By the GCD theorem, let $p(x)$, $q(x) \in \mathbb{Z}_7[x]$ such that $f(x) \cdot p(x) + g(x) \cdot q(x) = 1$. Explain why $(f(x) + \langle g(x)\rangle) \cdot (p(x) + \langle g(x)\rangle) = 1 + \langle g(x)\rangle$ in $\mathbb{Z}_7[x]/\langle g(x)\rangle$.

   Note: In other words, $f(x) + \langle g(x)\rangle$ has a multiplicative inverse $p(x) + \langle g(x)\rangle$.

   Solution. We have $(f(x) + \langle g(x)\rangle) \cdot (p(x) + \langle g(x)\rangle) = f(x) \cdot p(x) + \langle g(x)\rangle$. Moreover, $f(x) \cdot p(x) + \langle g(x)\rangle = 1 + \langle g(x)\rangle$, since $f(x) \cdot p(x) - 1 = g(x) \cdot (-q(x)) \in \langle g(x)\rangle$. Thus, $(f(x) + \langle g(x)\rangle) \cdot (p(x) + \langle g(x)\rangle) = 1 + \langle g(x)\rangle$, as desired.

5. **Prove:** Fix $g(x) \in F[x]$. If $g(x)$ is unfactorable, then $F[x]/\langle g(x)\rangle$ is a field. ← Here, F is a field.

   Hint: Let $\alpha(x) \in F[x]$ such that $\alpha(x) + \langle g(x)\rangle \neq 0 + \langle g(x)\rangle$. Then…

   - Explain why $\alpha(x)$ and $g(x)$ are relatively prime.
   - Show that $\alpha(x) + \langle g(x)\rangle$ has a multiplicative inverse.

   Solution. See Theorem 35.1(b) and its proof in Section 35.3 of the textbook.

6. (a) Once again, let $g(x) = x^2 + 1 \in \mathbb{Z}_7[x]$. How many elements does $\mathbb{Z}_7[x]/\langle g(x)\rangle$ contain? **Ans:** 49 elements.

   Solution. $\mathbb{Z}_7[x]/\langle g(x)\rangle = \{(ax + b) + \langle g(x)\rangle \mid a, b \in \mathbb{Z}_7\}$, which has $7^2 = 49$ distinct elements (i.e., 7 choices for each of a and b).

   (b) Find a prime p and a polynomial $g(x) \in \mathbb{Z}_p[x]$ such that the quotient ring $\mathbb{Z}_p[x]/\langle g(x)\rangle$ is a field containing 121 elements. Explain your reasoning.

   Solution. Let $g(x) = x^2 + 1 \in \mathbb{Z}_{11}[x]$. We can verify that $g(\alpha) \neq 0$ for all $\alpha \in \mathbb{Z}_{11}$. Thus, $g(x)$ has no root in $\mathbb{Z}_{11}$; and since $\deg g(x) = 2$, we conclude that $g(x)$ is unfactorable in $\mathbb{Z}_{11}[x]$. We have

   $$\mathbb{Z}_{11}[x]/\langle g(x)\rangle = \{(ax + b) + \langle g(x)\rangle \mid a, b \in \mathbb{Z}_{11}\}.$$

   With 11 choices for each of a and b, this quotient ring contains $11^2 = 121$ elements. And as $g(x)$ is unfactorable, we deduce that $\mathbb{Z}_{11}[x]/\langle g(x)\rangle$ is a field.

(c) Same as part (b), but with 343 elements. **Ans:** $x^3 + 2 \in \mathbb{Z}_7[x]$.

Solution. Let $g(x) = x^3 + 2 \in \mathbb{Z}_7[x]$. We can verify that $g(x)$ has no root in $\mathbb{Z}_7$ and hence is unfactorable in $\mathbb{Z}_7[x]$. We have

$$\mathbb{Z}_7[x]/\langle g(x)\rangle = \{(ax^2 + bx + c) + \langle g(x)\rangle \mid a,\, b,\, c \in \mathbb{Z}_7\}.$$

With 7 choices for each of a, b, and c, this quotient ring contains $7^3 = 343$ elements. And as $g(x)$ is unfactorable, we deduce that $\mathbb{Z}_7[x]/\langle g(x)\rangle$ is a field.

7. As in Problem #4, let $f(x) = 3x + 5$ and $g(x) = x^2 + 1$ in $\mathbb{Z}_7[x]$.

(a) Find $p(x)$, $q(x) \in \mathbb{Z}_7[x]$ such that $f(x) \cdot p(x) + g(x) \cdot q(x) = 1$.

Hint: Use polynomials $p(x)$ and $q(x)$ such that $\deg p(x) = 1$ and $\deg q(x) = 0$.

(b) Find the multiplicative inverse of $(3x + 5) + \langle x^2 + 1\rangle$ in $\mathbb{Z}_7[x]/\langle x^2 + 1\rangle$. ← You already found it!

8. Consider the quotient ring $\mathbb{Q}[x]/\langle x^2 - 2\rangle$.

(a) Explain why $\mathbb{Q}[x]/\langle x^2 - 2\rangle$ is a field.

Solution. Let $g(x) = x^2 - 2$. Note that $\deg g(x) = 2$ and $g(x)$ has no root in $\mathbb{Q}$. Thus, $g(x)$ is unfactorable in $\mathbb{Q}[x]$ and so $\mathbb{Q}[x]/\langle x^2 - 2\rangle$ is a field.

(b) Find the multiplicative inverse of $(7x + 4) + \langle x^2 - 2\rangle$ in $\mathbb{Q}[x]/\langle x^2 - 2\rangle$.

Hint: Observe that $x^2 + \langle x^2 - 2\rangle = \boxed{?} + \langle x^2 - 2\rangle$ in $\mathbb{Q}[x]/\langle x^2 - 2\rangle$.

Solution. Note that $x^2 + \langle x^2 - 2\rangle = 2 + \langle x^2 - 2\rangle$, since $x^2 - 2 \in \langle x^2 - 2\rangle$. Thus, *as coset representatives*, we can treat x^2 and 2 to be the same. We'll seek $(ax + b) + \langle x^2 - 2\rangle$ such that

$$((7x + 4) + \langle x^2 - 2\rangle) \cdot ((ax + b) + \langle x^2 - 2\rangle) = 1 + \langle x^2 - 2\rangle.$$

Expanding the left side gives

$$\begin{aligned}(7x + 4) \cdot (ax + b) + \langle x^2 - 2\rangle &= (7a \cdot x^2 + (4a + 7b)x + 4b) + \langle x^2 - 2\rangle \\ &= (7a \cdot 2 + (4a + 7b)x + 4b) + \langle x^2 - 2\rangle \\ &= ((4a + 7b)x + (14a + 4b)) + \langle x^2 - 2\rangle\end{aligned}$$

Setting this equal to $1 + \langle x^2 - 2\rangle$ implies $4a + 7b = 0$ and $14a + 4b = 0$. Solving this system of equations in $\mathbb{Q}$, we obtain $a = 7/82$ and $b = -2/41$, so that

$$((7x + 4) + \langle x^2 - 2\rangle)^{-1} = (\tfrac{7}{82}x - \tfrac{2}{41}) + \langle x^2 - 2\rangle.$$

9. **(Some Food for Thought)** Let $f(x) = x^2 + 1$.

(a) Explain why $f(x)$ is unfactorable in $\mathbb{Z}_3[x]$.

(b) Explain why $f(x)$ is factorable in $\mathbb{Z}_5[x]$.

(c) Explain why $f(x)$ is unfactorable in $\mathbb{Z}_7[x]$.

(d) Explain why $f(x)$ is unfactorable in $\mathbb{Z}_{11}[x]$.

(e) Explain why $f(x)$ is factorable in $\mathbb{Z}_{13}[x]$.

(f) Determine if $f(x)$ is factorable or unfactorable in $\mathbb{Z}_{17}[x]$, $\mathbb{Z}_{19}[x]$, $\mathbb{Z}_{23}[x]$, and $\mathbb{Z}_{29}[x]$.

(g) For which primes p is $f(x)$ factorable in $\mathbb{Z}_p[x]$? unfactorable in $\mathbb{Z}_p[x]$?