# Abstract Algebra
## Day 32 Class Work Solutions

For the problems below, fix $x^2 \in \mathbb{Z}_3[x]$ and define $\langle x^2 \rangle = \{x^2 \cdot q(x) \mid q(x) \in \mathbb{Z}_3[x]\}$. ← i.e., $\langle x^2 \rangle$ is the principal ideal generated by $x^2$.

1. (a) Explain why $2x^7 + x^5 + 2x^4$ is contained in $\langle x^2 \rangle$.

   **Solution.** We have $2x^7 + x^5 + 2x^4 = x^2 \cdot (2x^5 + x^3 + 2x^2)$, i.e., $2x^7 + x^5 + 2x^4$ is a multiple of $x^2$.

   (b) Explain why $x^6 + 2x$ is *not* contained in $\langle x^2 \rangle$.

   **Solution.** $x^2$ is not a factor of $x^6 + 2x$. In other words, there is no $q(x) \in \mathbb{Z}_3[x]$ such that $x^6 + 2x = x^2 \cdot q(x)$.

   (c) List three more elements of $\mathbb{Z}_3[x]$ that are contained in $\langle x^2 \rangle$.

   **Solution.** Answers will vary. Examples include $x^5 + 2x^4 + x^2$ and $2x^{10} + x^8 + x^5 + x^3$.

   (d) List three more elements of $\mathbb{Z}_3[x]$ that are *not* contained in $\langle x^2 \rangle$.

   **Solution.** Answers will vary. Examples include $x^5 + 2x^4 + 1$ and $2x^{10} + x^8 + x^5 + x$.

2. Let $\alpha(x), \beta(x) \in \mathbb{Z}_3[x]$ where $\alpha(x) = 2x^7 + x^5 + 2x^4 + \mathbf{2x + 1}$ and $\beta(x) = 2x + 1$. Explain why the cosets $\alpha(x) + \langle x^2 \rangle$ and $\beta(x) + \langle x^2 \rangle$ are equal, i.e., $\alpha(x) + \langle x^2 \rangle = \beta(x) + \langle x^2 \rangle$.

   **Hint:** In $\mathbb{Z}/5\mathbb{Z}$, $a + 5\mathbb{Z} = b + 5\mathbb{Z}$ if and only if... (What about in $\mathbb{Z}_3[x]/\langle x^2 \rangle$ ?)

   **Solution.** We have $\alpha(x) - \beta(x) = 2x^7 + x^5 + 2x^4 \in \langle x^2 \rangle$. Thus, $\alpha(x) + \langle x^2 \rangle = \beta(x) + \langle x^2 \rangle$.

3. (a) Let $f(x) = x^5 + 2x^2 + x + 2 \in \mathbb{Z}_3[x]$. Find $g(x) \in \mathbb{Z}_3[x]$ of smallest degree such that ← $\deg g(x) = 1$.

   $$f(x) + \langle x^2 \rangle = g(x) + \langle x^2 \rangle.$$

   **Solution.** Let $g(x) = x + 2$. Then, $f(x) - g(x) = x^5 + 2x^2 \in \langle x^2 \rangle$, which implies that $f(x) + \langle x^2 \rangle = g(x) + \langle x^2 \rangle$.

   (b) Repeat part (a), this time with $f(x) = 2x^9 + x^6 + 2x^3 + 1 \in \mathbb{Z}_3[x]$.

   **Solution.** Let $g(x) = 1$. Then $f(x) - g(x) = 2x^9 + x^6 + 2x^3 \in \langle x^2 \rangle$, which implies that $f(x) + \langle x^2 \rangle = g(x) + \langle x^2 \rangle$.

4. (a) Find all distinct elements of $\mathbb{Z}_3[x]/\langle x^2 \rangle$, i.e., distinct cosets of $\langle x^2 \rangle$ in $\mathbb{Z}_3[x]$. ← There are 9 cosets.

   **Solution.** The distinct elements of $\mathbb{Z}_3[x]/\langle x^2 \rangle$ are $(ax + b) + \langle x^2 \rangle$, where $a, b \in \mathbb{Z}_3$. More specifically, we have

   $$\begin{aligned}\mathbb{Z}_3[x]/\langle x^2 \rangle = \{&0 + \langle x^2 \rangle,\ 1 + \langle x^2 \rangle,\ 2 + \langle x^2 \rangle,\\ &x + \langle x^2 \rangle,\ (x+1) + \langle x^2 \rangle,\ (x+2) + \langle x^2 \rangle,\\ &2x + \langle x^2 \rangle,\ (2x+1) + \langle x^2 \rangle,\ (2x+2) + \langle x^2 \rangle\}\end{aligned}$$

   (b) Find the additive identity and the multiplicative identity of $\mathbb{Z}_3[x]/\langle x^2 \rangle$.

   **Solution.** They are $0 + \langle x^2 \rangle$ and $1 + \langle x^2 \rangle$, respectively.

   (c) Elizabeth says: "I found 9 cosets of the form $(ax + b) + \langle x^2 \rangle$. But how do I know for sure that they're all distinct? Why can't, for instance, $(2x+1) + \langle x^2 \rangle = (x+2) + \langle x^2 \rangle$ ?" How would you respond to Elizabeth?

   **Solution.** Suppose for contradiction that

   $$(2x + 1) + \langle x^2 \rangle = (x + 2) + \langle x^2 \rangle.$$

   Then we'd have $(2x + 1) - (x + 2) \in \langle x^2 \rangle$, i.e., $x - 1 \in \langle x^2 \rangle$. This implies $x - 1$ is a multiple of $x^2$, which is a contradiction. Similar argument can be used to show that any pair of the 9 cosets above are, in fact, distinct.

5. (a) Compute $((x+1)+\langle x^2\rangle)\cdot((2x+1)+\langle x^2\rangle)$ and verify that the product equals $1+\langle x^2\rangle$.

**Solution.**

$$\begin{aligned}((x+1)+\langle x^2\rangle)\cdot((2x+1)+\langle x^2\rangle) &= (x+1)(2x+1)+\langle x^2\rangle \\ &= (2x^2+3x+1)+\langle x^2\rangle \\ &= (2x^2+1)+\langle x^2\rangle \\ &= 1+\langle x^2\rangle\end{aligned}$$

where the last equality holds, because $(2x^2+1)-1=2x^2\in\langle x^2\rangle$.

(b) Anita says, "Our work in part (a) shows that $(x+1)+\langle x^2\rangle$ and $(2x+1)+\langle x^2\rangle$ are units." What might she mean?

**Solution.** The product of $(x+1)+\langle x^2\rangle$ and $(2x+1)+\langle x^2\rangle$ is $1+\langle x^2\rangle$, which is the multiplicative identity of $\mathbb{Z}_3[x]/\langle x^2\rangle$. Thus, $(x+1)+\langle x^2\rangle$ and $(2x+1)+\langle x^2\rangle$ are multiplicative inverses of each other, and thus are units.

6. The quotient ring $\mathbb{Z}_3[x]/\langle x^2\rangle$ is finite, so every nonzero element must be either a unit or a zero divisor (i.e., it cannot be neither). For each nonzero element $a(x)+\langle x^2\rangle$, determine if it's a unit or a zero divisor. Moreover, find a nonzero $b(x)+\langle x^2\rangle$ such that...

- For a unit: $(a(x)+\langle x^2\rangle)\cdot(b(x)+\langle x^2\rangle)=1+\langle x^2\rangle$.
- For a zero divisor: $(a(x)+\langle x^2\rangle)\cdot(b(x)+\langle x^2\rangle)=0+\langle x^2\rangle$.

**Solution.** Here are the classifications of the nonzero elements.

- $1+\langle x^2\rangle$ is a unit, because $(1+\langle x^2\rangle)\cdot(1+\langle x^2\rangle)=1+\langle x^2\rangle$.
- $2+\langle x^2\rangle$ is a unit, because $(2+\langle x^2\rangle)\cdot(2+\langle x^2\rangle)=1+\langle x^2\rangle$.
- $x+\langle x^2\rangle$ and $2x+\langle x^2\rangle$ are zero divisors, because

$$(x+\langle x^2\rangle)\cdot(2x+\langle x^2\rangle)=2x^2+\langle x^2\rangle=0+\langle x^2\rangle.$$

- $(x+1)+\langle x^2\rangle$ and $(2x+1)+\langle x^2\rangle$ are units, because

$$((x+1)+\langle x^2\rangle)\cdot((2x+1)+\langle x^2\rangle)=(2x^2+1)+\langle x^2\rangle=1+\langle x^2\rangle.$$

- $(x+2)+\langle x^2\rangle$ and $(2x+2)+\langle x^2\rangle$ are units, because

$$((x+2)+\langle x^2\rangle)\cdot((2x+2)+\langle x^2\rangle)=(2x^2+1)+\langle x^2\rangle=1+\langle x^2\rangle.$$

---

7. Consider the quotient ring $\mathbb{Z}_2[x]/\langle x^2\rangle$. (**Be careful:** The coefficient ring is $\mathbb{Z}_2$, not $\mathbb{Z}_3$.)

(a) Find all distinct elements of $\mathbb{Z}_2[x]/\langle x^2\rangle$, i.e., cosets $f(x)+\langle x^2\rangle$ where $f(x)\in\mathbb{Z}_2[x]$. ← There are 4 cosets.

**Solution.** We have $\mathbb{Z}_2[x]/\langle x^2\rangle=\{0+\langle x^2\rangle,\ 1+\langle x^2\rangle,\ x+\langle x^2\rangle,\ (x+1)+\langle x^2\rangle\}$.

(b) Construct the addition and multiplication tables for $\mathbb{Z}_2[x]/\langle x^2\rangle$.

**Solution.** Here is the addition table for $\mathbb{Z}_2[x]/\langle x^2\rangle$:

| $+$ | $0+\langle x^2\rangle$ | $1+\langle x^2\rangle$ | $x+\langle x^2\rangle$ | $(x+1)+\langle x^2\rangle$ |
|---|---|---|---|---|
| $0+\langle x^2\rangle$ | $0+\langle x^2\rangle$ | $1+\langle x^2\rangle$ | $x+\langle x^2\rangle$ | $(x+1)+\langle x^2\rangle$ |
| $1+\langle x^2\rangle$ | $1+\langle x^2\rangle$ | $0+\langle x^2\rangle$ | $(x+1)+\langle x^2\rangle$ | $x+\langle x^2\rangle$ |
| $x+\langle x^2\rangle$ | $x+\langle x^2\rangle$ | $(x+1)+\langle x^2\rangle$ | $0+\langle x^2\rangle$ | $1+\langle x^2\rangle$ |
| $(x+1)+\langle x^2\rangle$ | $(x+1)+\langle x^2\rangle$ | $x+\langle x^2\rangle$ | $1+\langle x^2\rangle$ | $0+\langle x^2\rangle$ |

And here is the multiplication table for $\mathbb{Z}_2[x]/\langle x^2\rangle$:

| $\cdot$ | $0+\langle x^2\rangle$ | $1+\langle x^2\rangle$ | $x+\langle x^2\rangle$ | $(x+1)+\langle x^2\rangle$ |
|---|---|---|---|---|
| $0+\langle x^2\rangle$ | $0+\langle x^2\rangle$ | $0+\langle x^2\rangle$ | $0+\langle x^2\rangle$ | $0+\langle x^2\rangle$ |
| $1+\langle x^2\rangle$ | $0+\langle x^2\rangle$ | $1+\langle x^2\rangle$ | $x+\langle x^2\rangle$ | $(x+1)+\langle x^2\rangle$ |
| $x+\langle x^2\rangle$ | $0+\langle x^2\rangle$ | $x+\langle x^2\rangle$ | $0+\langle x^2\rangle$ | $x+\langle x^2\rangle$ |
| $(x+1)+\langle x^2\rangle$ | $0+\langle x^2\rangle$ | $(x+1)+\langle x^2\rangle$ | $x+\langle x^2\rangle$ | $1+\langle x^2\rangle$ |

(c) Is $\mathbb{Z}_2[x]/\langle x^2\rangle$ a field? Why or why not? **Ans:** No. (Why not?)

**Solution.** No. The multiplication table shows that $(x+\langle x^2\rangle)\cdot(x+\langle x^2\rangle)=0+\langle x^2\rangle$. Thus, $x+\langle x^2\rangle$ is a zero divisor in $\mathbb{Z}_2[x]/\langle x^2\rangle$, which means that it is not a unit. And since not every nonzero element of $\mathbb{Z}_2[x]/\langle x^2\rangle$ is a unit, we conclude that $\mathbb{Z}_2[x]/\langle x^2\rangle$ is *not* a field.

8. (a) How many distinct elements does $\mathbb{Z}_5[x]/\langle x^2\rangle$ contain?

   (b) How about $\mathbb{Z}_7[x]/\langle x^2\rangle$?

   (c) How about $\mathbb{Z}_{11}[x]/\langle x^2\rangle$?

   (d) How about $\mathbb{Z}_{101}[x]/\langle x^2\rangle$?

   (e) How about $\mathbb{Z}_p[x]/\langle x^2\rangle$, where $p$ is prime? ← There are $p^2$ cosets.

**Solution.** We have $\mathbb{Z}_p[x]/\langle x^2\rangle=\{(ax+b)+\langle x^2\rangle \mid a, b\in\mathbb{Z}_p\}$. With $p$ choices for $a$ and $p$ choices for $b$, the quotient ring $\mathbb{Z}_p[x]/\langle x^2\rangle$ contains $p^2$ cosets/elements.

9. (a) Repeat Problem #8, but replace $\langle x^2\rangle$ with $\langle x^3\rangle$.

   (b) Repeat Problem #8, but replace $\langle x^2\rangle$ with $\langle x^n\rangle$, where $n$ is a positive integer.

10. Explore the quotient ring $\mathbb{Z}_3[x]/\langle x^2+1\rangle$, where $\langle x^2+1\rangle=\{(x^2+1)\cdot q(x) \mid q(x)\in\mathbb{Z}_3[x]\}$.

    (a) Find all distinct elements of $\mathbb{Z}_3[x]/\langle x^2+1\rangle$, i.e., distinct cosets of $\langle x^2+1\rangle$ in $\mathbb{Z}_3[x]$. ← There are 9 cosets.

    (b) For each nonzero element $a(x)+\langle x^2+1\rangle$, determine if it's a unit or a zero divisor.

    (c) Moreover, find a nonzero $b(x)+\langle x^2+1\rangle$ such that...

    - For a unit: $(a(x)+\langle x^2+1\rangle)\cdot(b(x)+\langle x^2+1\rangle)=1+\langle x^2+1\rangle$.
    - For a zero divisor: $(a(x)+\langle x^2+1\rangle)\cdot(b(x)+\langle x^2+1\rangle)=0+\langle x^2+1\rangle$.