Abstract Algebra
Day 27 Class Work Solutions

1. We just saw that $\mathbb{Z}$ is an integral domain, while $\mathbb{Z}_{12}$ is not.

   (a) Find other examples of an integral domain.

   Solution. Answers will vary. Examples include $\mathbb{Z}_7$ and the real numbers $\mathbb{R}$.

   (b) Find some non-examples, i.e., commutative rings that are *not* an integral domain.

   Solution. Answers will vary. Non-examples include $\mathbb{Z}_6$, $\mathbb{Z}_{10}$, and $\mathbb{Z}_{15}$.

2. Let α and β be elements of an integral domain. If $\alpha \cdot \beta = 0$, what conclusion can you make about α and β? Explain your reasoning.

   Ans: $\alpha = 0$ or $\beta = 0$ (or possibly both).

   Solution. If $\alpha \cdot \beta = 0$, we conclude that either α or β (or possibly both) must be zero. Otherwise, α and β would both be non-zero, making them zero divisors, which contradicts the fact that R is an integral domain.

3. **(Review of Group Theory)** In the *multiplicative* group U_{17}:

   (a) Find the multiplicative inverse of 6.

   Ans: $6^{-1} = 3$.

   Solution. Since $3 \cdot 6 = 1 \pmod{17}$, we have $6^{-1} = 3$.

   (b) Use your answer in part (a) to solve the equation $6x = 10 \pmod{17}$.

   Ans: $x = 13$.

   Solution. Multiply both sides of the equation by 3 to get $3 \cdot 6x = 3 \cdot 10 \pmod{17}$. And since $3 \cdot 6 = 1 \pmod{17}$, we obtain $x = 30 = 13 \pmod{17}$.

4. (a) In a multiplicative group G, explain why $ab = ac \implies b = c$.

   ← i.e., re-prove left cancellation in a group.

   Proof. Assume $ab = ac$ in a group. Multiply both sides of the equation *on the left* by a^{-1} to obtain $a^{-1}(ab) = a^{-1}(ac)$. Using the associative law gives $(a^{-1}a)b = (a^{-1}a)c$. Since $a^{-1}a = \varepsilon$, we get $\varepsilon b = \varepsilon c$. Finally, ε keeps all elements of the group unchanged, i.e., $\varepsilon b = b$ and $\varepsilon c = c$. Thus, $b = c$, as desired. ■

   (b) In the ring $\mathbb{Z}$, explain why

   $$ab = ac,\ a \neq 0 \implies b = c. \qquad (\clubsuit)$$

   Remark: You can't use the same proof as in part (a), since most $a \in \mathbb{Z}$ do not have a multiplicative inverse. Instead, use the fact that $\mathbb{Z}$ is an integral domain.

   Hint: If $ab = ac$, then $\boxed{???} = 0$.

   Proof. Assume $ab = ac$. Then $ab - ac = 0$ and thus $a \cdot (b - c) = 0$. If $b - c \neq 0$, then we'd have a pair of nonzero elements a and $b - c$ whose product is zero, which contradicts the fact that $\mathbb{Z}$ is an integral domain. Thus, $b - c = 0$ so that $b = c$. ■

   (c) Use a counter-example to show how ($\clubsuit$) is false in $\mathbb{Z}_{12}$. How does your proof from part (b) fail when working in $\mathbb{Z}_{12}$?

   Solution. For example, if $3b = 3c$ in $\mathbb{Z}_{12}$, we cannot conclude that $b = c$. We have $3 \cdot 9 = 3 \cdot 5$ in $\mathbb{Z}_{12}$, even though $9 \neq 5$. The proof from part (b) fails when we rewrite $3 \cdot 9 = 3 \cdot 5$ as $3 \cdot (9 - 5) = 0$ or, equivalently, $3 \cdot 4 = 0$. Then, since $\mathbb{Z}_{12}$ is *not* an integral domain, it is possible to have zero divisors such as 3 and 4.

5. (a) Find all the units in $\mathbb{Z}_7$. Do the same in $\mathbb{R}$, the set of real numbers.

   Solution. The units in $\mathbb{Z}_7$ are 1, 2, 3, 4, 5, 6, i.e., all the nonzero elements of $\mathbb{Z}_7$. Similarly, the units in $\mathbb{R}$ are all the nonzero real numbers.

   (b) Elizabeth says, "$\mathbb{Z}_7$ and $\mathbb{R}$ are *almost* multiplicative groups." What might she mean?

   Solution. Every nonzero element of $\mathbb{Z}_7$ has a multiplicative inverse. Likewise for $\mathbb{R}$.

Definition: A commutative ring is called a *field* if every nonzero element is a unit.

Key: In a field, we can always "divide" (i.e., multiply by a^{-1}), except when $a = 0$.

Recall: A *unit* is a ring element that has a multiplicative inverse.

---

6. In Problem #5, we saw that $\mathbb{Z}_7$ and $\mathbb{R}$ are fields.

   (a) Come up with a few other examples of a field.

   Solution. Examples of a field include $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_7$, and $\mathbb{Z}_p$ where p is prime.

   (b) Come up with some non-examples, i.e., commutative rings that are *not* a field.

   Solution. Non-examples include $\mathbb{Z}$ and $\mathbb{Z}_{12}$.

   (c) For each field in part (a), determine if it's an integral domain. Any conjecture?

   Solution. Yes, each field in part (a) is an integral domain. We conjecture that every field is an integral domain.

   (d) Find an integral domain that's not a field.

   ← Can you find more?

   Solution. $\mathbb{Z}$ is a possible example.

7. **Prove:** Every field is an integral domain.

   Proof. Let R be a field. To show that R is an integral domain, we must show that R does not contain any zero divisors. So, let $a \in R$ be a nonzero element. Since R is a field, a must be a unit. But a ring element cannot be both a unit and a zero divisor. Thus, a is *not* a zero divisor, from which we conclude that R is an integral domain. ■

8. Consider the ring $R = \mathbb{Z}_5[i] = \{a + bi \mid a, b \in \mathbb{Z}_5\}$. (Here, $i = \sqrt{-1}$ so that $i^2 = -1$.)

   (a) How many elements are in R? Explain your reasoning.

   Ans: 25 elements.

   Solution. Given $a + bi \in R$, there are five choices for a and five choices for b. Thus, R contains $5^2 = 25$ elements.

   (b) The element $1 + 4i \in R$ is a unit. Find its multiplicative inverse.

   Solution. We must find $a + bi \in R$ such that $(1 + 4i) \cdot (a + bi) = 1$. We have

   $$(1 + 4i) \cdot (a + bi) = (a - 4b) + (4a + b)i.$$

   Setting this equal to 1 (or $1 + 0i$) implies $a - 4b = 1$ and $4a + b = 0$. Solving this system of equations in $\mathbb{Z}_5$, we obtain $a = 3$ and $b = 3$. Thus, $(1 + 4i)^{-1} = 3 + 3i$.

   (c) The element $\alpha = 1 - 2i \in R$ is a zero divisor. Find a nonzero $\beta \in R$ where $\alpha \cdot \beta = 0$.

   Solution. We must find $\beta = a + bi \in R$ such that $(1 - 2i) \cdot (a + bi) = 0$. We have

   $$(1 - 2i) \cdot (a + bi) = (a + 2b) + (-2a + b)i.$$

   Setting this equal to 0 (or $0 + 0i$) implies $a + 2b = 0$ and $-2a + b = 0$. However, these are the same equation in $\mathbb{Z}_5$, since multiplying both sides of $a + 2b = 0$ by -2 gives $-2a - 4b = 0$ or $-2a + b = 0$, which is the second equation. Thus, we choose $a = 1$ so that $b = 2$, and we have $\beta = 1 + 2i$.

   (d) Is R an integral domain, a field, or neither?

   Solution. Neither, because it has a zero divisor.

9. A ring element $a \in R$ is called a *self inverse under multiplication* if $a^2 = 1$.

   (a) Find all self inverses in $\mathbb{Z}$. **Ans:** 1 and -1.

   Solution. 1 and -1.

   (b) Find all self inverses in $\mathbb{Z}_7$.

   Solution. 1 and $-1 = 6$.

   (c) Find all self inverses in $\mathbb{Z}_{12}$. (**Hint:** It's not just 1 and $-1 = 11$.)

   Solution. 1, 5, 7, and $-1 = 11$.

   (d) Find all self inverses in $\mathbb{Z}_{16}$.

   Solution. 1, 7, 9, and $-1 = 15$.

   (e) Find all self inverses in $\mathbb{Z}_{13}$.

   Solution. 1 and $-1 = 12$.

   (f) Any conjectures?

10. Determine all elements of an integral domain that are self inverses under multiplication. Explain your reasoning.

    Solution. Let a be a self inverse in an integral domain. Thus, $a^2 = 1$ so that $a^2 - 1 = 0$, which can be written as $(a-1) \cdot (a+1) = 0$. Since we're in an integral domain, we must have $a - 1 = 0$ or $a + 1 = 0$, so that a must equal 1 (the multiplicative identity) or -1 (the additive inverse of 1).

11. **(Some Food for Thought)** Consider the polynomial $f(x) = x^2 - 6x + 8$.

    (a) Factor the polynomial and use it to solve $x^2 - 6x + 8 = 0$ in $\mathbb{Z}$. **Ans:** $x = 2$ or 4.

    (b) Verify your result in part (a) by substituting each solution into $f(x)$.

    (c) Find all solutions to $x^2 - 6x + 8 = 0$ in $\mathbb{Z}_{15}$. (**Careful:** There are more than two.)

    (d) Anita says, "We found more than two solutions, since $\mathbb{Z}_{15}$ isn't an integral domain." What might she mean?

    (e) **(Challenge)** Find all solutions to $x^2 - 6x + 8 = 0$ in $\mathbb{Z}_{105}$. ← Yikes!