Abstract Algebra
Day 36 Class Work Solutions

1. Determine whether each ideal of $\mathbb{Z}$ is maximal.

   (a) $6\mathbb{Z}$ (b) $17\mathbb{Z}$ (c) $41\mathbb{Z}$ (d) $375\mathbb{Z}$ (e) $n\mathbb{Z}$

   Solution.

   (a) $6\mathbb{Z}$ is *not* maximal, since $6\mathbb{Z} \subsetneq 2\mathbb{Z} \subsetneq \mathbb{Z}$.

   (b) $17\mathbb{Z}$ is maximal.

   (c) $41\mathbb{Z}$ is maximal.

   (d) $375\mathbb{Z}$ is *not* maximal, since $375\mathbb{Z} \subsetneq 5\mathbb{Z} \subsetneq \mathbb{Z}$.

   (e) $n\mathbb{Z}$ is maximal if and only if n is prime.

2. Determine whether each ideal of $\mathbb{R}[x]$ is maximal. You don't have to justify these (yet). ← Your *instinct* says...?

   (a) $\langle x^2-1\rangle = \{(x^2-1)\cdot q(x) \mid q(x) \in \mathbb{R}[x]\}$, i.e., the set of all multiples of x^2-1.

   Solution. $\langle x^2-1\rangle$ is *not* maximal, since x^2-1 is factorable in $\mathbb{R}[x]$. ← See Problem #3.

   (b) $\langle x^2+1\rangle$

   Solution. $\langle x^2+1\rangle$ is maximal, since x^2+1 is unfactorable in $\mathbb{R}[x]$. ← See Problem #4.

3. Let $g(x) = x^2-1 \in \mathbb{R}[x]$. Below, we'll show that $\langle g(x)\rangle$ is *not* maximal in $\mathbb{R}[x]$.

   (a) **Prove:** $\langle g(x)\rangle \subseteq \langle x+1\rangle$. ← Just like $12\mathbb{Z} \subseteq 4\mathbb{Z}$.

   Hint: Let $\alpha(x) \in \langle g(x)\rangle$ and show that $\alpha(x) \in \langle x+1\rangle$.

   Proof. Let $\alpha(x) \in \langle g(x)\rangle$ so that $\alpha(x) = g(x)\cdot q(x)$ for some $q(x) \in F[x]$. Thus,

   $$\alpha(x) = (x^2-1)\cdot q(x) = ((x+1)(x-1))\cdot q(x) = (x+1)((x-1)\cdot q(x)),$$

   so that $\alpha(x) \in \langle x+1\rangle$. Thus, $\langle g(x)\rangle \subseteq \langle x+1\rangle$. ■

   (b) Find a polynomial $\beta(x)$ such that $\beta(x) \in \langle x+1\rangle$, but $\beta(x) \notin \langle g(x)\rangle$. **Ans:** $\beta(x) = x+1$.

   Solution. Answer will vary. A possible solution is $\beta(x) = x+1$, which is a multiple of $x+1$, but not a multiple of x^2-1.

   (c) Find a polynomial $\gamma(x)$ such that $\gamma(x) \in \mathbb{R}[x]$, but $\gamma(x) \notin \langle x+1\rangle$.

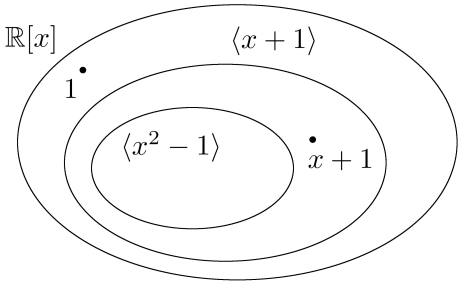
   Solution. Answer will vary. A possible solution is $\gamma(x) = 1$ (or any nonzero constant), which is in $\mathbb{R}[x]$, but not a multiple of $x+1$.

   (d) Use your results above to explain why **Recall:** $\langle g(x)\rangle \subsetneq \langle x+1\rangle$ means $\langle g(x)\rangle \subseteq \langle x+1\rangle$, but $\langle g(x)\rangle \neq \langle x+1\rangle$.

   $$\langle g(x)\rangle \subsetneq \langle x+1\rangle \subsetneq \mathbb{R}[x],$$

   i.e., $\langle x+1\rangle$ is *strictly* between $\langle g(x)\rangle$ and $\mathbb{R}[x]$. **So, $\langle g(x)\rangle$ is *not* maximal in $\mathbb{R}[x]$.**

   Solution. Combining the results of parts (a) and (b), we have $\langle g(x)\rangle \subsetneq \langle x+1\rangle$. Part (c) implies that $\langle x+1\rangle \subsetneq \mathbb{R}[x]$. Thus, $\langle g(x)\rangle \subsetneq \langle x+1\rangle \subsetneq \mathbb{R}[x]$. The picture below illustrates these set inclusions.



Recall. Every ideal of $F[x]$ is principal, i.e., $A = \langle p(x) \rangle$ for some $p(x) \in F[x]$. ← See Chapter 31.

4. Let $g(x) = x^2 + 1 \in \mathbb{R}[x]$. Below, we'll show that $\langle g(x) \rangle$ is maximal in $\mathbb{R}[x]$.

   (a) Elizabeth says, "Here's my plan. Let $\langle p(x) \rangle$ be an ideal where $\langle g(x) \rangle \subseteq \langle p(x) \rangle \subseteq \mathbb{R}[x]$. Then I'll show that $\langle p(x) \rangle$ must be equal to either $\langle g(x) \rangle$ or $\mathbb{R}[x]$." Explain why her approach will show that $\langle g(x) \rangle$ is maximal.

   Ans: This is the definition of a *maximal* ideal.

   Solution. Elizabeth's approach will show there cannot be an ideal that's *strictly* between $\langle g(x) \rangle$ and $\mathbb{R}[x]$ (i.e., between those two, but not equal to either one), which implies that $\langle g(x) \rangle$ is maximal.

   (b) **Prove:** If $\langle g(x) \rangle \subseteq \langle p(x) \rangle$, then $g(x) = p(x) \cdot q(x)$ for some $q(x) \in \mathbb{R}[x]$.

   Hint: $g(x) \in \langle g(x) \rangle$.

   Proof. Assume $\langle g(x) \rangle \subseteq \langle p(x) \rangle$. We have $g(x) = g(x) \cdot 1 \in \langle g(x) \rangle$. Since $\langle g(x) \rangle \subseteq \langle p(x) \rangle$, we have $g(x) \in \langle p(x) \rangle$, so that $g(x) = p(x) \cdot q(x)$ for some $q(x) \in \mathbb{R}[x]$. ■

   (c) Anita says, "But $g(x) = x^2 + 1$ is unfactorable in $\mathbb{R}[x]$. So $g(x) = p(x) \cdot q(x)$ would mean that either $p(x)$ or $q(x)$ has to be a constant." What might she mean?

   Solution. Since $g(x)$ is unfactorable, $g(x) = p(x) \cdot q(x)$ is *not* a legitimate factorization where $0 < \deg p(x), \deg q(x) < \deg g(x)$. Thus, the two possible cases are:

   (1) $\deg p(x) = 0$ and $\deg q(x) = \deg g(x)$, i.e., $p(x)$ is a constant.

   (2) $\deg p(x) = \deg g(x)$ and $\deg q(x) = 0$, i.e., $q(x)$ is a constant.

   Note that in both cases, we have $\deg g(x) = \deg p(x) + \deg q(x)$.

   (d) Suppose $p(x)$ is a constant. Say $p(x) = 3$, so that $g(x) = p(x) \cdot q(x)$ would be $x^2 + 1 = 3 \cdot \left(\frac{1}{3}x^2 + \frac{1}{3}\right)$. Explain why $\langle 3 \rangle = \mathbb{R}[x]$, so that $\langle p(x) \rangle = \mathbb{R}[x]$.

   Hint: $\langle 3 \rangle = \mathbb{R}[x]$ means every polynomial in $\mathbb{R}[x]$ is a multiple of 3.

   Ans: $f(x) = 3 \cdot \left(\frac{1}{3} f(x)\right)$.

   Solution. Let $f(x) \in \mathbb{R}[x]$. Then we can write $f(x)$ as $f(x) = 3 \cdot \left(\frac{1}{3} f(x)\right)$. Thus, every polynomial in $\mathbb{R}[x]$ is a multiple of 3, i.e., $\langle 3 \rangle = \mathbb{R}[x]$.

   (e) This time, suppose $q(x)$ is a constant. Say $q(x) = 3$ and $p(x) = \frac{1}{3}x^2 + \frac{1}{3}$, so that $g(x) = p(x) \cdot q(x)$ would be $x^2 + 1 = \left(\frac{1}{3}x^2 + \frac{1}{3}\right) \cdot 3$.

   Explain why $\langle \frac{1}{3}x^2 + \frac{1}{3} \rangle = \langle x^2 + 1 \rangle$, so that $\langle p(x) \rangle = \langle g(x) \rangle$.

   Hint: Show that $\langle \frac{1}{3}x^2 + \frac{1}{3} \rangle \subseteq \langle x^2 + 1 \rangle$ and $\langle x^2 + 1 \rangle \subseteq \langle \frac{1}{3}x^2 + \frac{1}{3} \rangle$.

   Solution. Let $\alpha(x) \in \langle \frac{1}{3}x^2 + \frac{1}{3} \rangle$, so that $\alpha(x) = (\frac{1}{3}x^2 + \frac{1}{3}) \cdot \beta(x)$ for some $\beta(x) \in \mathbb{R}[x]$. Then $\alpha(x) = (x^2 + 1) \cdot \left(\frac{1}{3}\beta(x)\right)$, so that $\alpha(x) \in \langle x^2 + 1 \rangle$. Thus, $\langle \frac{1}{3}x^2 + \frac{1}{3} \rangle \subseteq \langle x^2 + 1 \rangle$.

   Next, let $\alpha(x) \in \langle x^2 + 1 \rangle$, so that $\alpha(x) = (x^2 + 1) \cdot \beta(x)$ for some $\beta(x) \in \mathbb{R}[x]$. Then $\alpha(x) = \left(\frac{1}{3}x^2 + \frac{1}{3}\right) \cdot (3\beta(x))$, so that $\alpha(x) \in \langle \frac{1}{3}x^2 + \frac{1}{3} \rangle$. Thus, $\langle x^2 + 1 \rangle \subseteq \langle \frac{1}{3}x^2 + \frac{1}{3} \rangle$.

   Combining the two set inclusions implies $\langle \frac{1}{3}x^2 + \frac{1}{3} \rangle = \langle x^2 + 1 \rangle$, as desired.

   (f) Explain why $\langle g(x) \rangle$ is a maximal ideal.

   Solution. We considered an ideal $\langle p(x) \rangle$ such that $\langle g(x) \rangle \subseteq \langle p(x) \rangle \subseteq \mathbb{R}[x]$. Then we showed that $\langle p(x) \rangle = \langle g(x) \rangle$ (in part (e)) or $\langle p(x) \rangle = \mathbb{R}[x]$ (in part (d)). Thus, $\langle g(x) \rangle$ is maximal, since there is no ideal that is *strictly* between $\langle g(x) \rangle$ and $\mathbb{R}[x]$.

   ← Thus, we executed Elizabeth's plan.

5. Generalize your results from Problems #3 and #4 to prove each of the following.

   Theorem. Let F be a field and fix $g(x) \in F[x]$.

   (a) If $g(x)$ is factorable, then $\langle g(x) \rangle$ is *not* maximal in $F[x]$.

(b) If $g(x)$ is unfactorable, then $\langle g(x) \rangle$ is maximal in $F[x]$.

Solution. See Section 36.2. in the textbook.

6. **Prove:** The ideal $n\mathbb{Z}$ is maximal in $\mathbb{Z}$ if and only if n is prime.

Hint: This is an "if and only if" statement, so there are two directions to prove. For one of them, it would be easier to prove the contrapositive. ← Your polynomial proofs should help, too.

Proof. We must prove two implications:

- If $n\mathbb{Z}$ is maximal in $\mathbb{Z}$, then n is prime.
- If n is prime, then $n\mathbb{Z}$ is maximal in $\mathbb{Z}$.

For the first implication, we will prove its contrapositive, namely: If n is not prime, then $n\mathbb{Z}$ is not maximal in $\mathbb{Z}$. Assume that n is *not* prime. Thus, $n = ab$, where a, $b \in \mathbb{Z}$ and $1 < a$, $b < n$. We will show that $n\mathbb{Z} \subsetneq a\mathbb{Z}$. Suppose $\alpha \in n\mathbb{Z}$, so that $\alpha = n \cdot k$ where $k \in \mathbb{Z}$. Then $\alpha = (ab) \cdot k = a \cdot (bk) \in a\mathbb{Z}$ so that $\alpha \in a\mathbb{Z}$. Hence, $n\mathbb{Z} \subseteq a\mathbb{Z}$. Moreover, $a \in a\mathbb{Z}$ but $a \notin n\mathbb{Z}$ (since $1 < a < n$). This show that $n\mathbb{Z} \neq a\mathbb{Z}$, so that $n\mathbb{Z} \subsetneq a\mathbb{Z}$.

Certainly, $a\mathbb{Z} \subseteq \mathbb{Z}$. But $a\mathbb{Z} \neq \mathbb{Z}$, as $1 \in \mathbb{Z}$ but $1 \notin a\mathbb{Z}$ (since $a > 1$). Thus, we obtain $a\mathbb{Z} \subsetneq \mathbb{Z}$. Therefore, $n\mathbb{Z} \subsetneq a\mathbb{Z} \subsetneq \mathbb{Z}$, and thus $n\mathbb{Z}$ is *not* maximal in $\mathbb{Z}$.

To prove the second implication, assume that n is prime. Given that every ideal of $\mathbb{Z}$ is principal, consider an ideal $\langle d \rangle$ with $d > 0$ such that $n\mathbb{Z} \subseteq \langle d \rangle \subseteq \mathbb{Z}$. We must show that $\langle d \rangle = n\mathbb{Z}$ or $\langle d \rangle = \mathbb{Z}$. Since $n \in n\mathbb{Z}$ and $n\mathbb{Z} \subseteq \langle d \rangle$, we have $n \in \langle d \rangle$ so that $n = d \cdot k$ for some $k \in \mathbb{Z}$. But since n is prime, we must have $d = 1$ or $d = n$. If $d = 1$, then $\langle d \rangle = \langle 1 \rangle = \mathbb{Z}$. If $d = n$, then $\langle d \rangle = \langle n \rangle = n\mathbb{Z}$. Thus, $\langle d \rangle$ equals $n\mathbb{Z}$ or $\mathbb{Z}$, so that $n\mathbb{Z}$ is maximal in $\mathbb{Z}$. ■

7. Consider the ring $\mathbb{Z}_{12}$.

(a) Find all of its additive subgroups. ← There are six of them.

Solution. $\{0\}$, $\{0, 6\}$, $\{0, 4, 8\}$, $\{0, 3, 6, 9\}$, $\{0, 2, 4, 6, 8, 10\}$, $\mathbb{Z}_{12}$.

(b) Verify that each subgroup in part (a) satisfies the product absorption property. ← Thus, they're ideals.

Solution. I'll leave this up to you!

(c) Determine which ideals of $\mathbb{Z}_{12}$ are maximal. **Ans:** $\langle 3 \rangle$ and $\langle 2 \rangle$.

Solution. The maximal ideals are of $\mathbb{Z}_{12}$ are: $\{0, 3, 6, 9\}$ and $\{0, 2, 4, 6, 8, 10\}$.

- $\{0\}$ is *not* maximal, because $\{0\} \subsetneq \{0, 6\} \subsetneq \mathbb{Z}_{12}$.
- $\{0, 6\}$ is *not* maximal, because $\{0, 6\} \subsetneq \{0, 3, 6, 9\} \subsetneq \mathbb{Z}_{12}$.
- $\{0, 4, 8\}$ is *not* maximal, because $\{0, 4, 8\} \subsetneq \{0, 2, 4, 6, 8, 10\} \subsetneq \mathbb{Z}_{12}$.
- $\{0, 3, 6, 9\}$ is maximal, because there is no ideal strictly between $\{0, 3, 6, 9\}$ and $\mathbb{Z}_{12}$. Thus if there is an ideal A such that $\{0, 3, 6, 9\} \subseteq A \subseteq \mathbb{Z}_{12}$, then we must have $A = \{0, 3, 6, 9\}$ or $A = \mathbb{Z}_{12}$.
- $\{0, 2, 4, 6, 8, 10\}$ is maximal, as there is no ideal strictly between it and $\mathbb{Z}_{12}$.
- $\mathbb{Z}_{12}$ is *not* maximal; a maximal ideal M (of a ring R) must be different from R.

8. Repeat Problem #7 with the ring $\mathbb{Z}_7$.

Solution. The ideals of $\mathbb{Z}_7$ are $\{0\}$ and $\mathbb{Z}_7$ only. (Do you see why?) Then $\{0\}$ is a maximal ideal of $\mathbb{Z}_7$. If there is an ideal A such that $\{0\} \subseteq A \subseteq \mathbb{Z}_7$, then A must equal either $\{0\}$ or $\mathbb{Z}_7$, since those are the only ideals in $\mathbb{Z}_7$.

9. In Problem #7, we saw that $\mathbb{Z}_{12}$ has exactly two maximal ideals.

(a) Verify that $\mathbb{Z}_{20}$ has exactly two maximal ideals.

(b) Verify that $\mathbb{Z}_{28}$ has exactly two maximal ideals.

(c) Verify that $\mathbb{Z}_{18}$ has exactly two maximal ideals.

(d) Find a few more values of n for which $\mathbb{Z}_n$ has exactly two maximal ideals.

(e) What conjectures do you have?

10. Find a ring that has exactly three maximal ideals.

11. (a) Verify that 9 is *not* a unit in $\mathbb{Z}_{24}$. Then find a maximal ideal of $\mathbb{Z}_{24}$ containing 9.

(b) Verify that 10 is *not* a unit in $\mathbb{Z}_{35}$. Then find a maximal ideal of $\mathbb{Z}_{35}$ containing 10.

(c) Find a non-unit in $\mathbb{Z}_{30}$ and a maximal ideal of $\mathbb{Z}_{30}$ containing that non-unit element.

(d) Find a non-unit in $\mathbb{Z}_{54}$ and a maximal ideal of $\mathbb{Z}_{54}$ containing that non-unit element.

(e) What conjecture do you have?