Abstract Algebra
Day 30 Class Work Solutions

In the problems below, $F[x]$ is a polynomial ring where F is a field.

1. Let $f(x) = 2x + 7 \in \mathbb{R}[x]$.

   (a) Is $f(x)$ factorable or unfactorable in $\mathbb{R}[x]$? Explain your reasoning. **Ans:** Unfactorable.

   Solution. It is unfactorable. *In fact, all degree 1 polynomials are unfactorable.* Intuitively, we can not factor $f(x)$ into "smaller" factors. See Theorem 30.10 in the textbook for a complete proof of this fact.

   (b) Find $\alpha \in \mathbb{R}$ such that $f(\alpha) = 0$.

   Solution. Solving $2\alpha - 7 = 0$ in $\mathbb{R}$, we get $\alpha = \frac{7}{2}$.

2. (a) Is $f(x) = 4x + 2$ factorable or unfactorable in $\mathbb{Z}_7[x]$?

   (b) Is $f(x) = ax + b$ with $a \neq 0$ factorable or unfactorable in $F[x]$? ← i.e., $\deg f(x) = 1$.

   Solution. Both polynomials have degree 1 and thus are unfactorable.

3. Let $f(x) = x^3 + x + 1 \in \mathbb{Z}_3[x]$.

   (a) Compute $f(\alpha)$ for each $\alpha \in \mathbb{Z}_3$.

   Solution. We have $f(0) = 1$, $f(1) = 3 = 0$, and $f(2) = 11 = 2$, where the calculations are done in $\mathbb{Z}_3$.

   (b) Use your work in part (a) to determine if $f(x)$ is factorable or unfactorable in $\mathbb{Z}_3[x]$. Explain your reasoning. **Ans:** Factorable.

   Solution. Because $f(1) = 0$, we have $f(x) = (x-1) \cdot q(x)$ for some $q(x) \in \mathbb{Z}_3[x]$ with $\deg q(x) = 2$. Thus, $f(x)$ is factorable.

4. Let $f(x) = x^{5217} + 100 \in \mathbb{Z}_{101}[x]$.

   (a) Find $\alpha \in \mathbb{Z}_{101}$ such that $f(\alpha) = 0$.

   (b) Is $f(x)$ factorable or unfactorable in $\mathbb{Z}_{101}[x]$? Explain your reasoning.

   Solution. We have $f(1) = 101 = 0$ in $\mathbb{Z}_{101}$. Therefore, $f(x) = (x-1) \cdot q(x)$ for some $q(x) \in \mathbb{Z}_{101}[x]$ with $\deg q(x) = 5216$. Thus, $f(x)$ is factorable.

Definition. An element $\alpha \in F$ is a *root* of a polynomial $f(x)$ if $f(\alpha) = 0$.

← For example, $\alpha = 1$ is a root of $f(x)$ in Prob. #4.

5. Let $f(x) \in F[x]$ with $\deg f(x) \geq 2$.

   (a) **Prove:** If $f(x)$ has a root $\alpha \in F$, then $f(x)$ is factorable in $F[x]$.

   Solution. See Theorem 30.16 in the textbook for a complete proof. Here's the gist of the argument. If $f(\alpha) = 0$, then $f(x)$ factors as $f(x) = (x - \alpha) \cdot q(x)$ for some $q(x) \in F[x]$ with $\deg(x - \alpha)$, $\deg q(x) < \deg f(x)$. Thus, $f(x)$ is factorable.

(b) Why is the condition $\deg f(x) \geq 2$ needed here?

Hint: See Problem #1.

Solution. As in Problem #1, consider $f(x) = 2x - 7 \in \mathbb{R}[x]$. Then $f(x)$ has a root in $\mathbb{R}$, namely $\alpha = \frac{7}{2}$. However, $f(x)$ is *un*factorable in $\mathbb{R}[x]$. How does the argument in part (a) fail with $f(x) = 2x - 7$?

6. Let $f(x) \in F[x]$ with $\deg f(x) \geq 2$.

   (a) **True or False:** If $f(x)$ has no root in F, then $f(x)$ is unfactorable in $F[x]$.

   (b) Let $f(x) = x^4 + 3x^2 + 2 \in \mathbb{R}[x]$. Explain why $f(\alpha) > 0$ for all $\alpha \in \mathbb{R}$.

   ← So, $f(\alpha)$ never equals 0.

   (c) Factor $f(x) = x^4 + 3x^2 + 2$ in $\mathbb{R}[x]$.

   Ans: $(x^2 + 1) \cdot (x^2 + 2)$.

   (d) If necessary, go back and revisit part (a) of this question.

Solution. For all $\alpha \in \mathbb{R}$, we have $\alpha^4 \geq 0$ and $\alpha^2 \geq 0$ so that $f(\alpha) \geq 2$. Thus, $f(\alpha)$ never equals 0, which means that $f(x)$ has no root in $\mathbb{R}$. But we have $f(x) = (x^2 + 2)(x^2 + 1)$ so that $f(x)$ is factorable in $\mathbb{R}[x]$. Hence, the statement in part (a) is false. The fact that $f(x)$ has no root implies that $f(x)$ does not have a *linear* factor of the form $x - \alpha$. But, as seen in this example, $f(x)$ could still have a *quadratic* factor such as $x^2 + 2$.

7. Here's a salvage to Problem #6: **Assume $\deg f(x) = 2$ or 3.**

   (a) **Prove:** If $f(x)$ has no root in F, then $f(x)$ is unfactorable in $F[x]$.

   Hint: Try to prove its contrapositive.

   (b) Why was it necessary that $\deg f(x) = 2$ or 3? Where did you use that in your proof?

   (c) Is the polynomial in Problem #6(b) a counter-example? Why or why not?

Solution. See Theorem 30.19 in the textbook for a complete proof and an explanation of why $\deg f(x) = 2$ or 3 is necessary. The polynomial $f(x) = x^4 + 3x^2 + 2 \in \mathbb{R}[x]$ in Problem #6(b) is *not* a counterexample, because it has degree 4.

8. Determine if each polynomial is factorable or unfactorable.

   (a) $x^{100} - 1$ in $\mathbb{R}[x]$

   (b) $x^3 + x + 1$ in $\mathbb{Z}_5[x]$

   (c) $x^2 + 1$ in $\mathbb{Z}_{13}[x]$

   (d) $x^{1071} + 10x^{282} + 4x^{123} + 2$ in $\mathbb{Z}_{17}[x]$

   (e) $x^2 + x + 4$ in $\mathbb{Z}_{11}[x]$

   Solution.

   (a) $x^{100} - 1$ in $\mathbb{R}[x]$ is factorable, because $\alpha = 1$ is a root.

   (b) $x^3 + x + 1$ in $\mathbb{Z}_5[x]$ is unfactorable, because it has degree 3 and has no root in $\mathbb{Z}_5$.

   (c) $x^2 + 1$ in $\mathbb{Z}_{13}[x]$ is factorable, because $\alpha = 5$ is a root (so is $\alpha = 8$).

   (d) $x^{1071} + 10x^{282} + 4x^{123} + 2$ in $\mathbb{Z}_{17}[x]$ is factorable, because $\alpha = 1$ is a root.

   (e) $x^2 + x + 4$ in $\mathbb{Z}_{11}[x]$ is unfactorable, because it has degree 2 and has no root in $\mathbb{Z}_{11}$.

9. Consider $f(x) = x^4 - 1 \in \mathbb{Z}_5[x]$.

   (a) Elizabeth says, "I can tell right away that $f(x)$ is factorable." How might she know?

   Solution. We have $f(1) = 1^4 - 1 = 0$ in $\mathbb{Z}_5$, so that $\alpha = 1$ is a root.

   (b) Compute the product
   $$(x-1)(x-2)(x-3)(x-4)$$
   in $\mathbb{Z}_5[x]$ and verify that it equals $f(x)$.

   Solution. We have
   $$(x-1)(x-2)(x-3)(x-4) = x^4 - 10x^3 + 35x^2 - 50x + 24 = x^4 - 1,$$
   where the coefficients were computed in $\mathbb{Z}_5$.

10. (a) How do you think $x^6 - 1$ would factor in $\mathbb{Z}_7[x]$? Verify your conjecture.

    (b) How do you think $x^{10} - 1$ would factor in $\mathbb{Z}_{11}[x]$? Verify your conjecture.

    (c) How do you think $x^{12} - 1$ would factor in $\mathbb{Z}_{13}[x]$? Yes, please verify.

    (d) What's going on here? Can you generalize and justify?

11. (a) In $\mathbb{Z}_2[x]$, find the number of polynomials of the form $x^2 + bx + c$, with $b, c \in \mathbb{Z}_2$. ← The coefficient of x^2 is 1.

    (b) Of the polynomials in part (a), determine how many of them are factorable.

12. Repeat Problem #11 in $\mathbb{Z}_3[x]$; in $\mathbb{Z}_5[x]$; in $\mathbb{Z}_7[x]$; in $\mathbb{Z}_{11}[x]$; in $\mathbb{Z}_p[x]$ where p is prime.