Math 412. Quotient Rings of Polynomial Rings.

For this worksheet, \( \mathbb{F} \) always denotes a fixed field, such as \( \mathbb{Q}, \mathbb{R}, \mathbb{C}, \) or \( \mathbb{Z}_p \) for \( p \) prime.

**Definition.** Fix a polynomial \( f(x) \in \mathbb{F}[x] \). Define two polynomials \( g, h \in \mathbb{F}[x] \) to be congruent modulo \( f \) if \( f(g - h) \). We write \( g \equiv h \mod f \).

We write \([g]_f\) for the set \( \{g + kf \mid k \in \mathbb{F}[x]\} \) of all polynomials congruent to \( g \) modulo \( f \).

We write \( \mathbb{F}[x]/(f) \) for the set of all congruence classes of \( \mathbb{F}[x] \) modulo \( f \).

**Caution:** The elements of \( \mathbb{F}[x]/(f) \) are sets.

The set \( \mathbb{F}[x]/(f) \) has a natural ring structure called the Quotient Ring of \( \mathbb{F}[x] \) by the ideal \((f)\).

**A. Warm Up/Review.** Fix a polynomial \( f(x) \in \mathbb{F}[x] \) of degree \( d > 0 \).

1. Discuss what it means that congruence modulo \( f \) is an equivalence relation on \( \mathbb{F}[x] \).
2. Discuss with your group why every congruence class \([g]_f\) contains a unique polynomial of degree less than \( d \). What is the analogous fact for congruence classes in \( \mathbb{Z} \) modulo \( n \)?
3. Show that there are exactly four distinct congruence classes for \( \mathbb{Z}_2[x] \) modulo \( x^2 + x \).

   List them out, in set-builder notation. For each of the four, write it in the form \([g]_{x^2 + x}\) for two different \( g \).
4. How many distinct congruence classes are there for \( \mathbb{Z}_p[x] \) modulo \( f \), where \( f \) is a polynomial of degree \( d \)?

**B. Ring Structure on the set of Congruence Classes \( \mathbb{F}[x]/(f(x)) \).** Fix a polynomial \( f(x) \in \mathbb{F}[x] \) of degree \( d > 0 \).

1. Consider arbitrary \( g, h \in \mathbb{F}[x] \). Suppose \( g' \in [g]_f \) and \( h' \in [h]_f \). Prove that \( g' + h' \in [g + h]_f \).
2. Explain how (1) allows us to define a well-defined binary operation (call it “addition”) on the set \( \mathbb{F}[x]/(f(x)) \) of congruence classes. Note that the elements of \( \mathbb{F}[x]/(f(x)) \) are sets and the notation \([g]_f\) is biased—you can represent this set by many different \( g \)—so you need to be careful.
3. Suppose \( g' \in [g]_f \) and \( h' \in [h]_f \). Prove \(^2\) that \( g'h' \in [gh]_f \).
4. Explain how (3) allows us to define a well-defined binary operation (call it “multiplication”) on the set \( \mathbb{F}[x]/(f(x)) \) of congruence classes. Why is this non-obvious?
5. Find elements in \( \mathbb{F}[x]/(f(x)) \) that serve as additive and multiplicative identities for your operations in (2) and (4).
6. Discuss what needs to be checked to ensure that the operations defined in (2) and (4) make \( \mathbb{F}[x]/(f(x)) \) into a commutative ring. Now, illustrate how to check one or two of the axioms, pointing out how they follow from the corresponding axioms in \( \mathbb{F}[x] \). Without writing it all out, make sure everyone is confident how to prove that \( \mathbb{F}[x]/(f(x)) \) is commutative ring.

\(^2\)Hint: you need to show \( f|(g'h' - gh) \). Use the trick of “cleverly adding zero”: equivalently, you need to show \( f|(g'h' + (gh' - gh') - gh) \).
C. EXAMPLES. Consider an arbitrary monic degree two polynomial \(x^2 + ax + b \in \mathbb{Z}_2[x]\). We will investigate the quotient rings of the form \(\mathbb{Z}_2[x]/(x^2 + ax + b)\). There are four cases to consider, depending on the values of \(a\) and \(b\):

\[
R_1 = \mathbb{F}[x]/(x^2);
R_2 = \mathbb{F}[x]/(x^2 + 1);
R_3 = \mathbb{F}[x]/(x^2 + x);
R_4 = \mathbb{F}[x]/(x^2 + x + 1).
\]

1. Abusing notation slightly, the elements of each \(R_i\) can be denoted \([0]\), \([1]\), \([x]\), and \([x+1]\). Why? In what sense is this an “abuse”? These notations have completely different meanings in each \(R_i\). Explain.

2. Write down the addition table for \(R_1\). How do the addition tables for the other \(R_i\) look?

3. For each of the four rings \(R_i\), write out the multiplication tables.

4. For each of the four rings \(R_i\), identify all nilpotent elements.

5. For each of the four rings \(R_i\), identify all idempotent elements.

6. For each of the four rings \(R_i\), identify all zero divisors.

7. For each of the four rings \(R_i\), identify all units.

8. One of these \(R_i\) is a field (with four elements!). Which one?

9. None of the three rings \(R_2, R_3,\) or \(R_4\) can be isomorphic to any other. Explain why, using your answers to (4)–(7).

10. Find an isomorphism \(\phi : R_1 \rightarrow R_2\). [Hint: Your answers to (4)–(7) are a clue.]

11. Find an isomorphism \(\psi : R_3 \rightarrow \mathbb{Z}_2 \times \mathbb{Z}_2\). [Hint: Your answers to (4)–(7) are a clue.] There are two correct answers.

12. Explain why the ring \(\mathbb{Z}_4\) is not isomorphic to any of the rings \(R_i\). [Hint: Consider \(1 + 1\).]

D. RINGS WITH TWO OR THREE ELEMENTS:

1. Show that any two rings with two elements are isomorphic. That is, up to isomorphism, there is only one ring with two elements. What is this ring, up to isomorphism?

2. Show that any two rings with three elements are isomorphic. That is, up to isomorphism, there is only one ring with three elements. What is this ring, up to isomorphism? [Hint: you can call the elements 0, 1, and \(a\). Start making addition and multiplication tables and see what happens.]

E. RINGS WITH FOUR ELEMENTS:

1. You found a field with four elements! What is it? It is a finite field but not of the form \(\mathbb{Z}_p\) for any \(p\) (why not?). This is very exotic!

2. You showed in C that up to isomorphism, there are at least four different rings with four elements. Explain. List out representatives of each isomorphism type.

3. BONUS: Show that any ring with four elements is isomorphic to one on your list above.