Math 110A Homework 7

Jiaping Zeng

3/1/2021

1. Write out the addition and multiplication tables for the congruence class ring $F[x]/(p(x))$. In each case, is $F[x]/(p(x))$ a field?

   (a) $F = \mathbb{Z}/2\mathbb{Z}, p(x) = x^3 + x + 1$

   Answer:

$+$	$[0]$	$[1]$	$[x]$	$[x+1]$	$[x^2]$	$[x^2+1]$	$[x^2+x]$	$[x^2+x+1]$
$[0]$	$[0]$	$[1]$	$[x]$	$[x+1]$	$[x^2]$	$[x^2+1]$	$[x^2+x]$	$[x^2+x+1]$
$[1]$	$[1]$	$[0]$	$[x+1]$	$[x]$	$[x^2+1]$	$[x^2]$	$[x^2+x+1]$	$[x^2+x]$
$[x]$	$[x]$	$[x+1]$	$[0]$	$[1]$	$[x^2+x]$	$[x^2+x+1]$	$[x^2+$	$[x^2+1]$
$[x+1]$	$[x+1]$	$[x]$	$[1]$	$[0]$	$[x^2+x+1]$	$[x^2+x]$	$[x^2+1]$	$[x^2]$
$[x^2]$	$[x^2]$	$[x^2+1]$	$[x^2+x]$	$[x^2+x+1]$	$[0]$	$[1]$	$[x]$	$[x+1]$
$[x^2+1]$	$[x^2+1]$	$[x^2]$	$[x^2+x+1]$	$[x^2+x]$	$[1]$	$[0]$	$[x+1]$	$[x]$
$[x^2+x]$	$[x^2+x]$	$[x^2+x+1]$	$[x^2]$	$[x^2+1]$	$[x]$	$[x+1]$	$[0]$	$[1]$
$[x^2+x+1]$	$[x^2+x+1]$	$[x^2+x]$	$[x^2+1]$	$[x^2]$	$[x+1]$	$[x]$	$[1]$	$[0]$

$\cdot$	$[0]$	$[1]$	$[x]$	$[x+1]$	$[x^2]$	$[x^2+1]$	$[x^2+x]$	$[x^2+x+1]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[x]$	$[x+1]$	$[x^2]$	$[x^2+1]$	$[x^2+x]$	$[x^2+x+1]$
$[x]$	$[0]$	$[x]$	$[x^2]$	$[x^2+x]$	$[x+1]$	$[1]$	$[x^2+x+1]$	$[x^2+1]$
$[x+1]$	$[0]$	$[x+1]$	$[x^2+x]$	$[x^2+1]$	$[x^2+x+1]$	$[x^2+$	$[1]$	$[x]$
$[x^2]$	$[0]$	$[x^2]$	$[x+1]$	$[x^2+x+1]$	$[x^2+x]$	$[x]$	$[x^2+x]$	$[1]$
$[x^2+1]$	$[0]$	$[x^2+1]$	$[1]$	$[x^2]$	$[x]$	$[x^2+x+1]$	$[x+1]$	$[x^2+x]$
$[x^2+x]$	$[0]$	$[x^2+x]$	$[x^2+x+1]$	$[1]$	$[x^2+1]$	$[x+1]$	$[x]$	$[x^2]$
$[x^2+x+1]$	$[0]$	$[x^2+x+1]$	$[x^2+1]$	$[x]$	$[1]$	$[x^2+x]$	$[x^2]$	$[x+16]$

   (b) $F = \mathbb{Z}/3\mathbb{Z}, p(x) = x^2 + 1$

   Answer:

$+$	$[0]$	$[1]$	$[2]$	$[x]$	$[x+1]$	$[x+2]$	$[2x]$	$[2x+1]$	$[2x+2]$
$[0]$	$[0]$	$[1]$	$[2]$	$[x]$	$[x+1]$	$[x+2]$	$[2x]$	$[2x+1]$	$[2x+2]$
$[1]$	$[1]$	$[2]$	$[0]$	$[x+1]$	$[x+2]$	$[x]$	$[2x+1]$	$[2x+2]$	$[2x]$
$[2]$	$[2]$	$[0]$	$[1]$	$[x+2]$	$[x]$	$[x+1]$	$[2x+2]$	$[2x]$	$[2x+1]$
$[x]$	$[x]$	$[x+1]$	$[x+2]$	$[2x]$	$[2x+1]$	$[2x+2]$	$[0]$	$[1]$	$[2]$
$[x+1]$	$[x+1]$	$[x+2]$	$[x]$	$[2x+1]$	$[2x+2]$	$[2x]$	$[1]$	$[2]$	$[0]$
$[x+2]$	$[x+2]$	$[x]$	$[x+1]$	$[2x+2]$	$[2x]$	$[2x+1]$	$[2]$	$[0]$	$[1]$
$[2x]$	$[2x]$	$[2x+1]$	$[2x+2]$	$[0]$	$[1]$	$[2]$	$[x]$	$[x+1]$	$[x+2]$
$[2x+1]$	$[2x+1]$	$[2x+2]$	$[2x]$	$[1]$	$[2]$	$[0]$	$[x+1]$	$[x+2]$	$[x]$
$[2x+2]$	$[2x+2]$	$[2x]$	$[2x+1]$	$[2]$	$[0]$	$[1]$	$[x+2]$	$[x]$	$[x+1]$

$\cdot$	$[0]$	$[1]$	$[2]$	$[x]$	$[x+1]$	$[x+2]$	$[2x]$	$[2x+1]$	$[2x+2]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[x]$	$[x+1]$	$[x+2]$	$[2x]$	$[2x+1]$	$[2x+2]$
$[2]$	$[0]$	$[2]$	$[1]$	$[2x]$	$[2x+2]$	$[2x+1]$	$[x]$	$[x+2]$	$[x+1]$
$[x]$	$[0]$	$[x]$	$[2x]$	$[2]$	$[x+2]$	$[2x+2]$	$[1]$	$[x+1]$	$[2x+1]$
$[x+1]$	$[0]$	$[x+1]$	$[2x+2]$	$[x+2]$	$[2x]$	$[1]$	$[2x+1]$	$[2]$	$[x]$
$[x+2]$	$[0]$	$[x+2]$	$[2x+1]$	$[2x+2]$	$[1]$	$[x]$	$[x+1]$	$[2x]$	$[2]$
$[2x]$	$[0]$	$[2x]$	$[x]$	$[1]$	$[2x+1]$	$[x+1]$	$[2]$	$[2x+2]$	$[x+2]$
$[2x+1]$	$[0]$	$[2x+1]$	$[x+2]$	$[x+1]$	$[2]$	$[2x]$	$[2x+2]$	$[x]$	$[1]$
$[2x+2]$	$[0]$	$[2x+2]$	$[x+1]$	$[2x+1]$	$[x]$	$[2]$	$[x+2]$	$[1]$	$[2x]$

(c) $F = \mathbb{Z}/2\mathbb{Z}, p(x) = x^2 + 1$

Answer:

$+$	$[0]$	$[1]$	$[x]$	$[x+1]$
$[0]$	$[0]$	$[1]$	$[x]$	$[x+1]$
$[1]$	$[1]$	$[0]$	$[x+1]$	$[x]$
$[x]$	$[x]$	$[x+1]$	$[0]$	$[1]$
$[x+1]$	$[x+1]$	$[x]$	$[1]$	$[0]$

$\cdot$	$[0]$	$[1]$	$[x]$	$[x+1]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[x]$	$[x+1]$
$[x]$	$[0]$	$[x]$	$[1]$	$[x+1]$
$[x+1]$	$[0]$	$[x+1]$	$[x+1]$	$[0]$

2. Find a fourth-degree polynomial in $(\mathbb{Z}/2\mathbb{Z})[x]$ whose roots are the four elements of the field $(\mathbb{Z}/2\mathbb{Z})[x]/(x^2+x+1)$.

   Answer: As shown in Example 3, the four elements of $(\mathbb{Z}/2\mathbb{Z})[x]/(x^2+x+1)$ are $[0], [1], [x], [x+1]$. Then we have $x(x+1)(x^2+x+1) = x^4+2x^3+2x^2+x \equiv x^4+x$. Therefore the roots of $p(x) = x^4+x$ are the four elements of $(\mathbb{Z}/2\mathbb{Z})[x]/(x^2+x+1)$.

3. (a) Show that $(\mathbb{Z}/2\mathbb{Z})[x]/(x^3+x+1)$ is a field.

   Answer: By substitution, neither of 0 or 1 is a root of x^3+x+1 $(p(0) = 1, p(1) = 1)$. Therefore

x^3+x+1 is irreducible in $\mathbb{Z}/2\mathbb{Z}$ by Corollary 4.19. Then by Theorem 5.10 $(\mathbb{Z}/2\mathbb{Z})[x]/(x^3+x+1)$ is a field.

(b) Show that $(\mathbb{Z}/2\mathbb{Z})[x]/(x^3+x+1)$ contains all three roots of x^3+x+1.

Answer: $[x], [x^2], [x^2+x]$ are roots of x^3+x+1 in $(\mathbb{Z}/2\mathbb{Z})[x]/(x^3+x+1)$. Therefore $(\mathbb{Z}/2\mathbb{Z})[x]/(x^3+x+1)$ contains all three roots of x^3+x+1.

4. Show that $\mathbb{Q}[x]/(x^2-2)$ is not isomorphic to $\mathbb{Q}[x]/(x^2-3)$.
Answer: Suppose there is a solution to $a^2 = 2$ in $\mathbb{Q}[x]/(x^2-3)$, which would imply that $\sqrt{2} \in \mathbb{Q}$ which is a contradiction. Therefore $\mathbb{Q}[x]/(x^2-2)$ is not isomorphic to $\mathbb{Q}[x]/(x^2-3)$.

5. Show that $\mathbb{Q}[x]/(x^2-2)$ is isomorphic to $\mathbb{Q}[x]/(x^2+2x-1)$.
Answer: Let $f(x) = x+1$ and $\varphi(f(x)) = f(x+1)$, then $\varphi^{-1}(f(x)) = f(x-1)$. Note that $\varphi(x^2-2) = (x+1)^2-2 = x^2+2x-1$ and $\varphi(x^2+2x-1) = (x-1)^2+2(x-1)-1 = x^2-2$. Therefore $\mathbb{Q}[x]/(x^2-2)$ is isomorphic to $\mathbb{Q}[x]/(x^2+2x-1)$.

6. (a) Show that the set $I = \{(k,0)|k \in \mathbb{Z}\}$ is an ideal in the ring $\mathbb{Z}\times\mathbb{Z}$.
Answer: Take $(p,q) \in \mathbb{Z}\times\mathbb{Z}$ and $(k,0) \in I$, we have $(p,q)(k,0) = (kp,0) \in I$ and $(k,0)(p,q) = (kp,0) \in I$. Therefore I is an ideal.

(b) Show that the set $I = \{(k,k)|k \in \mathbb{Z}\}$ is *not* an ideal in the ring $\mathbb{Z}\times\mathbb{Z}$.
Answer: Take $(1,2) \in \mathbb{Z}\times\mathbb{Z}$ and $(k,k) \in I$, we have $(1,2)(k,k) = (k,2k)$ which is not in I for nonzero k. Therefore I is not an ideal.

7. List all distinct principal ideals in each ring:

(a) $\mathbb{Z}/5\mathbb{Z}$
Answer: $(0) = \{0\}$.

(b) $\mathbb{Z}/9\mathbb{Z}$
Answer: $(0) = \{0\}, (3) = \{3\}$.

(c) $\mathbb{Z}/12\mathbb{Z}$
Answer: $(0) = \{0\}, (2) = \{2,4,6,8,10,0\}, (3) = \{3,6,9,0\}, (4) = \{4,8,0\}, (6) = \{6,0\}$.

8. (a) If I and J are ideals of R, prove that $I \cap J$ is also an ideal.
Answer: Take $a, b \in I \cap J$ and $r \in R$, then $a-b \in I$ and $a-b \in J$ since I and J are ideals, so $a-b \in I\cap J$. We also have $ar \in I$ and $ra \in I$ since I is an ideal; Similarly, we also have $ar \in J$ and $ra \in J$ since J is an ideal. Therefore $ar \in I \cap J$ and $ra \in I \cap J$, so $I \cap J$ is an ideal by Theorem 6.1.

(b) If $\{I_k\}_{k\in S}$ is a (possibly infinite) family of ideals in R, prove that the intersection $\bigcap_{k\in S} I_k$ is also an ideal in R.
Answer: By induction on the number of elements n;
Base case: $n = 2$, $\{I_1, I_2\}$ is a family of ideals in R, then $I_1 \cap I_2$ is an ideal by part (a).
Inductive step: Suppose that the statement holds for $n-1$ elements, we want to show that it will also hold for n elements. Let $A = \bigcap_{k=1}^{n-1} I_k$, then A is an ideal by inductive hypothesis. Then

$A \cap I_n = \bigcap_{k=1}^{n} I_k$ is also an ideal by part (a).

Therefore $\bigcap_{k \in S} I_k$ is an ideal in R.

(c) Give an example in $\mathbb{Z}$ to prove that if I and J are ideals, that $I \cup J$ might not be an ideal (or even a subring).

Answer: Take $I = 2\mathbb{Z}$ and $J = 3\mathbb{Z}$, then $2 \in I$ and $3 \in J$ but $3 - 2 = 1 \notin I \cup J$. So $I \cup J$ is not a subring.