HW #10 Solutions

#1 a) $I = \left\{ a_2x^2 + a_3x^3 + a_4x^4 + \cdots + a_kx^k \;:\; \begin{array}{l} k \geq 2 \\ k \in \mathbb{Z} \\ a_i \in \mathbb{Z}_3 \end{array} \right\}$

Let's use the ideal criterion.

(subset, contains 0, closed under subtraction, closed under mult by elements in R.)

- I is by definition a subset of R.
- I contains 0 by definition.
- Suppose we have two elements of I, f(x) and g(x):

$$f(x) = f_2x^2 + f_3x^3 + \cdots + f_kx^k$$
$$g(x) = g_2x^2 + g_3x^3 + \cdots + g_\ell x^\ell$$

WLOG can assume $k=\ell$, just set some $f_i = 0$ or $g_i = 0$ if nec.

Then $f(x) - g(x) = (f_2 - g_2)x^2 + (f_3 - g_3)x^3 + \cdots + (f_k - g_k)x^k$,

which is also in I, since its linear and constant terms are zero. (Okay to just say clearly in words instead.)

- Next, let $f(x) \in I$ and $h(x) \in R$, so

$f(x) = f_2 x^2 + \cdots + f_k x^k$

$h(x) = h_0 + h_1 x + h_2 x^2 + \cdots + h_k x^k$

Again, can take same ending ~~degree~~ term WLOG, by setting some coeffs $= 0$ if necessary.

Then in the products $f(x)\,h(x)$ and $h(x)\,f(x)$, every nonzero term has degree at least 2, so these are both in I.

Thus I is an ideal of R.

#1b) Suppose we have two elements in R, $a(x)$ and $b(x)$, written in Div Alg form after dividing by x^2:

$$a(x) = x^2 q_a(x) + r_a(x)$$

$$b(x) = x^2 q_b(x) + r_b(x).$$

fs. $q_a, r_a \in \mathbb{Z}_3[x]$

$q_b, r_b \in \mathbb{Z}_3[x]$

Our remainders must each either be 0 or have degree ≤ 1, so $r_a(x) = a_1 x + a_0$

$r_b(x) = b_1 x + b_0$

fs $a_1, a_0, b_1, b_0 \in \mathbb{Z}_3$.

So $a(x) = x^2 q_a(x) + a_1 x + a_0$

$b(x) = x^2 q_b(x) + b_1 x + b_0$.

Now onto the proof: We know $a(x)$ and $b(x)$ are in the same coset of I $\iff$

$$a(x) - b(x) \in I$$

$\iff$

$$(x^2 q_a(x) + a_1 x + a_0) - (x^2 q_b(x) + b_1 x + b_0) \in I$$

$\iff$

$$x^2[q_a(x) - q_b(x)] + (a_1 - b_1)x + a_0 - b_0 \in I$$

$\iff$ $(a_1 - b_1)x + a_0 - b_0 \in I$

(since $x^2[q_a(x) - q_b(x)] \in I$, we can subtract it without changing whether we are in I.)

$\iff$ $a_1 - b_1 = 0$ and $a_0 - b_0 = 0$

(Since elements of I must have zero constant and linear terms.)

$\Leftrightarrow a_1 = b_1$ and $a_0 = b_0$

$\Leftrightarrow a_1 x + a_0 = b_1 x + b_0$

$\Leftrightarrow r_a(x) = r_b(x)$

$\Leftrightarrow$ $a(x)$ and $b(x)$ have the same remainder after dividing by x^2.

(Also ok to do the 2 directions separately.)

#1c) Part b showed that every $f(x) \in \mathbb{Z}_3[x]$ is in a coset with its remainder polynomial and that different remainders are in different cosets. Thus there is exactly one coset for each possible remainder. Since our remainders must be of the form

$r_1 x + r_0$ with $r_0, r_1 \in \mathbb{Z}_3$,

there are 9 such possibilities, so 9 cosets of I, i.e. 9 elts in R/I.

2a)

·	0+I	1+I	2+I	x+I	x+1+I	x+2+I	2x+I	2x+1+I	2x+2+I
0+I	0+I	0+I	0+I	0+I	0+I	0+I	0+I	0+I	0+I
1+I		1+I	2+I	x+I	x+1+I	x+2+I	2x+I	2x+1+I	2x+2+I
2+I			1+I	2x+I	2x+2+I	2x+1+I	x+I	x+2+I	x+1+I
x+I				0+I	x+I	2x+I	0+I	x+I	2x+I
x+1+I					2x+1+I	2+I	2x+I	1+I	x+2+I
x+2+I						x+1+I	x+I	2x+2+I	1+I
2x+I							0+I	2x+I	x+I
2x+1+I								x+1+I	2+I
2x+2+I									2x+1+I

this side determined by symmetry since R/F comm.

(Blue lines just to help visually.)

#2b) 0 is neither

2 zero divisors: $x+I$, $2x+I$ (from □ in table)

6 units: $1+I$, $2+I$, $x+1+I$, $2x+1+I$,

$1+I$: own inverse; $2+I$: own inverse; $x+1+I$, $2x+1+I$: inverse pair

$x+2+I$, $2x+2+I$ (from □ in table)

inverse pair.

#8) We know $\langle R/I, + \rangle$ is an abelian group with 9 elements, so it must be isomorphic to $\mathbb{Z}_3 \times \mathbb{Z}_3$ or $\mathbb{Z}_9$. Elements are of the form $(ax+b)+I$ with $a, b \in \mathbb{Z}_3$.

Notice adding 3 copies of any such element gives the zero coset.

$$3\left[(ax+b)+I\right] = 3(ax+b)+I \quad \text{(by coset addition rule)}$$

$$= (3ax+3b)+I \quad \text{since we are in } \mathbb{Z}_3.$$

$$= 0x+0+I$$

$$= 0+I$$

Thus every element has additive order ≤ 3, so we must be isomorphic to $\mathbb{Z}_3 \times \mathbb{Z}_3$ (since $\mathbb{Z}_9$ has an element of order 9.

Alternatively, show $\varphi: R/I \to \mathbb{Z}_3 \times \mathbb{Z}_3$

$(ax+b+I) \longmapsto (\bar{a}, \bar{b})$ is a group isomorphism.

To see R/I and $\mathbb{Z}_3 \times \mathbb{Z}_3$ are not isomorphic rings, look for a structural property where they differ. For example:

- R/I has exactly 2 zero divisors, but $\mathbb{Z}_3 \times \mathbb{Z}_3$ has at least 3: $(0,1)$, $(1,0)$, and $(0,2)$, since $(0,1)\cdot(1,0) = (0,2)\cdot(1,0) = (0,0)$.

- R/I has exactly 2 elements which are their own multiplicative inverses, but $\mathbb{Z}_3 \times \mathbb{Z}_3$ has more: $(1,1)$, $(2,2)$, $(1,2)$, and $(2,1)$.

Note: it is <u>NOT</u> enough to check that a map you used for the additive group isom fails the multiplicative Homom. Prop. This only shows your special map is not an isomorphism, not that no isom. exists.