Exercises 2

Please submit solutions by 3pm on Thursday 22nd February to the pigeonholes in 4W (ground floor).

(W) = Warm-up; (H) = Homework; (A)=Additional.

1. (W) Decide whether each of the following is a subring, an ideal, or neither; prove your assertions!

(1) $\{-1, 0, 1\} \subset \mathbb{Z}$;

(2) $\{a_0 + a_2x^2 + a_4x^4 + \cdots \mid a_i \in \mathbb{Q}\} \subset \mathbb{Q}[[x]]$;

(3) $\{a_2x^2 + a_3x^3 + a_4x^4 + \cdots \mid a_i \in \mathbb{Q}\} \subset \mathbb{Q}[[x]]$;

(4) $\{\text{polynomials of degree } \leq 2\} \subseteq \mathbb{Q}[x]$;

(5) $\{p \in \mathbb{Q}[x] \mid p(1) = 0\} \subset \mathbb{Q}[x]$.

2. (W) Let R be a ring, and let $R[x]$ denote the ring of polynomials with coefficients in R. Show that if R is an integral domain, then so is $R[x]$.

3. (W) Let $\sim$ be a congruence relation on a ring R.

(1) Prove that $[0]$, the congruence class of 0, is an ideal in R.

(2) For $a, b \in R$, show that $a \sim b \Leftrightarrow a - b \in [0]$.

(3) Show that the congruence classes of $\sim$ are the cosets of I, i.e., $[a] = a + [0]$ for all $a \in R$.

4. (H) Let R be an integral domain, and let $u \in R$ be a unit.

(1) Show that any element in $R[[x]]$ of the form $u + a_1x + a_2x^2 + \cdots$ is a unit in $R[[x]]$.

(2) Find the multiplicative inverse of $-1 + 2x \in \mathbb{Z}[[x]]$.

5. (H) Let $R = \mathbb{Z}_2[x]$ be the polynomial ring with coefficients in the field $\mathbb{Z}_2$, and consider the ideal $I = R(x^2 + x + 1)$ of R. Show that the quotient ring R/I has four elements [Hint: division algorithm!], and write down the addition and multiplication table for R/I. Deduce that R/I is a field.

6. (A) Let S be any set and let $R = \mathcal{P}(S)$ be the ring from Exercise Sheet 1. Let I be the collection of all the finite subsets of S. Show that I is an ideal of R.

The course website is: `http://people.bath.ac.uk/ac886/teaching/algebra2B/`

Solutions 2

1. (1) The subset $\{-1,0,1\} \subset \mathbb{Z}$ is not a subring and therefore not an ideal, because $1+1 \notin \{-1,0,1\}$.

(2) The subset $\{a_0 + a_2x^2 + a_4x^4 + \cdots \mid a_i \in \mathbb{Q}\} \subset \mathbb{Q}[[x]]$ is not an ideal, because it's not closed under multiplication by $x \in \mathbb{Q}[[x]]$. However, it is a subring: it's non-empty because it contains 0; and given any two elements $f = \sum_i a_{2i}x^{2i}, g = \sum_i b_{2i}x^{2i}$ in this set, we have that

$$f - g = \sum_i (a_{2i} - b_{2i})x^{2i} \quad \text{and} \quad f \cdot g = \sum_i \Big(\sum_{2j+2k=i} a_{2j}b_{2k} \Big) x^i \in E$$

The former evidently lies in the set, and the latter must also lie in the set precisely because each index i satisfying $i = 2j + 2k$ is even.

(3) The subset $\{a_2x^2 + a_3x^3 + a_4x^4 + \cdots \mid a_i \in \mathbb{Q}\} \subset \mathbb{Q}[[x]]$ is an ideal. In fact, it's the ideal in $\mathbb{Q}[[x]]$ generated by x^2, i.e., it's the subset of all elements in $\mathbb{Q}[[x]]$ of the form $f \cdot x^2$ for some $f \in \mathbb{Q}[[x]]$.

(4) The subset of polynomials of degree at most 2 is not a subring, because $x^2 \cdot x^2$ does not have degree at most 2.

(5) The subset $\{p \in \mathbb{Q}[x] \mid p(1) = 0\} \subset \mathbb{Q}[x]$ is the ideal generated by $(x-1) \in \mathbb{Q}[x]$. Indeed, the division algorithm tells us that 1 is a root of a polynomial if and only if $(x-1)$ is a factor.

2. You could prove this directly, but it's simpler to use the exercise from Sheet 1 which shows that $R[[x]]$ is an integral domain when R is. The result follows from Lemma 1.20 in the notes, because in this case the multiplicative identity of $R[[x]]$ is the power series $1 + 0x + 0x^2 + \cdots$ which clearly lies in $R[x]$.

3. (1) We first establish the given properties. Let $a, b \in [0]$, that is, $a \sim 0$ and $b \sim 0$. Since $\sim$ is a congruence, we have

$$-b = -b + 0 \sim -b + b = 0.$$

Since $\sim$ is a congruence it follows that $a - b = a + (-b) \sim 0 + 0 = 0$, so $a - b \in [0]$. For $r \in R$ and $a \in [0]$, we have $r \cdot a \sim r \cdot 0 = 0$ and $a \cdot r \sim 0 \cdot r = 0$, so $ra, ar \in [0]$ as required.

(2) Suppose that $a, b \in R$ satisfy $a \sim b$. Since $\sim$ is a congruence, we have

$$a - b = a + (-b) \sim b + (-b) = 0,$$

and thus $a - b \in [0]$. Conversely if $a - b \in [0]$ then $a - b = a + (-b) \sim 0$ and hence

$$a = a + (-b + b) \sim (a - b) + b \sim 0 + b = b$$

which shows that $a \sim b$.

(3) For $a, b \in R$, we have $b \in [a]$ if and only if $b \sim a$ if and only if $b - a \in [0]$ if and only if $b \in a + [0]$. Hence $[a] = a + [0]$.

4. (1) Let $p = u + a_1x + a_2x^2 + \cdots \in R[[x]]$. The goal is to find $q = b_0 + b_1x + b_2x^2 + \cdots \in R[[x]]$ such that

$$\begin{aligned} 1 + 0x + 0x^2 + 0x^3 + \cdots &= p \cdot q \\ &= (u + a_1x + a_2x^2 + \cdots) \cdot (b_0 + b_1x + b_2x^2 + b_3x^3 + \cdots) \\ &= \sum_i \Big(ub_i + a_1b_{i-1} + a_2b_{i-2} + \cdots + a_ib_0 \Big) x^i. \end{aligned}$$

This is a system of simultaneous equations

$$\begin{aligned} 1 &= ub_0 \\ 0 &= ub_1 + a_1 b_0 \\ 0 &= ub_2 + a_1 b_1 + a_2 b_0 \\ &\vdots \\ 0 &= ub_i + a_1 b_{i-1} + a_2 b_{i-2} + \cdots + a_i b_0 \\ &\vdots \end{aligned}$$

which has a solution: $b_0 = u^{-1}$, $b_1 = u^{-1}(-a_1 b_0)$, and in general once we have solved for $b_0, b_1, \ldots, b_{i-1}$ we can define

$$b_i = u^{-1} \cdot \big(- a_1 b_{i-1} - a_2 b_{i-2} - \cdots - a_i b_0 \big).$$

(2) In $\mathbb{Z}[[x]]$, the inverse $q = b_0 + b_1 x + b_2 x^2 + \cdots \in \mathbb{Z}[[x]]$ satisfies $b_0 = -1, b_1 = -2, \cdots,, b_i = -2^i$, so the inverse of $-1 + 2x$ is

$$-1 + (-2)x + (-4)x^2 + (-8)x^3 + \cdots$$

5. Let f be an arbitrary polynomial in $\mathbb{Z}_2[x]$ using division by $x^2 + x + 1$ with remainder, we get

$$f = (x^2 + x + 1)g + a_1 x + a_0 \text{ with } a_0, a_1 \in \mathbb{Z}_2.$$

It follows that $f + I = a_1 x + a_0 + I$; equivalently, we have

$$[f] = [a_1 x + a_0].$$

This means that there are exactly 4 elements in R/I depending on the possible values of $a_0, a_1 \in \mathbb{Z}_2$, namely $[0], [1], [x]$ and $[1 + x]$. Before writing up the addition and multiplication tables, notice that.

$$\begin{aligned} [x]^2 &= [-x - 1] = [x + 1] \\ [x] \cdot [x + 1] &= [x^2 + x] = [x + 1 + x] = [1] \\ [x + 1]^2 &= [x^2 + 2x + 1] = [x + 1 + 1] = [x]. \end{aligned}$$

Thus the addition and multiplication tables are

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

and

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

From the multiplication table we see that R/I is a field because every nonzero element is a unit.

6. Firstly I is non-empty as $\emptyset \in I$ (!!). We then need to check the closure properties. Let $A, B \in I$ and let X be any subset of S. Then $A + B = A \cap \overline{B} \cup B \cap \overline{A} \subseteq A \cup B$ is a finite subset of S and thus lies in I. Also $A \cdot X = X \cdot A = A \cap X \subseteq A$ is finite and thus $A \cdot X \in I$. Hence all the closure properties hold and I is an ideal of R.