Steven Charlton
Group 4

(A) Excellent – very thorough! ☺

Algebra and Number Theory

A ring R is a non-empty set with two binary operations $+$ and $\bullet$ such that:

- with respect to $+$, R is an abelian group:
  - it has an identity element
  - inverses exist for all elements
  - associativity holds
  - commutativity holds.
- associativity holds with respect to $\bullet$
- $\bullet$ is distributive over $+$

3) Clearly R is a non-empty set; for example it contains the function $z : x \rightarrow 0$.

$+$ is a binary operation on R: for all $f, g \in R$ and $x \in X$, $f(x)$ and $g(x)$ are integers, and since $+_{\mathbb{Z}}$ is a binary operation on $\mathbb{Z}$, $f(x) + g(x)$ is an integer. So $(f+g)(x)$ is an integer for all $x \in X$, hence $f+g$ is a map from X to $\mathbb{Z}$, thus $f+g \in R$. ✓

$\bullet$ is, similarly, a binary operation on R: $f(x)$ and $g(x)$ are integers so $f(x) \bullet g(x)$ is an integer for all $x \in X$, thus $f \bullet g \in R$. ✓

So R is closed under both $+$ and $\bullet$ ✓

- $(R, +)$ is an abelian group:
  - R is closed under $+$, as shown above.
  - The identity function is $0_R : x \rightarrow 0$.
    Clearly $0_R \in R$, and satisfies, for all $f \in R$ and $x \in X$:

$$\begin{aligned}
(f + 0_R)(x) &= f(x) + 0_R(x) \\
&= f(x) + 0 \\
&= f(x) \\
&= 0 + f(x) \\
&= 0_R(x) + f(x) \\
&= (0_R + f)(x) \quad ✓
\end{aligned}$$

since 0 is the additive identity on $\mathbb{Z}$, and $0_R(x) = 0$ for all x. Since the equalities hold for all x the functions themselves are equal, hence for all $f \in R$:

$$f + 0_R = f = 0_R + f \quad ✓$$

So as the identity property requires, there exists $0_R \in R$ such that for all $f \in R$, $f + 0_R = f = 0_R + f$. ✓

— Inverses exist for all elements. For all $f \in R$, define $\text{inv} f : x \to -f(x)$, where $-a$ is the additive inverse of a in $\mathbb{Z}$, which is another integer. Then $\text{inv} f \in R$, and satisfies for all $f \in R$ and $x \in X$:

$$\begin{aligned}
(f + \text{inv} f)(x) &= f(x) + (\text{inv} f)(x) \\
&= f(x) + -f(x) \\
&= 0 \\
&= 0_R(x) \\
&= -f(x) + f(x) \\
&= (\text{inv} f)(x) + f(x) \\
&= (\text{inv} f + f)(x)
\end{aligned}$$

Since $-f(x)$ is the additive inverse of the integer $f(x)$, 0 is the additive identity on $\mathbb{Z}$, and $0_R(x) = 0$ for all x. Hence for all $f \in R$:

$$f + \text{inv} f = 0_R = \text{inv} f + f$$

So inverses exist for all $f \in R$, as required, and $\text{inv} f \in R$ is that inverse. ✓

— Associativity holds. For all $f, g, h \in R$ and $x \in X$:

$$\begin{aligned}
(f + (g + h))(x) &= f(x) + (g+h)(x) \\
&= f(x) + (g(x) + h(x)) \\
&= (f(x) + g(x)) + h(x) \\
&= (f + g)(x) + h(x) \\
&= ((f+g) + h)(x)
\end{aligned}$$ ✓

which follows from the associativity of $+$ on $\mathbb{Z}$. Hence for all $f, g, h \in R$:

$$f + (g + h) = (f + g) + h$$

and so associativity holds. ✓

— Commutativity holds. For all $f, g \in R$ and $x \in X$:

$$\begin{aligned}
(f + g)(x) &= f(x) + g(x) \\
&= g(x) + f(x)
\end{aligned}$$

Algebra and Number Theory

$$= (g+f)(x)$$

which follows from the commutativity of $+$ on $\mathbb{Z}$. Hence for all $f, g \in R$:

$$f+g = g+f$$

and commutativity holds.

— And so $(R, +)$ is a commutative group.

— Associativity holds with respect to $\circ$. For all $f, g, h \in R$ and $x \in X$:

$$\begin{aligned}(f\circ(g\circ h))(x) &= f(x)\circ(g\circ h)(x)\\ &= f(x)\circ(g(x)\circ h(x))\\ &= (f(x)\circ g(x))\circ h(x)\\ &= (f\circ g)(x)\circ h(x)\\ &= ((f\circ g)\circ h)(x)\end{aligned}$$

which follows from the associativity of $\circ$ on $\mathbb{Z}$. Hence for all $f, g, h \in R$:

$$f\circ(g\circ h) = (f\circ g)\circ h$$

and $\circ$ is associative.

— Distributivity of $\circ$ over $+$ holds. For all $f, g, h \in R$ and $x \in X$:

$$\begin{aligned}(f\circ(g+h))(x) &= f(x)\circ(g+h)(x)\\ &= f(x)\circ(g(x)+h(x))\\ &= f(x)\circ g(x) + f(x)\circ h(x)\\ &= (f\circ g)(x) + (f\circ h)(x)\\ &= (f\circ g + f\circ h)(x)\end{aligned}$$

, and

$$\begin{aligned}((g+h)\circ f)(x) &= (g+h)(x)\circ f(x)\\ &= (g(x)+h(x))\circ f(x)\\ &= g(x)\circ f(x) + h(x)\circ f(x)\\ &= (g\circ f)(x) + (h\circ f)(x)\\ &= (g\circ f + h\circ f)(x)\end{aligned}$$

good

which follows from the distributivity of $\circ$ over $+$ on $\mathbb{Z}$. So for all $f, g, h \in R$:

$$f \circ (g+h) = f \circ g + f \circ h, \quad \text{and}$$
$$(g+h) \circ f = g \circ f + h \circ f$$

and distributivity holds.

— So all the required properties for R to be a ring hold, so $(R, +, \circ)$ is indeed a ring. ✓

Steven Charlton
Group 4

Algebra and Number Theory

6) Since R is a ring it is non-empty, in fact it contains 0_R, the additive identity on R.

So $R[[X]]$ is also non-empty, it contains for example:

$$z(X) = \sum_{i=0}^{\infty} 0_R X^i$$

Let:

$$f(X) = \sum_{i=0}^{\infty} a_i X^i$$
$$g(X) = \sum_{i=0}^{\infty} b_i X^i$$
$$h(X) = \sum_{i=0}^{\infty} c_i X^i$$

with $a_i, b_i, c_i \in R$ for all i, be elements of $R[[X]]$.

Then $+$ and $\bullet$ on $R[[X]]$ are defined, as on $R[X]$, by:

$$f(X) + g(X) = \sum_{i=0}^{\infty} (a_i + b_i) X^i$$
$$f(X) \bullet g(X) = \sum_{i=0}^{\infty} \left(\sum_{j=0}^{i} a_j b_{i-j}\right) X^i$$

— Since $a_i, b_i \in R$ and R is a ring, then $a_i + b_i \in R$, and $a_j b_{i-j} \in R$, so $\sum_{j=0}^{i} a_j b_{i-j} \in R$, hence both $f(X) + g(X)$ and $f(X) \bullet g(X)$ are elements of $R[[X]]$. So $+$ and $\bullet$ are binary operations and $R[[X]]$ is closed under them. ✓

— $(R[[X]], +)$ is an abelian group:

— $0_{R[[X]]}(X) = \sum_{i=0}^{\infty} 0_R X^i$ is the identity element in $R[[X]]$. ✓

Clearly $0_{R[[X]]}(X) \in R[[X]]$ since $0_R \in R$ is the identity under $+$ on R, and $0_{R[[X]]}(X)$ satisfies:

$$\begin{aligned} 0_{R[[X]]}(X) + f(X) &= \sum_{i=0}^{\infty} (0_R + a_i) X^i \\ &= \sum_{i=0}^{\infty} a_i X^i \\ &= f(X) \\ &= \sum_{i=0}^{\infty} (a_i + 0_R) X^i \\ &= f(X) + 0_{R[[X]]}(X) \end{aligned}$$

as required, since $0_R + a_i = a_i = a_i + 0_R$ on R. ✓

— Inverses exist; define $\operatorname{inv} f(X) = \sum_{i=0}^{\infty} \operatorname{inv} a_i X^i$, where $\operatorname{inv} a_i$ is the additive inverse of a_i in R. Since R is a ring $\operatorname{inv} a_i \in R$, so $\operatorname{inv} f(X) \in R[[X]]$ for any $f(X) \in R[[X]]$ and this satisfies:

$$
\begin{aligned}
f(X) + \operatorname{inv} f(X) &= \Sigma_{i=0}^{\infty} (a_i + \operatorname{inv} a_i) X^i \\
&= \Sigma_{i=0}^{\infty} 0_R X^i \\
&= 0_{R[[X]]}(X) \\
&= \Sigma_{i=0}^{\infty} (\operatorname{inv} a_i + a_i) X^i \\
&= \operatorname{inv} f(X) + f(X)
\end{aligned}
$$

as required, since $a_i + \operatorname{inv} a_i = 0_R = \operatorname{inv} a_i + a_i$ on R. So any $f(X) \in R[[X]]$ has an inverse $\operatorname{inv} f(X) \in R[[X]]$ as required. ✓

— Associativity holds:

$$
\begin{aligned}
f(X) + (g(X) + h(X)) &= \Sigma_{i=0}^{\infty} a_i X^i + \Sigma_{i=0}^{\infty} (b_i + c_i) X^i \\
&= \Sigma_{i=0}^{\infty} (a_i + (b_i + c_i)) X^i \\
&= \Sigma_{i=0}^{\infty} ((a_i + b_i) + c_i) X^i \\
&= \Sigma_{i=0}^{\infty} (a_i + b_i) X^i + \Sigma_{i=0}^{\infty} c_i X^i \\
&= (f(X) + g(X)) + h(X)
\end{aligned}
$$

which follows from the associativity of $+$ on R. ✓

— Commutativity holds:

$$
\begin{aligned}
f(X) + g(X) &= \Sigma_{i=0}^{\infty} (a_i + b_i) X^i \\
&= \Sigma_{i=0}^{\infty} (b_i + a_i) X^i \\
&= g(X) + f(X)
\end{aligned}
$$

which follows from the commutativity of $+$ on R. ✓

— So $(R[[X]], +)$ is a commutative group. ✓

— Associativity holds with respect to $\bullet$ on $R[[X]]$:

$$
f(X) \bullet (g(X) \bullet h(X)) = (\Sigma_{i=0}^{\infty} a_i X^i) \bullet (\Sigma_{i=0}^{\infty} (\Sigma_{j=0}^{i} b_j c_{i-j}) X^i)
$$

Put $x_i = \Sigma_{j=0}^{i} b_j c_{i-j}$

$$
\begin{aligned}
&= (\Sigma_{i=0}^{\infty} a_i X^i) \bullet (\Sigma_{i=0}^{\infty} x_i X^i) \\
&= \Sigma_{i=0}^{\infty} (\Sigma_{j=0}^{i} a_j x_{i-j}) X^i
\end{aligned}
$$

But $x_{i-j} = \Sigma_{k=0}^{i-j} b_k c_{i-j-k}$

$$
= \Sigma_{i=0}^{\infty} (\Sigma_{j=0}^{i} a_j (\Sigma_{k=0}^{i-j} b_k c_{i-j-k})) X^i
$$

On R $\bullet$ distributes over $+$, and is associati

Algebra and Number Theory

$$= \sum_{i=0}^{\infty} \underbrace{\left(\sum_{j=0}^{i} \sum_{k=0}^{i-j} a_j b_k c_{i-j-k} \right)} X^i$$

This is a sum over all terms like $a_x b_y c_z$ where the indices are non-negative and sum to i.

$$= \sum_{i=0}^{\infty} \left(\sum_{\substack{x+y+z=i \\ x,y,z \geq 0}} a_x b_y c_z \right) X^i$$ ✓ good

While:

$$(f(X) \circ g(X)) \circ h(X) = \left(\sum_{i=0}^{\infty} \left(\sum_{j=0}^{i} a_j b_{i-j} \right) X^i \right) \circ \left(\sum_{i=0}^{\infty} c_i X^i \right)$$
$$= \sum_{i=0}^{\infty} \left(\sum_{j=0}^{i} \left(\sum_{k=0}^{j} a_k b_{j-k} \right) c_{i-j} \right) X^i$$

On R $\circ$ distributes over $+$, and is associative

$$= \sum_{i=0}^{\infty} \underbrace{\left(\sum_{j=0}^{i} \sum_{k=0}^{j} a_k b_{j-k} c_{i-j} \right)} X^i$$

Indices sum to i

$$= \sum_{i=0}^{\infty} \left(\sum_{\substack{x+y+z=i \\ x,y,z \geq 0}} a_x b_y c_z \right) X^i$$ ✓

As before, so: $f(X) \circ (g(X) \circ h(X)) = (f(X) \circ g(X)) \circ h(X)$, and $\circ$ on $R[[X]]$ is associative. ✓

— Distributivity of $\circ$ over $+$ holds:

$$f(X) \circ (g(X) + h(X)) = \left(\sum_{i=0}^{\infty} a_i X^i \right) \circ \left(\sum_{i=0}^{\infty} (b_i + c_i) X^i \right)$$
$$= \sum_{i=0}^{\infty} \left(\sum_{j=0}^{i} a_j (b_{i-j} + c_{i-j}) \right) X^i$$

On R $\circ$ distributes over $+$.

$$= \sum_{i=0}^{\infty} \left(\sum_{j=0}^{i} (a_j b_{i-j} + a_j c_{i-j}) \right) X^i$$
$$= \sum_{i=0}^{\infty} \left(\sum_{j=0}^{i} a_j b_{i-j} + \sum_{j=0}^{i} a_j c_{i-j} \right) X^i$$
$$= \sum_{i=0}^{\infty} \left(\sum_{j=0}^{i} a_j b_{i-j} \right) X^i + \sum_{i=0}^{\infty} \left(\sum_{j=0}^{i} a_j c_{i-j} \right) X^i$$
$$= f(X) \circ g(X) + f(X) \circ h(X)$$

$$(g(X) + h(X)) \circ f(X) = \left(\sum_{i=0}^{\infty} (b_i + c_i) X^i \right) \circ \left(\sum_{i=0}^{\infty} a_i X^i \right)$$
$$= \sum_{i=0}^{\infty} \left(\sum_{j=0}^{i} (b_j + c_j) a_{i-j} \right) X^i$$
$$= \sum_{i=0}^{\infty} \left(\sum_{j=0}^{i} (b_j a_{i-j} + c_j a_{i-j}) \right) X^i$$
$$= \sum_{i=0}^{\infty} \left(\sum_{j=0}^{i} b_j a_{i-j} + \sum_{j=0}^{i} c_j a_{i-j} \right) X^i$$
$$= \sum_{i=0}^{\infty} \left(\sum_{j=0}^{i} b_j a_{i-j} \right) X^i + \sum_{i=0}^{\infty} \left(\sum_{j=0}^{i} c_j a_{i-j} \right) X^i$$
$$= g(X) \circ f(X) + h(X) \circ f(X)$$

✓

which follows from distributivity on R, so distributivity holds.

— All the criteria are met so $(R[[X]], +, \bullet)$ is a ring. ✓

Now $R[X]$ is the subset of $R[[X]]$ which contains elements which have only finitely many non-zero coefficients.

To show $R[X]$ is a subring, we need: $R[X]$ is non-empty; it is closed under addition and multiplication; it contains the identity; and inverses exist in $R[X]$ for all elements in $R[X]$.

Clearly $R[X]$ is non-empty, it contains $0_{R[[X]]}(x)$, the identity, since this has no non-zero coefficients.

Let $f(x) \in R[X]$ with $a_i = 0_R$ for $i \geq N$ since it has finitely many non-zero coefficients. And $g(x) \in R[X]$ with $b_i = 0_R$ for $i \geq M$.

Let $h(x) = f(x) + g(x)$ so $c_i = a_i + b_i$, then for $i \geq \max(N, M)$ $c_i = 0_R + 0_R = 0_R$, so $h(x)$ has finitely many non-zero coefficients, $h(x) \in R[X]$, and $R[X]$ is closed under addition. ✓

Let $h(x) = f(x) \circ g(x)$ so $c_i = \sum_{j=0}^{i} a_j b_{i-j}$. If $c_i \neq 0_R$ $\Rightarrow a_j b_{i-j} \neq 0_R$ for some $0 \leq j \leq i$. So $a_j \neq 0_R$ and $b_{i-j} \neq 0_R$ since $0_R \cdot x = 0_R = x \cdot 0_R$ $\forall x \in R$, so $j < N$ and $i - j < M \Rightarrow i - j + j = i < N + M$. Hence for $i \geq N + M$ $c_i = 0$ and $h(x)$ has finitely many non-zero coefficients, $h(x) \in R[X]$, and $R[X]$ is closed under multiplication ✓

Inverses exist in $R[X]$. Let $h(x) = \mathrm{inv}\, f(x)$ ✓, so $c_i = \mathrm{inv}\, a_i$. For $i \geq N$, $c_i = \mathrm{inv}\, 0_R = 0_R$, so $h(x)$ has finitely many non-zero coefficients so is in $R[X]$, hence all elements in $R[X]$ have inverses in $R[X]$ ✓

And so $R[X]$ is indeed a subring of $R[[X]]$. ✓

Well done!