David Owen Horace Cutler Math 146: Homework 1 February 2, 2024

Exercise 1. Let R be a ring with at least two elements. Let $0 = 0_R$ be the additive identity and $1 = 1_R$ be the multiplicative identity. For any $x \in R$, let $-x$ denote its additive inverse.

(a) Prove that $0 \neq 1$.

(b) Prove that $(-a) \cdot b = -(a \cdot b)$ and $a \cdot (-b) = -(a \cdot b)$ for any $a, b \in R$.

Solution: *Proof.* We consider (a) first. For the sake of contradiction, say $0 = 1$. Recall as proved in class that we have the following:

$$(0 \cdot a) = (a \cdot 0) = 0, \, \forall a \in R$$

Let $a \in R$ such that $a \neq 0, a \neq 1$. This element exists as we stipulated R have at least two elements, and $0 = 1$. Then the following holds:

$$\begin{aligned} 0 &= 1 \\ \to a \cdot 0 &= a \cdot 1 \\ \to 0 &= a \end{aligned} \tag{1}$$

But this is an obvious contradiction, and so it cannot be that $0 \neq 1$.

Consider (b) then. Let $a, b \in R$, we want first to prove that $(-a) \cdot b = -(a \cdot b)$, which is exactly that $a \cdot b + (-a) \cdot b = 0$. For this, note the following chain of equivalencies, largely by the distributive property:

$$\begin{aligned} a \cdot b + (-a) \cdot b &= 0 \\ \Leftrightarrow (a - a) \cdot b &= 0 \\ \Leftrightarrow 0 \cdot b &= 0 \end{aligned} \tag{2}$$

We then move to prove $a \cdot (-b) = -(a \cdot b)$, which is in this case that $a \cdot b + a \cdot (-b) = 0$. A similar argument follows:

$$\begin{aligned} a \cdot b + a \cdot (-b) &= 0 \\ \Leftrightarrow a \cdot (b - b) &= 0 \\ \Leftrightarrow a \cdot 0 &= 0 \end{aligned} \tag{3}$$

Thus, using our earlier remark, (b) holds. □

Exercise 2. Let $\mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\}$ and $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$, where i denotes the squareroot of -1.

(a) Prove that $\mathbb{Q}(i)$ and $\mathbb{Z}[i]$ are rings.

(b) Prove that $\mathbb{Q}(i)$.

(c) Prove that $\mathbb{Z}[i]$ is an integral domain.

Solution: *Proof.* We consider (a) first. For both of these candidate rings, we define the operations in the natural way, i.e the following:

$$\begin{aligned}(a+bi)+(c+di) &= (a+c)+(b+d)i \\ (a+bi)\times(c+di) &= (ac-bd)+(bc+ad)i\end{aligned} \tag{4}$$

Note both of these expressions define binary operations (in particular we have closure under this operation), as both $\mathbb{Z}$ and $\mathbb{Q}$ are closed under addition.

We move to prove $\mathbb{Q}(i)$ and $\mathbb{Z}[i]$ are rings then. For simplicity of demonstration, for each property I verify for both rings, I will only write one proof.

This is as all the properties I use will be true in both $\mathbb{Q}$ and $\mathbb{Z}$ (and so the proofs would be exactly identical, except for imagining the variables to integers instead of rational numbers, and vice versa).

We first verify both have abelian group structures under addition:

1. *(Commutativity of Addition)* We just use the commutativity of addition on $\mathbb{Z}$ and $\mathbb{Q}$:

$$(a+bi)+(c+di) = (a+c)+(b+d)i = (c+a)+(d+b)i = (c+di)+(a+bi) \tag{5}$$

2. *(Associativity of Addition)* We similarly use the associativity of addition on $\mathbb{Z}$ and $\mathbb{Q}$:

$$\begin{aligned}&((a+bi)+(c+di))+(e+fi)\\ &=((a+c)+(b+d)i)+(e+fi)\\ &=((a+c)+e)+((b+d)+f)i\\ &=(a+(c+e))+(b+(d+f))i\\ &=(a+bi)+((c+e)+(d+f)i)\\ &=(a+bi)+((c+di)+(e+fi))\end{aligned} \tag{6}$$

3. *(Existence of an Additive Identity)* We just take the additive identity in $\mathbb{Z}$ or $\mathbb{Q}$ and consider $0+0i$, we need only one direction as we verified commutativity:

$$(a+bi)+(0+0i) = (a+0)+(b+0)i = a+bi \tag{7}$$

4. *(Existence of Additive Inverses)* One predicts that we just levee additive inverses from $\mathbb{Z}$ and $\mathbb{Q}$. We only need one direction as we verified commutativity.

$$(a+bi)+(-a-bi) = (a-a)+(b-b)i = 0+0i \tag{8}$$

These factors together gives us our desired abelian group structure under addition. We move then to verify monoid structure under multiplication:

1. *(Associativity of Multiplication)* We can show this using distributivity and commutativity for $\mathbb{Z}$ or $\mathbb{Q}$.

$$\begin{aligned}
&((a+bi)\times(c+di))\times(e+fi)\\
&=((ac-bd)+(cb+ad)i)\times(e+fi)\\
&=((ac-bd)e-(cb+ad)f)+((cb+ad)e+(ac-bd)f)i\\
&=(ace-bde-cbf-adf)+(cbe+ade+acf-bdf)i\\
&=(ace-adf-bcf-bde)+(bce-bdf+acf+ade)i\\
&=(a+bi)\times((ce-df)+(cf+de)i)\\
&=(a+bi)\times((c+di)\times(e+fi))
\end{aligned} \tag{9}$$

2. *(Existence of a Multiplicative Identity)* We take just the additive identity 1 from $\mathbb{Q}$ or $\mathbb{Z}$ and claim that $1+0i$ is the identity:

$$(a+bi)\times(1+0i)=(a-b(0))+(b+a(0))i=a+bi \tag{10}$$

   I prove only one direction, as I will verify in the following part (showing $\mathbb{Q}(i)$ is a field) that this multiplication is commutative.

We just show the last criteria then, that the operations cooperate with respect to distribution.

1. *(Distributivity of Multiplication over Addition)* We use commutativity and distributivity from $\mathbb{Z}$ and $\mathbb{Q}$.

$$\begin{aligned}
&(a+bi)\times((c+di)+(e+fi))\\
&=(a+bi)\times((c+e)+(d+f)i)\\
&=(a(c+e)-b(d+f))+(b(c+e)+a(d+f))i\\
&=(ac+ae-bd-bf)+(bc+be+ad+af)i\\
&=(ac-bd+ae-bf)+(bc+ad+be+af)i\\
&=((ac-bd)+(bc+ad)i)+((ae-bf)+(be+af)i)\\
&=((a+bi)\times(c+di))+((a+bi)\times(e+fi))
\end{aligned} \tag{11}$$

I only prove one direction here as I show commutative multiplication in the next part. Thus, with all of these axioms verified, both $\mathbb{Z}[i]$ and $\mathbb{Q}(i)$ are rings.

We will now prove that $\mathbb{Q}(i)$ is a field, i.e. (b). For this, we need to ensure our multiplication is commutative and that all non-zero elements have inverses. Note here we already have $0\neq 1$ as a result of the previous part.

1. *(Commutativity of Multiplication)* We apply the commutativity of addition and multiplication in $\mathbb{Q}$.

$$\begin{aligned}
&(a+bi)\times(c+di)\\
&=(ac-bd)+(bc+ad)i\\
&=(ca-db)+(da+cb)i\\
&=(c+di)\times(a+bi)
\end{aligned} \tag{12}$$

2. *(Existence of Multiplicative Inverses)* Consider $a+bi$ such that $a \neq 0$ or $b \neq 0$. Then the numbers $\frac{a}{a^2+b^2}$ and $\frac{b}{a^2+b^2}$ are defined.

   Moreover, they are rational numbers (as the rationals are closed under these operations; this is why we couldn't make $\mathbb{Z}[i]$ a field). We show a multiplicative exists inverse as follows, using commutativity in $\mathbb{Q}$:

$$\begin{aligned}
&(a+bi) \times \Big(\frac{a}{a^2+b^2} + \frac{-b}{a^2+b^2}i\Big) \\
&= \Big(\frac{a^2}{a^2+b^2} + \frac{b^2}{a^2+b^2}\Big) + \Big(\frac{ba}{a^2+b^2} - \frac{ab}{a^2+b^2}\Big) \\
&= 1 + 0i
\end{aligned} \tag{13}$$

   As we showed commutativity, this one direction shows inverses exists.

   We just need to show (c) then, i.e. $\mathbb{Z}[i]$ is an integral domain. Remark for this sake that our proof of commutativity in $\mathbb{Q}(i)$ applies here, so we just need to show that $(a+bi) \times (c+di) = 0+0i \to a+bi = 0+0i$ or $c+di = 0+0i$:

3. *(Integral Domain Condition)* Suppose that we have $(a+bi) \times (c+di) = 0+0i$, then that is exactly that:

$$(ac-bd) + (bc+ad)i = 0+0i$$

   So it must be that $ac-bd = 0$ and $bc+ad = 0$. Thus $(ac-bd)^2 = a^2c^2+b^2d^2-2acbd = 0$ and $(bc+ad)^2 = b^2c^2+a^2d^2+2acbd = 0$. Summing yields the following:

$$\begin{aligned}
a^2d^2 + a^2c^2 + b^2d^2 + b^2c^2 &= 0 \\
\to a^2(d^2+c^2) + b^2(d^2+c^2) &= 0 \\
\to (a^2+b^2)(d^2+c^2) &= 0
\end{aligned} \tag{14}$$

   Then, using the fact that $\mathbb{Z}$ is an integral domain, it is either that $a^2+b^2 = 0$ or d^2+c^2. In the former case, it must be $a, b = 0$. In the latter, it is that $c, d = 0$.

   In particular, this has that $a+bi = 0+0i$ or $c+di = 0+0i$, which has that the integral domain condition holds. As $\mathbb{Z}[i]$ is then additionally commutative, it is an integral domain.

□

Exercise 3. Let A be an abelian group. An *endomorphism* of A is a group homomorphism $\phi : A \to A$.

Let $\mathrm{End}(A)$ denote the set of all endomorphisms of A.

(a) Prove that if $\phi_1, \phi_2 \in \text{End}(A)$, then the function $\phi_1 + \phi_2 : A \to A$ defined by $(\phi_1 + \phi_2)(a) = \phi_1(a) + \phi_2(a)$ is also in $\text{End}(A)$. That is, prove that $\phi_1 + \phi_2$ is a homomorphism.

Proof. Consider some $a, b \in A$. Then, using that ϕ_1 and ϕ_2 are homomorphisms and commutativity:

$$\begin{aligned}(\phi_1 + \phi_2)(a + b) = \phi_1(a + b) + \phi_2(a + b) = \phi_1(a) + \phi_2(a) + \phi_1(b) + \phi_2(b) \\ = (\phi_1 + \phi_2)(a) + (\phi_1 + \phi_2)(b)\end{aligned} \tag{15}$$

So $\phi_1 + \phi$ is a homomorphism, and thus also in $\text{End}(A)$. □

(b) Prove that if $\phi_1, \phi_2 \in \text{End}(A)$, then the function $\phi_1 \circ \phi_2 : A \to A$ defined by $(\phi_1 \circ \phi_2)(a) = \phi_1(\phi_2(a))$ is also in $\text{End}(A)$.

Proof. Again, this is tantamount to show that the defined function is a homomorphism. For this sake, let $a, b \in A$ and consider the following:

$$\begin{aligned}(\phi_1 \circ \phi_2)(a + b) = \phi_1(\phi_2(a + b)) = \phi_1(\phi_2(a) + \phi_2(b)) \\ = \phi_1(\phi_2(a)) + \phi_1(\phi_2(b)) = (\phi_1 \circ \phi_2)(a) + (\phi_1 \circ \phi_2)(b)\end{aligned} \tag{16}$$

□

(c) Prove that $\text{End}(A)$ is a ring with the given operations.

Proof. We will verify each operation by hand.

(a) *(Commutativity of Addition)* Let $\phi_1, \phi_2 \in \text{End}(A)$ and $a \in A$. Then, using commutativity in A:

$$\begin{aligned}(\phi_1 + \phi_2)(a) = \phi_1(a) + \phi_2(a) \\ = \phi_2(a) + \phi_1(a) = (\phi_2 + \phi_1)(a)\end{aligned} \tag{17}$$

(b) *(Associativity of Addition)* Here we just use the associativity of A.

$$\begin{aligned}((\phi_1 + \phi_2) + \phi_3)(a) = (\phi_1 + \phi_2)(a) + \phi_3(a) = \phi_1(a) + \phi_2(a) + \phi_3(a) \\ = \phi_1(a) + (\phi_2 + \phi_3)(a) = (\phi_1 + (\phi_2 + \phi_3))(a)\end{aligned} \tag{18}$$

(c) *(Existence of an Additive Identity)* Recall the zero homomorphism $0_A : A \to A$ defined by $0_A(a) = 0_A$ for $0 \in A$. Trivially, this is an endomorphism.

We claim is is in fact the additive identity:

$$(0_A + \phi_1)(a) = 0_A(a) + \phi_1(a) = 0_A + \phi_1(a) = \phi_1(a) \tag{19}$$

As we already have commutativity, this shows the existence on an inverse.

(d) *(Existence of Additive Inverses)* Given some endomorphism ϕ, we consider the mapping $\tau : A \to A$ given by $\tau(a) = -\phi(a)$, i.e. the additive inverse of $\phi(a)$ in A.

We check first this is an endomorphism by showing it is a homomorphism:

$$\begin{aligned} \tau(a+b) = -\phi(a+b) = -(\phi(a) + \phi(b)) = \\ -\phi(a) - \phi(b) = \tau(a) + \tau(b) \end{aligned} \tag{20}$$

So $\tau \in \mathrm{End}(A)$, so we just check it fulfills the definition of an additive inverse:

$$\begin{aligned} (\phi + \tau)(a) = \phi(a) + \tau(a) = \phi(a) - \phi(a) \\ = 0_A = 0_A(a) \end{aligned} \tag{21}$$

As we already showed commutativity, one direction suffices. We move now to check it has a monoid structure under multiplication.

(e) *(Associativity of Multiplication)* For this, simply note the following:

$$\begin{aligned} ((\phi_1 \circ \phi_2) \circ \phi_3)(a) = (\phi_1 \circ \phi_2)(\phi_3(a)) \\ = \phi_1(\phi_2(\phi_3(a))) = \phi((\phi_2 \circ \phi_3)(a)) \\ = (\phi \circ (\phi_2 \circ \phi_3))(a) \end{aligned} \tag{22}$$

(f) *(Existence of an Multiplicative Identity)* Consider the mapping $\mathbb{1} : A \to A$ given by $\mathbb{1}(a) = a$.

We first check $\mathbb{1} \in \mathrm{End}(A)$ by verifying it is a homomorphism:

$$\mathbb{1}(a+b) = a + b = \mathbb{1}(a) + \mathbb{1}(b) \tag{23}$$

And then we check this is the desired multiplicative identity:

$$\begin{aligned} (\phi \circ \mathbb{1})(a) = \phi(\mathbb{1}(a)) = \phi(a) \\ (\mathbb{1} \circ \phi)(a) = \mathbb{1}(\phi(a)) = \phi(a) \end{aligned} \tag{24}$$

And thus we have a multiplicative identity.

(g) *(Distributivity of Multiplication over Addition)* We just use the fact we are dealing with homomorphisms.

$$\begin{aligned} (\phi_1 \circ (\phi_2 + \phi_3))(a) = \phi_1((\phi_2 + \phi_3)(a)) \\ = \phi_1(\phi_2(a) + \phi_3(a)) = \phi_1(\phi_2(a)) + \phi_1(\phi_3(a)) \\ = (\phi_1 \circ \phi_2)(a) + (\phi_1 \circ \phi_3)(a) \\ = ((\phi_1 \circ \phi_2) + (\phi_1 \circ \phi_3))(a) \end{aligned} \tag{25}$$

This verifies left distributivity, where the proof for right distributivity is essentially the exact same.

All these facts taken together have that $\mathrm{End}(A)$ is a ring. □

(d) Find End($\mathbb{Z}$) and End($\mathbb{Q}$).

Proof. We claim that End($\mathbb{Z}$) $\cong \mathbb{Z}$ and End($\mathbb{Q}$) $\cong \mathbb{Q}$.

We start with End($\mathbb{Z}$) $\cong \mathbb{Z}$. For this sake, we define a mapping $\phi : \mathbb{Z} \to \text{End}(\mathbb{Z})$ by $n \mapsto nx$ (i.e. $n \in \mathbb{Z}$ maps to the function defined by nx for $x \in \mathbb{Z}$).

We verify first this mapping sends integers to homomorphisms, i.e. $nx : A \to A$ is an endomorphism. This is obvious though, as:

$$n(x+y) = nx + ny$$

We need to show ϕ is a ring homomorphism then. For this, we just note the following arguments:

$$\begin{aligned} (\phi(n+m))(x) &= (\phi(n) + \phi(m))(x) \\ &\Leftrightarrow (n+m)x = nx + mx \\ &\Leftrightarrow (n+m)x = (n+m)x \end{aligned} \tag{26}$$

$$\begin{aligned} (\phi(nm))(x) &= (\phi(n) \circ \phi(m))(x) \\ (nm)x &= n(mx) \\ (nm)x &= nm(x) \end{aligned}$$

We want to verify then that ϕ is injective, which is tantoument to showing its kernel is just the additive identity of $\mathbb{Z}$.

This is obvious however, as we can tell no other element besides 0 will be sent to the zero homomorphism as $n(1) \neq 0$ unless n is zero, that is $\phi(n)$ is not the zero homomorphism unless $n = 0$.

Last, we verify surjectivity. For this sake, let φ be an endomorphism of $\mathbb{Z}$, and consider $\varphi(1)$. We claim for $x \in \mathbb{Z}$:

$$\varphi(x) = x\varphi(1)$$

This is easily shown using the properties of the homomorphism (and, more abstractly, how addition and multiplication "relate" in $\mathbb{Z}$):

$$\varphi\Big(\sum_{i=1}^{x} 1\Big) = \sum_{i=1}^{x} \phi(1) = x\varphi(1) \tag{27}$$

Note here I sort of implicitly assumed $x \geq 0$, but one recovers the proof by considering sums of -1 to $|x|$ in the general case (particularly because $\varphi(-a) = -\varphi(a)$).

With this shown then, it holds that with $n = \varphi(1)$, ϕ maps n to this endomorphism. Thus we have surjectivity, and so End($\mathbb{Z}$) $\cong \mathbb{Z}$.

Note then that this construction works exactly the same for $\mathbb{Q}$; the only thing that

changes at all is the surjectivity argument (note here the mapping we are using is $\frac{p}{q} \mapsto \frac{p}{q}x$). With this in mind, we claim for $\frac{p}{q} \in \mathbb{Q}$ given some $\varphi \in \text{End}(\mathbb{Q})$ that:

$$\varphi\Big(\frac{p}{q}\Big) = \frac{p}{q}\varphi(1)$$

For this, we note:

$$\varphi(1) = \varphi\Big(q\frac{1}{q}\Big) = \varphi\Big(\sum_{i=1}^{q}\frac{1}{q}\Big) = \sum_{i=1}^{q}\varphi\Big(\frac{1}{q}\Big) = q\varphi\Big(\frac{1}{q}\Big) \tag{28}$$

Which consequently has:

$$\varphi\Big(\frac{p}{q}\Big) = \varphi\Big(\sum_{i=1}^{p}\frac{1}{q}\Big) = \sum_{i=1}^{p}\varphi\Big(\frac{1}{q}\Big) = \sum_{i=1}^{p}\frac{\varphi(1)}{q} = \frac{p}{q}\varphi(1) \tag{29}$$

Using the same argument we presented with the integers then, given $\varphi(1)$ is a rational number, this shows $\varphi(1)$ maps to this φ. Thus it is surjective, and so we have $\text{End}(\mathbb{Q}) \cong \mathbb{Q}$.

Note again here I tacitly assumed $\frac{p}{q} > 0$, but one saves the general case using the tactic I outlined in showing $\text{End}(\mathbb{Z}) \cong \mathbb{Z}$. □

(e) Let $n \geq 2$ be an integer. Find $\text{End}(\mathbb{Z}^n)$.

Proof. We claim that $\text{End}(\mathbb{Z}^n) \cong M_{n\times n}(\mathbb{Z})$. Consider the mapping $\phi : M_{n\times n}(\mathbb{Z}) \to \text{End}(\mathbb{Z}^n)$ given by $M \mapsto Mx$ for $M \in M_{n\times n}(\mathbb{Z})$.

Again, our arguments in the previous part show that this mapping assigns matrices to homomorphisms and that this is a ring homomorphism.

This is because we only use distributivity when showing the analogous results for $\mathbb{Z}$ and $\mathbb{Q}$, so it holds for matrices (as matrix multiplication distributes).

Injectivity trivial follows from the fact that $Ax = Bx$ for $x \in \mathbb{Z}^n$ has $A = B$, so the only matrix that can be mapped to the zero homomorphism (which is multiplication by the zero matrix here) is the zero matrix.

In line with the previous parts then, the only interesting thing is surjectivity. For this sake, let $\varphi \in \text{End}(\mathbb{Z}^n)$. Let e_i denote the i-th unit vector; we consider the matrix M consisting of the column vectors given by $\varphi(e_i)$ for $1 \leq i \leq n$, i.e:

$$M = \begin{bmatrix} | & | & \dots & | \\ \varphi(e_1) & \varphi(e_2) & \dots & \varphi(e_n) \\ | & | & \dots & | \end{bmatrix} \tag{30}$$

Trivially, $M \in M_{n\times n}\mathbb{Z}$. We show then $Mx = \varphi(x)$ then:

$$Mx = \begin{bmatrix} | & | & \dots & | \\ \varphi(e_1) & \varphi(e_2) & \dots & \varphi(e_n) \\ | & | & \dots & | \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = x_1\varphi(e_1) + ... + x_n\varphi(e_n) \tag{31}$$

But obviously as well:

$$\varphi(x) = \varphi\Big(\sum_{i=1}^{n} x_i e_i\Big) = \sum_{i=i}^{n} x_i\varphi(e_i) \tag{32}$$

And so it holds. Note here technically we need linearity with respect to scalars, i.e. that $\varphi(cx) = c\varphi(x)$ for $c \in \mathbb{Z}, x \in \mathbb{Z}^n$, but as c is an integer in this case, it is simple (again, if $c < 0$, we just take sums of -1 to $|c|$ instead):

$$c\varphi(x) = \sum_{i=1}^{c} \varphi(x) = \varphi\Big(\sum_{i=1}^{c} x\Big) = \varphi(cx) \tag{33}$$

With this, (32) definitely holds. It follows $Mx = \varphi(x)$ for all x, and so M maps to φ under the defined mapping. Thus it is surjective, and it follows $\mathrm{End}(\mathbb{Z}^n) \cong M_{n\times n}(\mathbb{Z})$. □

Exercise 4. Let R a be a commutative ring.

(a) Let $f \in R[x]$ be a zero-divisor of degree n, i.e. $f = \sum_{i=0}^{n} a_i x^i$. Let $g \in R[x]$ such that $f \cdot g = 0$, and suppose g has at least degree 1. Let $h = a_n \cdot g$. Prove that $f \cdot h = 0$, and that either $h = 0$ or the degree of h is strictly less than the degree of g.

Proof. We write $g = \sum_{i=0}^{m} b_i x^i$. Recall from the definition of $f \cdot g$:

$$\begin{aligned} f \cdot g &= \sum_{l=0}^{n+m} \Big(\sum_{\substack{i+j=l \\ i,j\in\mathbb{N}}} a_i b_j \Big) x^l = 0 \\ \to \forall l \in \{0, ..., n+m\}, &\sum_{\substack{i+j=l \\ i,j\in\mathbb{N}}} a_i b_j = 0 \end{aligned} \tag{34}$$

Notice then that as $h = a_n \cdot g$, its coefficients are just those of g multiplied by a_n. In particular, we have:

$$f \cdot h = \sum_{l=0}^{n+m} \Big(\sum_{\substack{i+j=l \\ i,j\in\mathbb{N}}} a_i a_n b_j \Big) x^l \tag{35}$$

But then of course, for any l:

$$\sum_{\substack{i+j=l \\ i,j\in\mathbb{N}}} a_i a_n b_j = a_n \Big(\sum_{\substack{i+j=l \\ i,j\in\mathbb{N}}} a_i b_j \Big) = a_n(0) = 0 \tag{36}$$

□

So the coefficients of $f \cdot h$ are all zero, so $f \cdot h = 0$.

For the second aspect of the proof, note that for $l = n + m$, we have:

$$\sum_{\substack{i+j=l \\ i,j \in \mathbb{N}}} a_i b_j = a_n b_m \tag{37}$$

Again, as $f \cdot g = 0$, we know then that the left sum is equal to zero, so it must be $a_n b_m = 0$. But this is the first coefficient of h, so it either that outright $h = 0$ or at least that the m-th degree term is annihilated as its coefficient is zero.

In particular, this gives either $h = 0$ or that h is strictly less in degree than g (as g is degree m).

(b) Suppose that $h = 0$. Prove that either $a_{n-1} \cdot g = 0$ or that $a_{n-1} \cdot g$ has degree smaller than g and $f \cdot (a_{n-1} \cdot g) = 0$.

Proof. As $h = 0$, we have exactly that $a_n b_m, a_n b_{m-1}, ...a_n b_0 = 0$. We take $l = n+m-1$ in the product formula for $f \cdot g$ then, which yields the following:

$$\sum_{\substack{i+j=n+m-1 \\ i,j \in \mathbb{N}}} a_i b_j = a_{n-1} b_m + a_n b_{m-1} \tag{38}$$

As $f \cdot g = 0$ then, this sum must be zero, i.e. $a_{n-1} b_m + a_n b_{m-1} = 0$.

However, we already know that $a_n b_{m-1} = 0$ as $h = 0$. So it must be $a_{n-1} b_m = 0$.

By the exact same logic as the previous part then, it must either be that outright $a_{n-1} \cdot g = 0$, or at the very least the m-th degree term of $a_{n-1} \cdot g$ is annihilated, i.e. $a_{n-1} \cdot g$ has degree smaller than g.

Additionally, the argument given in (35) and (36) gives us that $f \cdot (a_{n-1} \cdot g) = 0$. □

(c) Iterating, show that either $a_i \cdot g = 0$ for every i or there exists a polynomial $g_n \neq 0$ of degree strictly smaller than g such that $f \cdot g_2 = 0$.

Proof. Consider some $1 \leq i \leq n$. Here, it is enough to demonstrate that assuming $a_i \cdot g, a_{i+1} \cdot g, ..., a_n \cdot g = 0$ has either $a_{i-1} \cdot g = 0$ or that $a_{i-1} \cdot g$ has strictly less degree than g with $f \cdot (a_{i-1} \cdot g) = 0$ (i.e., we are performing some sort of strong-inductive descent, where the base case for this has been established in the previous steps).

Recall once again the product formula for $f \cdot g = 0$, in particular for the value $l = i + m - 1$. Then we get the following (ignore the slight abuse of notation the sum; one i is fixed and the other isn't):

$$\sum_{\substack{i+j=i+m-1 \\ i,j \in \mathbb{N}}} a_i b_j = a_{i-1} b_m + a_i b_{m-1} + a_{i+1} b_{m-2} ... = 0 \tag{39}$$

But we assumed $a_i \cdot g, a_{i+1} \cdot g, ..., a_n \cdot g = 0$, so the constants $a_i b_{m-1}, a_{i+1} b_{m-2}...$ are annihilated. Thus it must be again that $a_{i-1} b_m = 0$.

The same argument given in the previous two parts then has that the polynomial $a_{i-1} \cdot g$ is either outright zero of less degree. In the latter case then, we would say $g_2 = a_{i-1} \cdot g$, in which case $f \cdot g_2 = 0$ again by (35) and (36). □

(d) Prove that if $a_i \cdot g = 0$ for every i, then there is some non-zero $b \in R$ such that $b \cdot f = 0$.

Proof. We claim that $b = b_m$ (note we considered g as m-th degree polynomial for $m \geq 1$, so we are assuming $b_m \neq 0$).

For this, we simply consider the product formula for $b_m \cdot f$:

$$b_m \cdot f = \sum_{\substack{i+j=l \\ i,j \in \mathbb{N}}} b_m a_j = b_m a_n + b_m a_{n-1} + ... + b_m a_0 \tag{40}$$

We assumed $a_i \cdot g = 0$ for every i though, so the terms in the sum of (40) must vanish, as they are all just coefficients in $a_i \cdot g$ products. Thus $b_m \cdot f = 0$. □

(e) Put it all together. That is prove, that $f \in R[x]$ is a zero-divisor if and only if there is some $b \in R$ such that $b \cdot f = 0$.

Proof. Obviously, by definition, if there is some $b \in R$ such that $b \cdot f = 0$, then f is a zero divisor.

We construct the converse argument now, which boils down to considering what happens if we get some polynomial of strictly degree than g called g_n such that $f \cdot g_2 = 0$.

However, we note this case is obvious, as we simply repeat our construction with this g_2, then either we get $a_i \cdot g_2 = 0$ for all i (which resolves it by (d)), or another g_3 such that $deg(g) > deg(g_2) > deg(g_3)$ where we still have $f \cdot g_3 = 0$.

Continuing this process either gets us some $a_i \cdot g_k = 0$ for all i (which resolves it again by (d)) or we continue the process until the deg of some g_k is forced to be 0, in which case $g_k \neq 0$ suffices as our b.

This completes the exercise. □