Math 762 **Spring 2016**
Homework 1 **Drew Armstrong**

Problem 1. Infinite Products and Coproducts in Ab. We have seen that finite products and coproducts agree in Ab. However, the same is not true for **infinite** products and coproducts. Let I be a set and let $\{A_i\}_{i\in I}$ be a family of abelian groups, each equal to some fixed group A.

(a) Show that the set $A^I := \text{Hom}_{\mathsf{Set}}(I, A)$ is an abelian group. Furthermore, show that we can think of this group as the infinite product $\Pi_{i\in I} A_i$ in the category Ab.

(b) Let $A^{\oplus I}$ denote the subgroup of A^I in which **all but finitely many** elements of I are sent to the identity element $0 \in A$. Show that we can think of $A^{\oplus I}$ as the infinite coproduct $\bigoplus_{i\in I} A_i$ in the category Ab.

(c) Show that the inclusion $A^{\oplus I} \subseteq A^I$ can be strict. [Hint: Let $A = \mathbb{Z}/10\mathbb{Z}$ and $I = \mathbb{Z}$.]

Proof. For part (a), consider two functions $a, b \in A^I$ denoted by $i \mapsto a_i$ and $i \mapsto b_i$. Then we define the function "$a + b$" $\in A^I$ by setting

$$(a + b)_i := a_i + b_i \text{ for all } i \in I. \tag{1}$$

The constant zero function $0 \in A^I$ defined by $0_i := 0_A$ is an identity element for this operation, and every function $a \in A^I$ has an inverse $-a \in A^I$ defined by $(-a)_i := -a_i$. Since associativity is inherited from $(A, +, 0_A)$ this defines an abelian group structure on A^I.

For each index $i \in I$ note that the function $\pi_i : A^I \to A_i$ defined by $\pi_i(a) := a_i$ is a group homomorphism by (1). Now suppose we have an abelian group B together with group homomorphisms $\varphi_i : B \to A_i$ for each $i \in I$. In this case I claim that **there exists a unique group homomorphism $\varphi : B \to A^I$ satisfying**

$$\begin{tikzcd} B \arrow[r, "\varphi"'] \arrow[rr, bend left, "\varphi_i"] & A^I \arrow[r, "\pi_i"'] & A_i \end{tikzcd} \quad \text{for all } i \in I.$$

Indeed, given any element $b \in B$ the condition $\pi_i(\varphi(b)) = \varphi_i(b)$ requires that we define the function $\varphi(b) \in A^I$ by setting $\varphi(b)_i := \varphi_i(b)$ for all $i \in I$. To see that the resulting function $\varphi : B \to A^I$ is a group homomorphism note that for all $b, c \in B$ and $i \in I$ we have

$$\varphi(b + c)_i = \varphi_i(b + c) = \varphi_i(b) + \varphi_i(c) = \varphi(b)_i + \varphi(c)_i = (\varphi(b) + \varphi(c))_i,$$

and hence $\varphi(b + c) = \varphi(b) + \varphi(c)$. We conclude that the pair $(A^I, \{\pi_i\}_{i\in I})$ is the categorical product $\prod_{i\in I} A_i$ in Ab.

For part (b), define the subgroup $A^{\oplus I} \subseteq A^I$ consisting of functions $a \in A^I$ such that $a_i = 0$ for all but finitely many $i \in I$ (i.e., functions of "finite support"). Note that for each $i \in I$ we have a set function $\iota_i : A_i \to A^{\oplus I}$ defined by

$$\iota_i(a)_j := \begin{cases} a & \text{if } i = j \\ 0_A & \text{if } i \neq j \end{cases}.$$

Note that for all $a, c \in A$ we have

$$\iota_i(a + b)_i = a + c = \iota_i(a)_i + \iota_i(c)_i = (\iota_i(a) + \iota_i(c))_i$$

and for all $j \neq i$ we have

$$\iota_i(a + c)_j = 0_A = 0_A + 0_A = \iota_i(a)_j + \iota_i(c)_j = (\iota_i(a) + \iota_i(c))_j$$

It follows that $\iota_i(a+c) = \iota_i(a) + \iota_i(c)$ and we conclue that ι_i is a group homomorphism. Now suppose we have an abelian group B together with group homomorphisms $\varphi_i : A_i \to B$ for each $i \in I$. In this case I claim that **there exists a unique group homomorphism $\varphi : A^{\oplus I} \to B$ satisfying**

$$\begin{tikzcd} A_i \arrow[r, "\iota_i"'] \arrow[rr, bend left, "\varphi_i"] & A^{\oplus I} \arrow[r, "\varphi"'] & B \end{tikzcd}$$

for all $i \in I$.

Indeed, given any function $a \in A^{\oplus I}$ note that we can write $a = \sum_{i \in I} \iota_i(a_i)$, where the sum is defined by (1). [The sum is finite because $a_i = 0_A$ and hence $\iota_i(a_i) = 0_A$ for all but finitely many $i \in I$.] Now the requirement that $\varphi \circ \iota_i = \varphi_i$ for all $i \in I$ implies that

$$(2) \qquad \varphi(a) = \varphi\left(\sum_{i \in I} \iota_i(a_i)\right) = \sum_{i \in I} \varphi(\iota_i(a_i)) = \sum_{i \in I} \varphi_i(a_i).$$

Note that the sum on the right exists because we have $a_i = 0_A$ and hence $\varphi_i(a_i) = 0_B$ for all but finitely many $i \in I$. Hence the requirement (2) uniquely determines a function $\varphi : A^{\oplus I} \to B$. And this function φ is a group homomorphism since for all $a, b \in A^{\oplus I}$ we have

$$\begin{aligned} \varphi(a+b) &= \sum_{i \in I} \varphi_i((a+b)_i) \\ &= \sum_{i \in I} \varphi_i(a_i + b_i) \\ &= \sum_{i \in I} (\varphi_i(a_i) + \varphi_i(b_i)) \\ &= \sum_{i \in I} \varphi_i(a_i) + \sum_{i \in I} \varphi_i(b_i) \\ &= \varphi(a) + \varphi(b). \end{aligned}$$

We conclude that the pair $(A^{\oplus I}, \{\iota_i\}_{i \in I})$ is the categorical coproduct $\bigoplus_{i \in I} A_i$ in Ab.

The hint for part (c) was supposed to be cute, but maybe it was too cute. Anyway, if $A = \mathbb{Z}/10\mathbb{Z}$ and $I = \mathbb{Z}$ then we will think of a function $a \in A^I$ as a formal power series $\sum_{i \in \mathbb{Z}} a_i \cdot 10^i$. If we choose one decimal expansion for each real number then we obtain an inclusion $\mathbb{R} \subseteq A^I$. Similarly, each function of finite support $a \in A^{\oplus I}$ determines a rational number so we obtain an inclusion $A^{\oplus I} \subseteq \mathbb{Q}$. Putting these together gives

$$A^{\oplus I} \subseteq \mathbb{Q} \subsetneq \mathbb{R} \subseteq A^I.$$

□

Problem 2. What is a polynomial? Let $(M, \cdot, 1_M)$ be a monoid and let $(R, +, \circ, 0_R, 1_R)$ be a ring. The monoid ring $R[M]$ is the abelian group $R^{\oplus M}$ together with the following operation: for all $a, b \in R[M]$ and $m \in M$ we define $a * b \in R[M]$ by the formula

$$(a * b)_m := \sum_{m_1 \cdot m_2 = m} a_{m_1} \circ b_{m_2}.$$

Note that the sum on the right exists because $a_{m_1} \circ b_{m_2} = 0_R$ for all but finitely many pairs $(m_1, m_2) \in M^2$. One can check (you don't need to) that this defines a ring structure on $R[M]$.

(a) Show that there is an obvious injective ring homomorphism $R \hookrightarrow R[M]$.

(b) Thinking of $(\mathbb{N}, +, 0)$ as a monoid, prove that the monoid ring $R[\mathbb{N}]$ is isomorphic to the polynomial ring in one variable $R[x]$. [Remark: In fact, we could think of $R[\mathbb{N}]$ as the **definition** of the polynomial ring. I mean, what *is* x anyway?]

Proof. For part (a), consider an element $r \in R$. We will define a function $r \in R[M]$ with the same name (to conserve notation) by setting

$$r_m := \begin{cases} r & \text{if } m = 1_M \\ 0_R & \text{if } m \neq 1_M \end{cases}.$$

Note that this defines an injective homomorphism of abelian groups $R \hookrightarrow R[M]$. To show that this is a ring homomorphism consider any $r, s \in R$. Then we have

$$(r * s)_{1_M} = \sum_{m \in M^\times} r_m \circ s_{m^{-1}}$$

where $M^\times$ is the group of units of M. Since $r_m \circ s_{m^{-1}} = 0_R$ for all $m \neq 1_M$, the sum evaluates to $(r * s)_{1_M} = r_{1_M} \circ s_{1_M} = r \circ s$. If $m \neq 1_M$ then $m_1 \cdot m_2 = m$ implies that $m_1 \neq 1_M$ or $m_2 \neq 1_M$ and we have

$$(r * s)_m = \sum_{m_1 \cdot m_2 = m} r_{m_1} \circ s_{m_2} = \sum_{m_1 \cdot m_2 = m} 0_R = 0_R.$$

In summary, we conclude that $(r * s)_m = (r \circ s)_m$ for all $m \in M$.

For part (b), we will define a function $P : R[\mathbb{N}] \to R[x]$ by sending the function $a \in R[\mathbb{N}]$ to the polynomial $P(a) := \sum_{n \in \mathbb{N}} a_n x^n$. This function is bijective by the definition of $R[x]$ (omitted). To see that P is a ring homomorphism, first note that $1 \in R \subseteq R[\mathbb{N}]$ gets sent to $P(1) = 1 \in R[x]$. Then note that for all $a, b \in R[M]$ we have

$$\begin{aligned} P(a) + P(b) &= \left(\sum_{n \in \mathbb{N}} a_n x^n \right) + \left(\sum_{n \in \mathbb{N}} b_n x^n \right) \\ &= \sum_{n \in \mathbb{N}} (a_n + b_n) x^n \\ &= \sum_{n \in \mathbb{N}} (a + b)_n x^n \\ &= P(a + b) \end{aligned}$$

and

$$\begin{aligned} P(a)P(b) &= \left(\sum_{n \in \mathbb{N}} a_n x^n \right) \left(\sum_{n \in \mathbb{N}} b_n x^n \right) \\ &= \sum_{n \in \mathbb{N}} \left(\sum_{n_1 + n_2 = n} a_{n_1} \circ b_{n_2} \right) x^n \\ &= \sum_{n \in \mathbb{N}} (a * b)_n x^n \\ &= P(a * b). \end{aligned}$$

□

[Remark: If M and R have some topological structure then we can try to form a ring out of more general kinds of functions $M \to R$. For example, if $M = (\mathbb{R}, +, 0)$ and $R = (\mathbb{R}, +, \cdot, 0, 1)$ then we can try to define the "convolution" of $f, g : \mathbb{R} \to \mathbb{R}$ by

$$(f * g)(x) := \int f(t)g(x-t)dt.$$

As we see now, this is just a straightforward generalization of polynomial multiplication.]

Problem 3. Evaluation of Polynomials. Let $\varphi : R \to S$ be a ring homomorphism and assume that the image of φ is in the center of S:

$$\operatorname{im}\varphi \subseteq Z(S) := \{t \in S : st = ts \text{ for all } s \in S\}.$$

(a) For all $s \in S$ prove that **there exists a unique ring homomorphism** $\varphi_s : R[x] \to S$ satisfying $\varphi_s(x) = s$ and $\varphi_s(r) = \varphi(r)$ for all $r \in R$ (thought of as a subring of $R[x]$ via Problem 2(a)). [Remark: When $R \subseteq S$ is a subring with inclusion homomorphism $i : R \hookrightarrow S$ we refer to the map $i_s : R[x] \to S$ as evaluation at s.]

(b) Show that the result of part (a) can fail when the image of φ is **not** in the center of S. [Remark: This is the place where the theories of commutative and noncommutative rings begin to diverge.]

Proof. For part (a), let $\varphi : R \to S$ be a ring homomorphism such that $\operatorname{im}\varphi \subseteq Z(S)$ and let $i : R \to R[x]$ be the injective homomorphism from Problem 2(a). For each $s \in S$ we want to show that there exists a unique ring homomorphism $\varphi_s : R[x] \to S$ such that $\varphi_s(x) = s$ and such that the following diagram commutes:

$$\begin{tikzcd} R \arrow[r, "i"'] \arrow[rr, bend left, "\varphi"] & R[x] \arrow[r, "\varphi_s"'] & S \end{tikzcd} .$$

Given any polynomial $\sum_{n\in\mathbb{N}} a_n x^n \in R[x]$, the desired homomorphism φ_s must satisfy

$$\varphi_s\left(\sum_{n\in\mathbb{N}} a_n x^n\right) = \sum_{n\in\mathbb{N}} \varphi_s(a_n)\varphi_s(x)^n = \sum_{n\in\mathbb{N}} \varphi(a_n)s^n. \tag{3}$$

Since we have $a_n = 0_r$ and hence $\varphi(a_n)s^n = 0_S$ for all but finitely many $n \in \mathbb{N}$ the sum on the right exists and the requirement (3) defines a function $\varphi_s : R[x] \to S$. To see that this function φ_s is a ring homomorphism first note that it sends $1_R \in R \subseteq R[x]$ to $\varphi(1_R)s^0 = 1_S s^0 = 1_S \in S$. Then note that for all polynomials $\sum_{n\in\mathbb{N}} a_n x^n$ and $\sum_{n\in\mathbb{N}} b_n x^n$ we have

$$\begin{aligned}
\varphi_s\left(\sum_{n\in\mathbb{N}} a_n x^n + \sum_{n\in\mathbb{N}} b_n x^n\right) &= \varphi_s\left(\sum_{n\in\mathbb{N}} (a_n + b_n) x^n\right) \\
&= \sum_{n\in\mathbb{N}} \varphi(a_n + b_n)s^n \\
&= \sum_{n\in\mathbb{N}} (\varphi(a_n) + \varphi(b_n))s^n \\
&= \sum_{n\in\mathbb{N}} \varphi(a_n)s^n + \sum_{n\in\mathbb{N}} \varphi(b_n)s^n \\
&= \varphi_s\left(\sum_{n\in\mathbb{N}} a_n x^n\right) + \varphi_s\left(\sum_{n\in\mathbb{N}} b_n x^n\right).
\end{aligned}$$

Finally, since $s\varphi(r) = \varphi(r)s$ for all $r \in R$ we have

$$\begin{aligned}
\varphi_s\left(\left(\sum_{n\in\mathbb{N}} a_n x^n\right)\left(\sum_{n\in\mathbb{N}} b_n x^n\right)\right) &= \varphi_s\left(\sum_{n\in\mathbb{N}}\left(\sum_{n_1+n_2=n} a_{n_1}b_{n_2}\right)x^n\right)\\
&= \sum_{n\in\mathbb{N}} \varphi\left(\sum_{n_1+n_2=n} a_{n_1}b_{n_2}\right)s^n\\
&= \sum_{n\in\mathbb{N}}\left(\sum_{n_1+n_2=n} \varphi(a_{n_1})\varphi(b_{n_2})\right)s^n\\
&\overset{!}{=} \left(\sum_{n\in\mathbb{N}} \varphi(a_n)s^n\right)\left(\sum_{n\in\mathbb{N}} \varphi(b_n)s^n\right)\\
&= \varphi_s\left(\sum_{n\in\mathbb{N}} a_n x^n\right)\varphi_s\left(\sum_{n\in\mathbb{N}} b_n x^n\right).
\end{aligned}$$

We used the commutativity of s in the step labeled (!).

For part (b), assume that the set function $\varphi_s : R[x] \to S$ defined in (3) is a ring homomorphism and consider any $r \in R$. By applying φ_s to the polynomials $x + r$ and $x - r$ in $R[x]$ and their product $(x - r)(x + r) = x^2 - r^2$ we obtain

$$\varphi_s(x + r)\varphi_s(x - r) = (s + \varphi(r))(s - \varphi(r)) = s^2 + \varphi(r)s - s\varphi(r) - \varphi(r)^2$$

and

$$\varphi_s((x + r)(x - r)) = \varphi_s(x^2 - r^2) = s^2 - \varphi(r)^2.$$

Then since φ_s is a ring homomorphism we must have

$$\begin{aligned}
\varphi_s(x + r)\varphi_s(x - r) &= \varphi_s((x + r)(x - r))\\
s^2 + \varphi(r)s - s\varphi(r) - \varphi(r)^2 &= s^2 - \varphi(r)^2\\
\varphi(r)s &= s\varphi(r).
\end{aligned}$$

In conclusion, we have shown that if $s \in S$ does **not** commute with the image of $\varphi : R \to S$ then the set function $\varphi_s : R[x] \to S$ defined in (3) is **not** a ring homomorphism. □

The next two problems illustrate an important difference between commutative and noncommutative rings.

Problem 4. Descartes' Theorem. Let R be a **commutative ring** and for all $\alpha \in R$ consider the evaluation morphism $i_\alpha : R[x] \to R$ from Problem 3. For simplicity we will use the notation "$f(\alpha)$" $:= i_\alpha(f(x))$.

(a) Given $f(x) \in R[x]$ and $\alpha \in R$, prove that we have $f(\alpha) = 0$ if and only if $f(x) = (x - \alpha)g(x)$ for some $g(x) \in R[x]$. [Hint: Use division with remainder.]

(b) If R is, furthermore, an integral domain (i.e., if $ab = 0$ implies $a = 0$ or $b = 0$) then the degree function $\deg : R[x] \setminus \{0\} \to \mathbb{N}$ satisfies $\deg(fg) = \deg(f) + \deg(g)$. Use this fact to prove that a polynomial of degree n over an integral domain has at most n distinct roots. [Hint: Use part (a) and induction.]

Proof. For part (a), let $\alpha \in R$ and consider the polynomial $x - \alpha \in R[x]$. Since this polynomial is monic (its leading coefficient is a unit) there exist polynomials $q(x), r(x) \in R[x]$ such that

- $f(x) = (x - \alpha)q(x) + r(x)$,

- $r(x) = 0$ or $\deg(r(x)) < \deg(x - \alpha)$.

The second condition implies that $r(x)$ is a constant. Let's call it $r(x) = r \in R$. Now apply the ring homomorphism $i_\alpha : R[x] \to R$ to get

$$\begin{aligned} f(\alpha) &= i_\alpha(f(x)) \\ &= i_\alpha((x-\alpha)q(x) + r) \\ &= i_\alpha(x-\alpha)i_\alpha(q(x)) + i_\alpha(r) \\ &= (\alpha - \alpha)q(\alpha) + r \\ &= r. \end{aligned}$$

We conclude that $f(x) = (x - \alpha)q(x) + f(\alpha)$ and it follows that $f(\alpha) = 0$ if and only if $f(x)$ is divisible by $(x - \alpha)$ in $R[x]$.

For part (b), let R be an integral domain and assume for induction that any polynomial of degree $n - 1$ in $R[x]$ has as most $n - 1$ distinct roots in R. Now consider a polynomial $f(x) \in R[x]$ of degree n. If $f(x)$ has no roots then we are done. Otherwise, suppose there exists $\alpha \in R$ such that $f(\alpha) = 0$. By part (a) this means that we have

$$f(x) = (x - \alpha)g(x) \tag{4}$$

for some $g(x) \in R[x]$, and since R is a domain we must have $\deg(g) = n - 1$. Now suppose that $\beta \neq \alpha$ is any other root of $f(x)$. Evaluating equation (4) at β gives

$$\begin{aligned} f(\beta) &= (\beta - \alpha)g(\beta) \\ 0 &= (\beta - \alpha)g(\beta). \end{aligned}$$

Since $\beta - \alpha \neq 0$ and since R is a domain this implies that $g(\beta) = 0$. But by induction there can be at most $n - 1$ distinct such β and we conclude that $f(x)$ has at most $1 + (n - 1) = n$ distinct roots in R. □

Problem 5. The Original Noncommutative Ring. The ring (actually an $\mathbb{R}$-algebra) of quaternions was defined by William Rowan Hamilton on the 16th of October, 1843. He defined it as the 4-dimensional $\mathbb{R}$-vector space

$$\mathbb{H} := \{a\mathbf{1} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} : a, b, c, d \in \mathbb{R}\},$$

where the abstract basis elements $\mathbf{1}, \mathbf{i}, \mathbf{j}, \mathbf{k}$ satisfy the relations

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = \mathbf{ijk} = -\mathbf{1}.$$

(a) Prove that $\mathbb{H}$ can be realized as a subring (actually an $\mathbb{R}$-subalgebra) of the ring of 2×2 matrices over $\mathbb{C}$. [Hint: Let $i \in \mathbb{C}$ be the imaginary unit. Show that the $\mathbb{R}$-linear map defined on the basis by

$$\mathbf{1} \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \mathbf{i} \mapsto \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad \mathbf{j} \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \mathbf{k} \mapsto \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

is injective. Then show that the relations are satisfied.]

(b) Use part (a) to compute the center $Z(\mathbb{H})$.

(c) It seems that the polynomial $x^2 + \mathbf{1} \in \mathbb{H}[x]$ of degree 2 has at least **three** distinct roots: $\mathbf{i}, \mathbf{j}, \mathbf{k} \in \mathbb{H}$. What's the problem?

Proof. For part (a), let $\varphi : \mathbb{H} \to \mathrm{Mat}_{2\times 2}(\mathbb{C})$ be the linear map defined in the hint. Then for all $a\mathbf{1} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \in \mathbb{H}$ we have

$$\begin{aligned}
\varphi(a\mathbf{1} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}) &= a\varphi(\mathbf{1}) + b\varphi(\mathbf{i}) + c\varphi(\mathbf{j}) + d\varphi(\mathbf{k}) \\
&= a\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + b\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} + c\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} + d\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \\
&= \begin{pmatrix} a+ib & c+id \\ -c+id & a-ib \end{pmatrix}.
\end{aligned}$$

Note that this function is injective since if we have

$$\begin{gathered}
\varphi(a\mathbf{1} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}) = \varphi(e\mathbf{1} + f\mathbf{i} + g\mathbf{j} + h\mathbf{k}) \\
\begin{pmatrix} a+ib & c+id \\ -c+id & a-ib \end{pmatrix} = \begin{pmatrix} e+if & g+ih \\ -g+ih & e-if \end{pmatrix}
\end{gathered}$$

then it follows that $a + ib = e + if$ (hence $a = e$ and $b = f$) and $c + id = g + ih$ (hence $c = g$ and $d = h$), and we conclude that $a\mathbf{1} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} = e\mathbf{1} + f\mathbf{i} + g\mathbf{j} + h\mathbf{k}$. Now to show that $\varphi : \mathbb{H} \hookrightarrow \mathrm{Mat}_{2\times 2}(\mathbb{C})$ is a ring homomorphism it is sufficient to show that the images $\varphi(\mathbf{1}), \varphi(\mathbf{i}), \varphi(\mathbf{j}), \varphi(\mathbf{k})$ satisfy Hamilton's relations.

[Indeed, Hamilton's definition can be expressed in modern terms as follows. Let $R := \mathbb{R}\langle \mathbf{1}, \mathbf{i}, \mathbf{j}, \mathbf{k}\rangle$ be the ring of polynomials in the **noncommuting** indeterminates $\mathbf{1}, \mathbf{i}, \mathbf{j}, \mathbf{k}$ and let $I := \langle \mathbf{i}^2 + \mathbf{1}, \mathbf{j}^2 + \mathbf{1}, \mathbf{k}^2 + \mathbf{1}, \mathbf{ijk} + \mathbf{1}\rangle \subseteq R$ be the smallest two-sided ideal containing (i.e., generated by) the set $A := \left\{\mathbf{i}^2 + \mathbf{1}, \mathbf{j}^2 + \mathbf{1}, \mathbf{k}^2 + \mathbf{1}, \mathbf{ijk} + \mathbf{1}\right\}$. Then we define

$$\mathbb{H} := \frac{R}{I} = \frac{R}{\langle A\rangle}.$$

Moreover, this definition satisfies the following universal property: Let $\varphi : R \to S$ be any ring homomorphism sending A to zero. Then it must also send $I = \langle A\rangle$ to zero and it follows that there exists a unique ring homomorphism $\bar{\varphi} : R/I \to S$ such that

$$\begin{tikzcd}
 & R \arrow[dl, "\pi"'] \arrow[dr, "\varphi"] & \\
R/I \arrow[rr, "\bar{\varphi}"'] & & S
\end{tikzcd}$$

In our case we have $S = \mathrm{Mat}_{2\times 2}(\mathbb{C})$ and $\varphi : R \to S$ is the unique ring homomorphism defined by the hint. By abuse of notation we have also written $\bar{\varphi} = \varphi$. Surely this is not the way Hamilton thought about the problem.]

And this is verified by the following computations:

$$\begin{aligned}
\varphi(\mathbf{i})^2 &= \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -\varphi(\mathbf{1}), \\
\varphi(\mathbf{j})^2 &= \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -\varphi(\mathbf{1}), \\
\varphi(\mathbf{k})^2 &= \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -\varphi(\mathbf{1}), \\
\varphi(\mathbf{i})\varphi(\mathbf{j})\varphi(\mathbf{k}) &= \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -\varphi(\mathbf{1}).
\end{aligned}$$

For part (b), since φ is an injective ring homomorphism it is enough to find all $\alpha := a\mathbf{1} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \in \mathbb{H}$ such that $\varphi(\alpha)\varphi(\beta) = \varphi(\beta)\varphi(\beta)$ for all $\beta \in \mathbb{H}$. In particular we must have

$$\begin{aligned} \varphi(\alpha)\varphi(\mathbf{i}) &= \varphi(\mathbf{i})\varphi(\alpha) \\ \begin{pmatrix} a+ib & c+id \\ -c+id & a-ib \end{pmatrix}\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} &= \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}\begin{pmatrix} a+ib & c+id \\ -c+id & a-ib \end{pmatrix} \\ \begin{pmatrix} ia-b & -ic+d \\ -ic-d & -ia-b \end{pmatrix} &= \begin{pmatrix} ia-b & ic-d \\ ic+d & -ia-b \end{pmatrix}, \end{aligned}$$

which implies that $-ic+d = ic-d$, hence $c=0$ and $d=0$. And we must also have

$$\begin{aligned} \varphi(\alpha)\varphi(\mathbf{j}) &= \varphi(\mathbf{j})\varphi(\alpha) \\ \begin{pmatrix} a+ib & 0 \\ 0 & a-ib \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} &= \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} a+ib & 0 \\ 0 & a-ib \end{pmatrix} \\ \begin{pmatrix} 0 & a+ib \\ -a+ib & 0 \end{pmatrix} &= \begin{pmatrix} 0 & a-ib \\ -a-ib & 0 \end{pmatrix}, \end{aligned}$$

which implies that $a+ib = a-ib$, hence $b=0$. We conclude that $\alpha = a\mathbf{1}+0\mathbf{i}+0\mathbf{j}+0\mathbf{k}$. Thus the center of $\mathbb{H}$ consists of the "purely real" quaterions:

$$Z(\mathbb{H}) = \{a\mathbf{1}+0\mathbf{i}+0\mathbf{j}+0\mathbf{k} : a \in \mathbb{R}\} \approx \mathbb{R}.$$

In particular, if $\alpha \in \mathbb{H}$ is **not** purely real then the solution to Problem 3(b) shows that the evaluation function $\varphi_\alpha : \mathbb{H}[x] \to \mathbb{H}$ is **not** a ring homomorphism. Thus the proof of Problem 4, which assumes that evaluation is a homomorphism, fails in this case. This explains the strange observation in part (c). □

[Remark: In fact, one can show that every purely imaginary quaternion $a\mathbf{i}+b\mathbf{j}+c\mathbf{k} \in \mathbb{H}$ satisfying $a^2+b^2+c^2=1$ is a root of the polynomial $x^2+\mathbf{1} \in \mathbb{H}[x]$. That's a lot of roots! In 1965 Gordon and Motzkin showed how to fix this situation by proving that a polynomial of degree n over a division ring D has roots in at most n **conjugacy classes** of D.]

Problem 6. Monomorphisms and Epimorphisms. The notions of injective and surjective functions are not categorically well-behaved. In a general category they should be replaced with the notions of "monomorphism" and "epimorphism".

Let $\alpha : X \to Y$ be a morphism in a category $\mathscr{C}$. We say that α is a monomorphism if for all objects $Z \in \mathscr{C}$ and all morphisms $\beta_1, \beta_2 : Z \to X$ we have

$$\alpha \circ \beta_1 = \alpha \circ \beta_2 \implies \beta_1 = \beta_2.$$

We say α is an epimorphism if for all $Z \in \mathscr{C}$ and $\beta_1, \beta_2 : Y \to Z$ we have

$$\beta_1 \circ \alpha = \beta_2 \circ \alpha \implies \beta_1 = \beta_2.$$

(a) In the category Set, prove that monomorphisms are the same as injective functions and epimorphisms are the same as surjective functions.

(b) In the category Rng, prove that an epimorphism may fail to be surjective.

Proof. For part (a) consider two sets $X, Y \in$ Set and a function $\alpha : X \to Y$.

We will first show that α is injective if and only if it is a monomorphism. So let $\alpha : X \to Y$ be injective and consider any functions $\beta_1, \beta_2 : Z \to X$ such that $\alpha \circ \beta_1 = \alpha \circ \beta_2$. Then for any element $z \in Z$ we have $\alpha(\beta_1(z)) = \alpha(\beta_2(z))$, and the fact that α is injective implies that $\beta_1(z) = \beta_2(z)$. We conclude that $\beta_1 = \beta_2$ and hence α is a monomorphism.

Conversely, let $\alpha : X \to Y$ be a monomorphism and suppose that we have $\alpha(x_1) = \alpha(x_2)$ for some elements $x_1, x_2 \in X$. Now let $Z = \{*\}$ be a set with one element and consider the functions $\beta_1, \beta_2 : Z \to X$ defined by $\beta_1(*) := x_1$ and $\beta_2(*) := x_2$. Since $\alpha \circ \beta_1 = \alpha \circ \beta_2$ as functions, the fact that α is a monomorphism implies that $\beta_1 = \beta_2$, and hence $x_1 = \beta_1(*) = \beta_2(*) = x_2$. We conclude that α is injective.

Next we will show that α is surjective if and only if it is an epimorphism. So let $\alpha : X \to Y$ be surjectve and consider any functions $\beta_1, \beta_2 : Y \to Z$ such that $\beta_1 \circ \alpha = \beta_2 \circ \alpha$. For any element $y \in Y$ there exists an element $x \in X$ such that $\alpha(x) = y$ so that

$$\beta_1(y) = \beta_1(\alpha(x)) = \beta_2(\alpha(x)) = \beta_2(y).$$

We conclude that $\beta_1 = \beta_2$ and hence α is an epimorphism.

Conversely, suppose that $\alpha : X \to Y$ is an epimorphism and consider a set $Z = \{0, 1\}$ with two elements. We will define functions $\beta_1, \beta_2 : Y \to Z$ by setting $\beta_1(y) := 1$ for all $y \in Y$ and

$$\beta_2(y) := \begin{cases} 1 & \text{if } y \in \operatorname{im}\alpha \\ 0 & \text{if } y \notin \operatorname{im}\alpha \end{cases}.$$

Now observe that $\beta_1(\alpha(x)) = 1 = \beta_2(\alpha(x))$ for all $x \in X$ and hence $\beta_1 \circ \alpha = \beta_2 \circ \alpha$. Since α is an epimorphism this implies that $\beta_1 = \beta_2$. Finally, the fact that $\beta_2(y) = \beta_1(y) = 1$ for all $y \in Y$ implies that $\operatorname{im}\alpha = Y$, hence α is surjective.

For part (b), consider the unique ring homomorphism $i : \mathbb{Z} \to \mathbb{Q}$. Clearly this is not a surjection, but we will show that it is an epimorphism. Indeed, for any ring homomorphism $\varphi : \mathbb{Q} \to R$ and any $0 \neq q \in \mathbb{Z}$ we must have $\varphi\left(i(q)\right)\varphi\left(i(q)^{-1}\right) = \varphi\left(i(q)i(q)^{-1}\right) = \varphi(1_{\mathbb{Q}}) = 1_R$ and hence $\varphi\left(i(q)^{-1}\right) = \varphi\left(i(q)\right)^{-1}$. Now consider any two ring homomorphisms $\beta_1, \beta_2 : \mathbb{Q} \to R$ such that $\beta_1 \circ i = \beta_2 \circ i$. Then for all $p, q \in \mathbb{Z}$ with $q \neq 0$ we have

$$\beta_1\left(i(p)i(q)^{-1}\right) = \beta_1\left(i(p)\right)\beta_1\left(i(q)\right)^{-1} = \beta_2\left(i(p)\right)\beta_2\left(i(q)\right)^{-1} = \beta_2\left(i(p)i(q)^{-1}\right).$$

Since every element of $\mathbb{Q}$ can be written in the form $i(p)i(q)^{-1}$ for some $p, q \in \mathbb{Z}$ this implies that $\beta_1 = \beta_2$ and hence $i : \mathbb{Z} \to \mathbb{Q}$ is an epimorphism. □