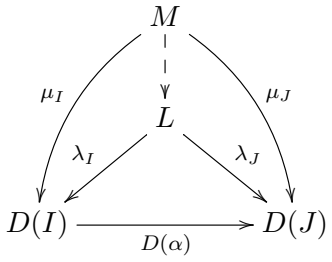
**Math 762** **Spring 2016**
**Homework 2** **Drew Armstrong**

---

**Problem 1. Limits and Colimits.** Let $\mathcal{C}$ be any category and let $\mathcal{I}$ be a small category. A diagram of shape $\mathcal{I}$ in $\mathcal{C}$ is just a covariant functor $D : \mathcal{I} \to \mathcal{C}$. The limit of the diagram (if it exists) is a structure $\varprojlim D = (L, \{\lambda_I\}_{I \in \mathcal{I}})$ where

- $L \in \mathcal{C}$ is an object and $\lambda_I : L \to D(\mathcal{I})$ are morphisms such that for all objects $I, J \in \mathcal{I}$ and morphisms $\alpha \in \mathrm{Hom}_{\mathcal{I}}(I, J)$ we have $D(\alpha) \circ \lambda_I = \lambda_J$.
- If $M \in \mathcal{C}$ is another object with morphisms $\mu_I : M \to D(\mathcal{I})$ satisfying the first property, then **there exists a unique morphism** $M \to L$ such that:

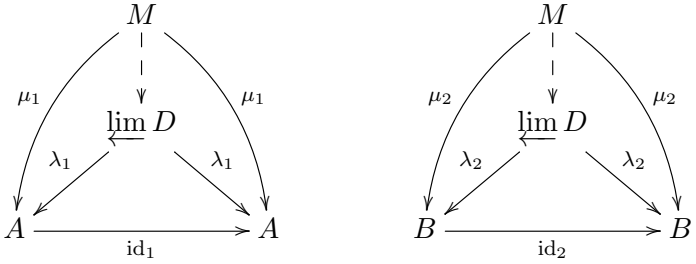



In other words, the limit $\varprojlim D$ is a final object in a certain category (of "cones"). We define the colimit $\varinjlim D$ by reversing all arrows in the definition.

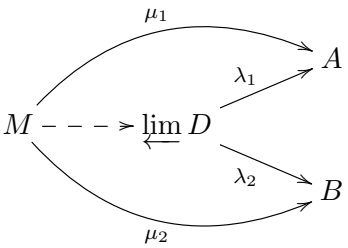
(a) Given objects $A, B \in \mathcal{C}$, express the categorical product $A \times B$ as a limit.
(b) Suppose there exists a zero object $0 \in \mathcal{C}$. Given a morphism $\varphi : X \to Y$ in $\mathcal{C}$, express the categorical kernel of $\varphi$ as a limit.
(c) (Optional) Let $R$ be a ring and think of $\mathcal{I} = (\mathbb{N}, \leq)$ as a category with a unique arrow $i \to j$ for each $i \leq j$ in $\mathbb{N}$. Now let $D : \mathcal{I} \to R$-Mod be a diagram in which each morphism $D(\alpha)$ is injective. Prove that the colimit $\varinjlim D$ exists.

*Proof.* (a): Let $\mathcal{I}$ be the following category with two objects and two morphisms:

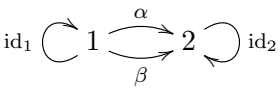

Let $A, B$ be objects in a category $\mathcal{C}$ and consider the unique functor $D : \mathcal{I} \to \mathcal{C}$ defined by $D(1) = A$ and $D(2) = B$. Now the limit $\varprojlim D$ (if it exists) is defined by satisfying the following two commutative diagrams:



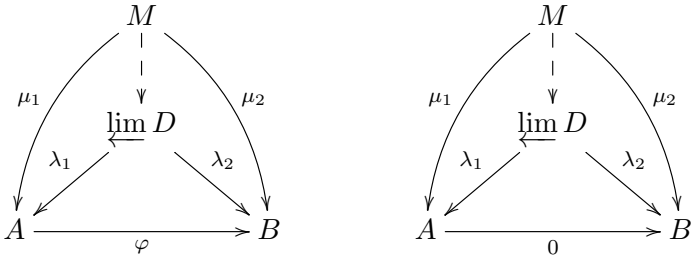
Putting these two diagrams together into one shows that the limit coincides exactly with the definition of the categorical product:



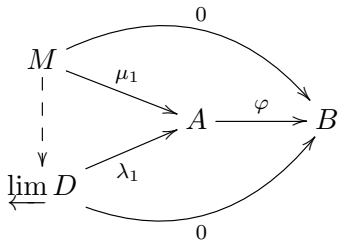

(b): Let $\mathcal{I}$ be the following category with two objects and four morphisms:




Let $\mathcal{C}$ be any category containing a zero object and consider any morphism $\varphi : A \to B$ in $\mathcal{C}$. Let $D : \mathcal{I} \to \mathcal{C}$ be the unique functor defined by $D(1) = A$, $D(2) = B$, $D(\alpha) = \varphi$ and $D(\beta) = 0$ (the zero morphism). Now the limit $\varprojlim D$ (if it exists) is defined by satisfying four commutative diagrams. Two of these diagrams are just the same as in part (a). Here are the new diagrams:




In particular, the second of these new diagrams just says that $\lambda_2 = 0$ and $\mu_2 = 0$. Thus the limit (if it exists) is defined by the following single diagram, which is the same diagram that defines the kernel of the morphism $\varphi : A \to B$:

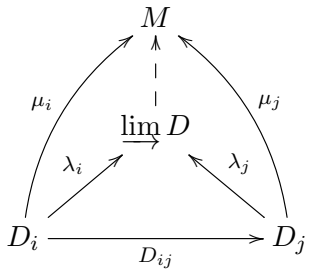



(c): I assigned this problem because we already secretly used this fact in class (during the proof that PID $\Rightarrow$ UFD), but then I realized that it's too difficult/annoying so I made it optional. Here's my sketch of a solution.

Consider the category $\mathcal{I}$ with objects $\mathbb{N} = \{1, 2, 3, \ldots\}$ and for each $i \leq j$ a unique morphism $\varphi_{ij} : i \to j$. (Thus for each $i \in \mathbb{N}$ the morphism $\varphi_{ii}$ is the identity $\mathrm{id}_i : i \to i$.) Now consider a functor $D : \mathcal{I} \to R\text{-Mod}$ such that $D(\varphi_{ij}) : D(i) \to D(j)$ is an **injective** homomorphism of $R$-modules for all $i \leq j$. To save notation, let's write $D_i := D(i)$ and $D_{ij} := D(\varphi_{ij})$. To find the **colimit** of the diagram $D$, we are looking for an $R$-module $\varinjlim D$ and a collection of $R$-module homomorphisms $\lambda_i : D_i \to \varinjlim D$ such that

- For all $i \leq j$ we have $D_{ij} \circ \lambda_i = \lambda_j$.

- If $M$ is any other $R$-module with $R$-module homomorphisms $\mu_i : D_i \to M$ such that $D_{ij} \circ \mu_i = \mu_j$ for all $i \leq j$ then there exists a unique map $\varinjlim D \to M$ satisfying




If such a module exists then it is unique (since it's an initial object in a certain category); the problem is to **construct it**. The intuition behind the construction is to think of each injective morphism $D_{ij} : D_i \hookrightarrow D_j$ as an actual **inclusion** so that our diagram becomes an increasing chain of modules:

$$D_1 \subseteq D_2 \subseteq D_3 \subseteq \cdots .$$

In this case we usually express the colimit as the "infinite union" $\cup_{n\in\mathbb{N}} D_n$. The problem is to make this formal.

There are various ways to do this. To gain a good understanding, we should probably first construct the "infinite union" as a set and then upgrade it to an abelian group and an $R$-module. First we will define $\cup_{n\in\mathbb{N}} D_n$ as a set of equivalence classes of ordered pairs

$$\bigcup_{n\in\mathbb{N}} D_n := \{(i, d_i) : i \in \mathbb{N}, d_i \in D_i\}/\sim$$

where the relation $(i, d_i) \sim (j, d_i)$ is defined by

- $i \leq j$ and $D_{ij}(d_i) = d_j$, or
- $j \leq i$ and $D_{ji}(d_j) = d_i$.

If $i = j$ then since $D_{ii} = D(\varphi_{ii}) = D(\mathrm{id}_i) = \mathrm{id}_{D_i}$ we have $(i, d_i) \sim (i, d_i)$. Thus $\sim$ is a symmetric and reflexive relation. To show that $\sim$ is transitive, assume that we have $(i, d_i) \sim (j, d_j)$ and $(j, d_j) \sim (k, d_k)$ and without loss of generality assume that $i \leq j \leq k$ so that $d_k = D_{jk}(d_j)$ and $d_j = D_{ij}(d_i)$. Since $\varphi_{jk} \circ \varphi_{ij}$ is a morphism $i \to k$ and since there is a **unique** such morphism in $\mathcal{I}$ we must have $\varphi_{jk} \circ \varphi_{ij} = \varphi_{ik}$ and hence

$$D_{jk} \circ D_{ij} = D(\varphi_{jk}) \circ D(\varphi_{ij}) = D(\varphi_{jk} \circ \varphi_{ij}) = D(\varphi_{ik}) = D_{ik}.$$

It follows that $d_k = D_{jk}(d_j) = D_{jk}(D_{ij}(d_i)) = D_{ik}(d_i)$ and hence $(i, d_i) \sim (k, d_k)$. After this we define for each $i \in \mathbb{N}$ the function $\lambda_i : D_i \to \cup_{n\in\mathbb{N}} D_n$ that sends $d_i \in D_i$ to the equivalence class of $(i, d_i)$ in $\cup_{n\in\mathbb{N}} D_n$.

That was just the definition; there is still a lot of work to do. Next we need to prove that $(\cup_{n\in\mathbb{N}} D_n, \{\lambda_n\}_{n\in\mathbb{N}})$ satisfies the universal property of the colimit in the category of sets. To make the colimit into an $R$-module we will then define for $i, j \in \mathbb{N}$ and $r \in R$ the operations

$$(i, d_i) + (j, d_j) = (K, D_{kK}(d_k) + d_K) \qquad \text{and} \qquad r(i, d_i) = (i, rd_i),$$

where $k = \min\{i, j\}$ and $K = \max\{i, j\}$. Finally, one needs to check that these operations are (1) well-defined, (2) make $\cup_{n\in\mathbb{N}} D_n$ into an $R$-module, and (3) that the $R$-module structure is preserved by all the commutative diagrams. I spent a while writing down a proof of this; I realized that the proof was way too long; and then I regretted wasting time on it. □

[Remark: It was a bit tricky to see that the underlying index category of a kernel has **two parallel morphisms**, one of which gets sent to the zero morphism. More generally, we can consider

diagrams $D : \mathcal{I} \to \mathcal{C}$ in which the two parallel arrows get sent to two arbitrary morphisms $\varphi$ and $\psi$. The limit of such a diagram (if it exists) is called the "equalizer" of $\varphi$ and $\psi$; if you decode the definition in the category of sets you will see why.]

**Problem 2. Length Equals Dimension For Vector Spaces.** Consider a field $K$ and a vector space $V \in K$-Vec. Recall that a composition series of length $n$ is a chain of subspaces

$$0 = V_0 \subsetneq V_1 \subsetneq \cdots \subsetneq V_n = V$$

in which each quotient $V_{i+1}/V_i$ is simple (i.e. has no nontrivial subspaces). Prove that $V$ has a composition series of length $n$ if and only if it has a basis of size $n$. Hence the length of a vector space is the same as its dimension.

*Proof.* First, suppose that $b_1, b_2, \ldots, b_n \in V$ is a basis. Now let $V_0 := (0) = 0$ and for each $1 \leq i \leq n$ define the subspace

$$V_k := (b_1, b_2, \ldots, b_k).$$

I claim that for each $1 \leq k < n$ the quotient $V_{k+1}/V_i$ is simple. Indeed, let $W \subseteq V_{k+1}/V_i$ be a subspace that is not the trivlal subspace $(0 + V_k)$. Then there exists a coset $a + V_k$ in $W$ such that $a \in V_{k+1} \setminus V_k$. By definition of $V_{k+1}$ we can write

$$a = \sum_{i=1}^{k+1} r_i b_i$$

for some $r_1, \ldots, r_{k+1} \in K$ and since $a \notin V_k$ we must have $r_{k+1} \neq 0$. Then since $K$ is a field we can divide by $r_{k+1}$ to get

$$b_{k+1} = \frac{1}{r_{k+1}} a - \sum_{i=1}^{k} \frac{r_i}{r_{k+1}} b_i. \tag{1}$$

Finally, consider an arbitrary coset $b + V_k$ in $V_{k+1}/V_k$. Since $b \in V_{r+1}$ we can write

$$b = \sum_{i=1}^{k+1} s_i b_i$$

for some $s_1, \ldots, s_{k+1} \in K$. Then replacing $b_{k+1}$ by the expression (1) gives

$$b = \frac{1}{r_{k+1}} a + \sum_{i=1}^{k} \left( s_i - \frac{r_i}{r_{k+1}} \right) b_i \in (a + V_k).$$

It follows that

$$V_{k+1}/V_k \subseteq (a + V_k) \subseteq W \subseteq V_{k+1}/V_k$$

and hence $W = V_{k+1}/V_k$ as desired.

Conversely, suppose that we have a chain of subspaces

$$0 = V_0 \subsetneq V_1 \subsetneq \cdots \subsetneq V_n = V$$

in which the quotient $V_{k+1}/V_k$ is simple for each $1 \leq k < n$. Then certainly $V_0$ has a basis of size zero (i.e. the empty set). Now let $1 \leq k < n$ and assume for induction that $V_k$ has a basis of size $k$, say

$$b_1, b_2, \ldots, b_k \in V_k.$$

In this case we will construct a basis for $V_{k+1}$ of size $k + 1$. Since $V_{k+1}/V_k$ is nontrivial there exists a coset $b + V_k$ with $b \in V_{k+1} \setminus V_k$ and since $V_{k+1}/V_k$ is simple we must have $V_{k+1}/V_k = (b + V_k)$. I claim that $b, b_1, b_2, \ldots, b_k \in V_{k+1}$ is a basis. To see that this set is spanning, consider an arbitrary element $a \in V_{k+1}$. Since $V_{k+1}/V_k = (b + V_k)$ there exists

$r \in K$ such that $a + V_k = rb + V_k$ and hence $a - rb \in V_k$. But then we have $r_1, r_2, \ldots, r_k \in K$ such that

$$a - rb = \sum_{i=1}^{k} r_i b_i$$

$$a = rb + \sum_{i=1}^{k} r_i b_i$$

as desired. To see that the set is independent, consider any $r, r_1, r_2, \ldots, r_{k+1} \in K$ such that

$$rb + \sum_{i=1}^{k} r_i b_i = 0.$$

If $r \neq 0$ then we can divide by $r$ to obtain $b = -\sum_{i=1}^{k} (r_i/r) b_i \in V_k$, which contradicts the fact that $b \notin V_k$. So we must have $r = 0$. But then since $b_1, b_2, \ldots, b_k$ is a linearly independent set we must have $r_1 = r_2 = \cdots = r_k = 0$, as desired. □

[Remark: There are two ways to view this result. (1) Assuming the Steinitz Exchange Lemma, we can view this as a proof of the Jordan–Hölder Theorem for vector spaces. (2) Assuming the Jordan–Hölder Theorem for vector spaces, we can view this as a proof of the Steinitz Exchange Lemma.]

**Problem 3. Localization of a Module.** Let $M$ be a module over a commutative ring $R$ and let $S \subseteq R$ be a submonoid. Then we define the set of "fractions"

$$S^{-1}M := \left\{ \left[\frac{m}{s}\right] : m \in M, s \in S \right\}$$

with the equivalence relation

$$\left[\frac{m}{s}\right] = \left[\frac{n}{t}\right] \quad \iff \quad \exists\, u \in S,\, u(sn - tm) = 0.$$

(a) Prove that this is indeed an equivalence relation.
(b) Prove that the operations

$$\left[\frac{m}{s}\right] + \left[\frac{n}{t}\right] = \left[\frac{sn + tm}{st}\right] \quad \text{and} \quad r\left[\frac{m}{s}\right] = \left[\frac{rm}{s}\right]$$

are well-defined.
(c) Prove that the operations from part (b) make $S^{-1}M$ into an $R$-module and that the map $M \to S^{-1}M$ defined by $m \mapsto [m/1]$ is an $R$-module homomorphism.

*Proof.* (a): Since $1 \in S$ we have for all $m \in M$ and $s \in S$ that $1(sm - sm) = 1 \cdot 0 = 0$ and hence $[m/s] = [m/s]$. Also, given $m, n \in M$ and $s, t, u \in S$ we have

$$u(sn - tm) = 0 \qquad \iff \qquad u(tm - sn) = 0$$

and hence $[m/s] = [t/n]$ if and only if $[t/n] = [m/s]$. We have shown that the relation is reflexive and symmetric. To show that the relation is transitive, assume that we have $[m/s] = [m'/s']$ and $[m'/s'] = [m'', s'']$ for some $m, m', m'' \in M$ and $s, s', s'' \in S$. Thus by definition there exist $u, v \in S$ such that

$$u(sm' - s'm) = 0 \qquad \text{and} \qquad v(s'm'' - s''m') = 0.$$

Then we have

$$0 = vs'' \cdot 0 + us \cdot 0$$

$$
\begin{aligned}
&= (vs'')(u(sm' - s'm)) + (us)(v(s'm'' - s''m')) \\
&= \cancel{vs''usm'} - vs''us'm + usvs'm'' - \cancel{usvs''m'} \\
&= uvs'sm'' - uvs's''m \\
&= (uvs')(sm'' - s''m),
\end{aligned}
$$

and since $uvs' \in S$ this implies that $[m/s] = [m''/s'']$ as desired. [Note that the commutativity of $R$ was heavily used here. I don't see how we could possibly do without it.]

(b): Suppose that we have $[m/s] = [m'/s']$ and $[n/t] = [n'/t']$ for some $m, m', n, n' \in M$ and $s, s', t, t' \in S$. Thus by definition there exist $u, v \in S$ such that

$$
u(sm' - s'm) = 0 \qquad \text{and} \qquad v(tn' - t'n) = 0.
$$

To prove that scalar multiplication is well-defined, consider any $r \in R$ and note that

$$
u(srm' - s'rm) = ru(sm' - s'm) = ru \cdot 0 = 0,
$$

hence $[rm/s] = [rm'/s']$. To prove that addition is well-defined note that we have $uv \in S$ with

$$
\begin{aligned}
(uv)(st(t'm' + s'n') - s't'(tm + sn)) &= uvstt'm' + uvsts'n' - uvs't'tm - uvs't'sn \\
&= vtt'(u(sm' - s'm)) + uss'(v(tn' - t'n)) \\
&= vtt' \cdot 0 + uss' \cdot 0 \\
&= 0,
\end{aligned}
$$

hence $[(tm + sn)/st] = [(t'm' + s'n')/s't']$.

(c): To see that $(S^{-1}M, +)$ is an abelian group first note that addition is commutative. Indeed, for all $[m/s]$ and $[n/t]$ in $S^{-1}M$ we have

$$
\left[\frac{m}{s}\right] + \left[\frac{n}{t}\right] = \left[\frac{sn + tm}{st}\right] = \left[\frac{tm + sn}{ts}\right] = \left[\frac{n}{t}\right] + \left[\frac{m}{s}\right].
$$

Note that $[0/1]$ is an identity element since for all $[m/s] \in S^{-1}M$ we have $[0/1] + [m/s] = [(1m + s0)/1s] = [m/s]$, and inverses are given by $-[m/s] = [(-m)/s]$ since we have $[m/s] + [(-m)/s] = [(s(-m) + sm)/ss] = [0/ss] = [0/1]$. Finally, note that addition is associative since for all $[m/s]$, $[m'/s']$ and $[m''/s'']$ in $S^{-1}M$ we have

$$
\begin{aligned}
\left[\frac{m}{s}\right] + \left(\left[\frac{m'}{s'}\right] + \left[\frac{m''}{s''}\right]\right) &= \left[\frac{m}{s}\right] + \left[\frac{s'm'' + s''m'}{s's''}\right] \\
&= \left[\frac{s(s'm'' + s''m') + (s's'')m}{s(s's'')}\right] \\
&= \left[\frac{(ss')m'' + s''(sm' + s'm)}{(ss')s''}\right] \\
&= \left[\frac{sm' + s'm}{ss'}\right] + \left[\frac{m''}{s''}\right] \\
&= \left(\left[\frac{m}{s}\right] + \left[\frac{m'}{s'}\right]\right) + \left[\frac{m''}{s''}\right].
\end{aligned}
$$

Now for all $r \in R$ define the function $\varphi_r : S^{-1}M \to S^{-1}M$ by $[m/s] \mapsto [rm/s]$. From part (b) we know that this function is well-defined. To see that $\varphi_r \in \mathrm{End}_{\mathsf{Ab}}(S^{-1}M)$ note that for all $[m/s]$ and $[n/t]$ in $S^{-1}M$ we have

$$
r\left(\left[\frac{m}{s}\right] + \left[\frac{n}{t}\right]\right) = r\left[\frac{sn + tm}{st}\right]
$$

$$
\begin{aligned}
&= \left[\frac{r(sn+tm)}{st}\right] \\
&= \left[\frac{srn+trm}{st}\right] \\
&= \left[\frac{rm}{s}\right] + \left[\frac{rn}{t}\right] \\
&= r\left[\frac{m}{s}\right] + r\left[\frac{n}{t}\right].
\end{aligned}
$$

Then to see that $\varphi : R \to \mathrm{End}_{\mathsf{Ab}}(S^{-1}M)$ is a ring homomorphism first note that for all $[m/s] \in S^{-1}M$ we have $1[m/s] = [m/s] = \mathrm{id}_{S^{-1}M}([m/s])$. Then note that for all $[m/s] \in S^{-1}M$ and $r_1, r_2 \in R$ we have

$$
(r_1 r_2)\left[\frac{m}{s}\right] = \left[\frac{(r_1 r_2)m}{s}\right] = \left[\frac{r_1(r_2 m)}{s}\right] = r_1\left[\frac{r_2 m}{s}\right] = r_1\left(r_2\left[\frac{m}{s}\right]\right),
$$

and

$$
\begin{aligned}
r_1\left[\frac{m}{s}\right] + r_2\left[\frac{m}{s}\right] &= \left[\frac{r_1 m}{s}\right] + \left[\frac{r_2 m}{s}\right] \\
&= \left[\frac{sr_1 m + sr_2 m}{ss}\right] \\
&= \left[\frac{s(r_1+r_2)m}{ss}\right] \\
&= \left[\frac{(r_1+r_2)m}{s}\right] \\
&= (r_1+r_2)\left[\frac{m}{s}\right].
\end{aligned}
$$

Finally, to see that $m \mapsto [m/1]$ is an $R$-module homomorphism $M \to S^{-1}M$ note that for all $m, n \in M$ and $r \in R$ we have

$$
\left[\frac{m+rn}{1}\right] = \left[\frac{m}{1}\right] + \left[\frac{rn}{1}\right] = \left[\frac{m}{1}\right] + r\left[\frac{n}{1}\right].
$$

□

[Remark: I've never seen that proof written out in full (you're welcome, internet). Proving that the relation "$\exists\, u \in S,\, u(sn - tm) = 0$" is transitive is definitely the trickiest part. Seeing the details emphasizes that the naive definition of localization doesn't generalize to noncommutative rings. In that case I suppose one would try to generalize the universal property of localization. We'll talk about the universal property later when we discuss "restriction and extension of scalars".]

**Problem 4. Rank Exists Over a Domain.** Let $R$ be an integral domain and let $S = R\backslash\{0\}$. Then we can identify the field of fractions $K = \mathrm{Frac}(R)$ with the localization $S^{-1}R$. Let $M$ be any $R$-module and let $A \subseteq M$ be any subset.

(a) Show that we can regard $S^{-1}M$ as a $K$-module.

(b) If $A$ is $R$-linearly independent in $M$ prove that the image of $A$ under $M \to S^{-1}M$ (let's call it $S^{-1}A$) is $K$-linearly independent in $S^{-1}M$.

(c) If $A \subseteq M$ is a **maximal** $R$-linearly independent subset prove that $S^{-1}A \subseteq S^{-1}M$ is a **maximal** $K$-linearly independent subset. Conclude that any two such sets have the same cardinality. [Hint: Let $A \subseteq M$ be $R$-linearly independent. Then we know from part (a) that $S^{-1}A \subseteq S^{-1}M$ is $K$-linearly independent. Suppose there exists

$n \in S^{-1}M \setminus S^{-1}A$ such that $S^{-1}A \cup \{n\}$ is $K$-linearly independent. Then we can write $n = [m/s]$ for some $m \in M \setminus A$ and $s \in S$. Show that the set $A \cup \{m\} \subseteq M$ is $R$-linearly independent.]

*Proof.* (a): We know from Problem 3 that $S^{-1}M$ is an $R$-module under the action $r[m/s] = [rm/s]$. To extend this to a $K$-module we will define

$$\left[\frac{a}{b}\right]\left[\frac{m}{s}\right] := \left[\frac{am}{bs}\right]$$

for all $a \in R$, $m \in M$, and $b, s \in S = R \setminus \{0\}$. To see that this operation is well-defined suppose that we have $[a/b] = [a'/b']$ in $S^{-1}R$ and $[m/s] = [m'/s']$ in $S^{-1}M$. That is, suppose there exist $u, v \in S$ such that

$$u(ba' - ab') = 0_R \qquad \text{and} \qquad v(sm' - s'm) = 0_M.$$

Now define the module element $n := sab'm' \in M$ and observe that

$$\begin{aligned}
(uv)(bsa'm' - b's'am) &= (uv)(bsa'm' - n + n - b's'am) \\
&= uvbsa'm' - uvn + uvn - uvb's'am \\
&= v(u(bsa'm' - n)) + u(v(n - b's'am)) \\
&= v(u(sba'm' - sab'm')) + u(v(sab'm' - b's'am)) \\
&= vs(u(ba' - ab'))m' + uab'(v(sm' - s'm)) \\
&= vs \cdot 0_R \cdot m' + uab' \cdot 0_M \\
&= 0_M.
\end{aligned}$$

Since $uv \in S$ this implies that $[(am)/(bs)] = [(a'm')/(b's')]$ as desired. Next, observe that for all $[a/b], [a'/b'] \in S^{-1}R$ and $[m/s], [m'/s'] \in S^{-1}M$ we have

$$\begin{aligned}
\left[\frac{a}{b}\right]\left(\left[\frac{m}{s}\right] + \left[\frac{m'}{s'}\right]\right) &= \left[\frac{a}{b}\right]\left[\frac{sm' + s'm}{ss'}\right] \\
&= \left[\frac{a(sm' + s'm)}{b(ss')}\right] \\
&= \left[\frac{ba(sm' + s'm)}{bbss'}\right] \\
&= \left[\frac{(bs)(am') + (bs')(am)}{(bs)(bs')}\right] \\
&= \left[\frac{am}{bs}\right] + \left[\frac{am'}{bs'}\right] \\
&= \left[\frac{a}{b}\right]\left[\frac{m}{s}\right] + \left[\frac{a}{b}\right]\left[\frac{m'}{s'}\right],
\end{aligned}$$

and

$$\begin{aligned}
\left(\left[\frac{a}{b}\right] + \left[\frac{a'}{b'}\right]\right)\left[\frac{m}{s}\right] &= \left[\frac{ba' + b'a}{bb'}\right]\left[\frac{m}{s}\right] \\
&= \left[\frac{(ba' + b'a)m}{bb's}\right] \\
&= \left[\frac{s(ba' + b'a)m}{sbb's}\right]
\end{aligned}$$

$$= \left[\frac{(bs)(a'm) + (b's)(am)}{(bs)(b's)}\right]$$
$$= \left[\frac{am}{bs}\right] + \left[\frac{a'm}{b's}\right]$$
$$= \left[\frac{a}{b}\right]\left[\frac{m}{s}\right] + \left[\frac{a'}{b'}\right]\left[\frac{m}{s}\right],$$

and, finally,

$$\left[\frac{a}{b}\right]\left(\left[\frac{a'}{b'}\right]\left[\frac{m}{s}\right]\right) = \left[\frac{a}{b}\right]\left[\frac{a'm}{b's}\right] = \left[\frac{a(a'm)}{b(b's)}\right] = \left[\frac{(aa')m}{(bb')s}\right] = \left[\frac{aa'}{bb'}\right]\left[\frac{m}{s}\right] = \left(\left[\frac{a}{b}\right]\left[\frac{a'}{b'}\right]\right)\left[\frac{m}{s}\right].$$

[Remark: I wrote the proof of (a) so that it applies to general commutative rings $R$, general $R$-modules $M$, and general submonoids $S \subseteq R$. I will emphasize that I've never seen a full proof of this written out (you're welcome, internet).]

(b): Let the set $A = \{m_a\}_{a \in A} \subseteq M$ be $R$-linearly independent and consider the set

$$S^{-1}A := \left\{\left[\frac{m_a}{1}\right]\right\}_{a \in A} \subseteq S^{-1}M.$$

If $S^{-1}A$ is not $K$-linearly independent then we have a nontrivial linear relation

$$\sum_{a \in A} \left[\frac{r_a}{s_a}\right]\left[\frac{m_a}{1}\right] = \left[\frac{0_M}{1}\right] \tag{2}$$

for some fractions $[r_a/s_a] \in K$. Note that $[r_a/s_a] = [0_R/1]$ if and only if $r_a = 0_R$ and recall from the definition of linear dependence that we must have $r_a = 0_R$ for all but finitely many $a \in A$. Now consider the product of denominators $s := \prod_{a \in A} s_a$ taken over the finitely many fractions whose numerator is nonzero. Since $R$ is an integral domain we must have $s \neq 0_R$. Now act on both sides of (2) by the scalar $[s/1] \in K$ to get

$$\sum_{a \in A} \left[\frac{sr_a}{s_a}\right]\left[\frac{m_a}{1}\right] = \left[\frac{0_M}{1}\right]. \tag{3}$$

For each $a \in A$ we will define the (nonzero) element $\hat{s}_a := \prod_{b \in A \setminus \{a\}} s_b$, so that $[sr_a/s_a] = [\hat{s}_a r_a/1]$. Thus (3) becomes

$$\sum_{a \in A} \left[\frac{\hat{s}_a r_a}{1}\right]\left[\frac{m_a}{1}\right] = \left[\frac{0_M}{1}\right]. \tag{4}$$

Finally, since the relation (2) was assumed to be nontrivial there exists $a' \in A$ such that $r_{a'} \neq 0_R$ and then since $R$ is a domain we have $\hat{s}_{a'} r_{a'} \neq 0_R$. It follows that $[\hat{s}_{a'} r_{a'}/1] \neq [0_R/1]$ and we conclude that (4) is a nontrivial $R$-linear relation among the elements of $A$. Contradiction.

(c): Now suppose that $A = \{m_a\}_{a \in A} \subseteq M$ is a **maximal** $R$-linearly independent set. We know from part (b) that the set $S^{-1}A = \{[m_a/1]\}_{a \in A} \subseteq S^{-1}M$ is $K$-linearly independent. I claim, in fact, that $S^{-1}A \subseteq S^{-1}M$ is a **maximal** $K$-linearly independent set. To prove this, suppose for contradiction that there exists an element $[m/s] \in S^{-1}M \setminus S^{-1}A$ such that the set $S^{-1}A \cup \{[m/s]\}$ is $K$-linearly independent. Note that $m \notin A$ since otherwise we would have a nontrivial $K$-linear relation

$$\left[\frac{1}{s}\right]\left[\frac{m}{1}\right] = \left[\frac{m}{s}\right]$$

among the elements of $S^{-1}A \cup \{[m/s]\}$, contradicting the maximality of $S^{-1}A$. But now we will show that the set $A \cup \{m\} \subseteq M$ is $R$-linearly independent, which will contradict the

maximality of $A$. To do this, suppose that we have an $R$-linear relation

$$rm + \sum_{a \in A} r_a m_a = 0_M$$

for some elements $r, r_a \in R$. Since $[r/1][m/1] = [rs/1][m/s]$, this induces the $K$-linear relation

$$\left[\frac{rs}{1}\right]\left[\frac{m}{s}\right] + \sum_{a \in A}\left[\frac{r_a}{1}\right]\left[\frac{m_a}{1}\right] = \left[\frac{0_M}{1}\right].$$

But we assumed that the set $S^{-1}A \cup \{[m/s]\}$ is $K$-linearly independent so this implies that $[r_a/1] = [0_R/1]$ (and hence $r_a = 0_R$) for all $a \in A$ and that $[rs/1] = [0_R/1]$ (and hence $rs = 0_R$). Since $s \neq 0_R$ and since $R$ is an integral domain this implies that $r = 0_R$.

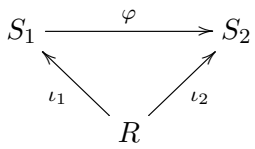
We conclude that $S^{-1}A$ is a maximal $K$-linearly independent subset of the $K$-vector space $S^{-1}M$. Finally, suppose that $B$ is any other maximal $R$-linearly independent subset of $M$, so that $S^{-1}B$ is another maximal $K$-linearly independent subset of $S^{-1}M$. Since $K$ is a field this implies that $S^{-1}A$ and $S^{-1}B$ are also minimal $K$-generating sets for $S^{-1}M$, hence they are bases. Then from the Steinitz Exchange Lemma we conclude that

$$|A| = |S^{-1}A| = |S^{-1}B| = |B|.$$

□

[Remark: And that's that. Believe it or not, this is the shortest proof I could find that the rank of a module over an integral domain is well-defined. If you know of a shorter proof please tell me. But please fill in all the details first to make sure that it really *is* shorter.]

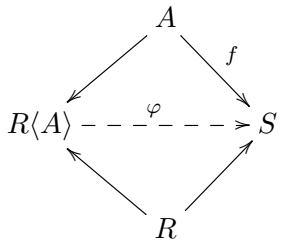
**Problem 5. The Category $R$-Alg.** Let $R$ be a ring. We define an $R$-algebra as a pair $(\iota, S)$ where $S$ is a ring and $\iota : R \to S$ is a ring homomorphism such that $\operatorname{im}\iota \subseteq Z(S)$. A morphism of $R$-algebras $\varphi : (\iota_1, S_1) \to (\iota_2, S_2)$ is defined as a ring homomorphism $\varphi : S_1 \to S_2$ such that




(a) Explain why $\mathbb{Z}$-Alg = Rng.

(b) Prove that an $R$-algebra $(\iota, S)$ is also an $R$-module in a natural way (i.e. by forgetting the monoid structure on $S$).

(c) Conversely, given any set $A$ there exists an $R$-algebra $R\langle A\rangle$ (called the free $R$-algebra generated by $A$) with the following universal property: For all set functions $f : A \to S$ there exists a unique $R$-algebra homomorphism $\varphi : R\langle A\rangle \to S$ such that




If $|A| = n$ then we can identify $R\langle A\rangle$ with the $R$-algebra $R\langle x_1, \ldots, x_n\rangle$ of polynomials in the $n$ **noncommuting indeterminates** $x_1, \ldots, x_n$. Use this idea to find the initial object in the category $R$-Alg.

(d) Given a subset $A \subseteq S$ of an $R$-algebra, let $i_A : R\langle A\rangle \to S$ be the unique $R$-algebra morphism defined in part (c). If $i_A$ is injective we say that the set $A$ is $R$-algebraically independent in $S$ and if $i_A$ is surjective we say $A$ is an $R$-algebraic generating set for $S$. If $i_A$ is bijective we say that $A$ is an $R$-algebra basis for $S$. Prove that an algebra basis is necessarily a **maximal** algebraically independent set and a **minimal** algebraic generating set. [To make notation easier you can assume that the basis is finite.]

*Proof.* This is one of those problems that doesn't ask you to do much; just to stare at some definitions and try to make sense of them. Unfortunately, there are various different definitions of the word "algebra" and I got them kind of muddled. Here are the standard possibilities:

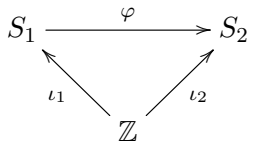
(A1) An $R$-algebra is a ring homomorphism $\iota : R \to S$ between general rings.

(A2) An $R$-algebra is a ring homomorphism $\iota : R \to S$ where $R$ is commutative and $\operatorname{im}\iota$ is contained in the center of $S$.

(A3) An $R$-algebra is a ring homomorphism $\iota : R \to S$ between commutative rings.

The definition I gave was similar to (A2) but I didn't require $R$ to be commutative. We'll see in a moment why that's probably not a good definition.

(a): Let $R = \mathbb{Z}$ and let $\iota : R \to S$ be an $R$-algebra under either of the definitions (A1) or (A2). That is, let $S$ be a general ring with a ring homomorphism $\iota : \mathbb{Z} \to S$. Since $\mathbb{Z}$ is the initial object in the category of rings we know that $\iota$ is uniquely determined so it gives us no extra information. If $\varphi : S_1 \to S_2$ is any ring homomorphism if $\iota_1 : \mathbb{Z} \to S_1$ and $\iota_2 : \mathbb{Z} \to S_2$ are the unique homomorphisms from $\mathbb{Z}$ then by uniqueness we must have $\iota_2 = \varphi \circ \iota_1$ and the following diagram commutes:




We conclude that objects of $\mathbb{Z}$-Alg are just rings and morphisms in $\mathbb{Z}$-Alg are just ring homomorphisms, hence $\mathbb{Z}$-Alg = Rng. If we use definition (A3) then $\mathbb{Z}$-Alg is isomorphic to the category of **commutative rings**.

(b): Let $\iota : R \to S$ be an $R$-algebra under any of the three standard definitions and let $|S|$ denote the underlying abelian group of the ring $S$. Now consider the function $\lambda$ that sends an element $r \in R$ to the function $\lambda_r : |S| \to |S|$ defined by $\lambda_r(s) := \iota(r)s$. Note that $\lambda_r$ is an endomorphism of $(|S|, +, 0)$ since for all $s, t \in |S|$ we have

$$\lambda_r(s+t) = \iota(r)(s+t) = \iota(r)s + \iota(r)t = \lambda_r(s) + \lambda_r(t).$$

Thus we have defined a function $\lambda : R \to \mathrm{End}_{\mathsf{Ab}}(|S|)$. To see that this is a ring homomorphism note that for all $r_1, r_2 \in R$ and $s \in |S|$ we have

$$\lambda_{r_1+r_2}(s) = \iota(r_1+r_2)s = (\iota(r_1)+\iota(r_2))s = \iota(r_1)s + \iota(r_2)s = \lambda_{r_1}(s) + \lambda_{r_2}(s),$$

and

$$\lambda_{r_1 r_2}(s) = \iota(r_1 r_2)s = (\iota(r_1)\iota(r_2))s = \iota(r_1)(\iota(r_2)s) = \lambda_{r_1}(\lambda_{r_2}(s)),$$

and, finally,

$$\lambda_{1_R}(s) = \iota(1_R)s = 1_S \cdot s = s.$$

(c): The word "conversely" here is supposed to suggest that we can also turn an $R$-module into an $R$-algebra in a canonical way. This should be a "free functor" $R$-Mod $\to R$-Alg that is left adjoint to the "forgetful functor" $R$-Alg $\to R$-Mod described in part (b). But then I didn't describe how to do this.

Instead, I described how to form the "free $R$-algebra" generated by a set $A$. The description of this free object will differ depending on the definition of $R$-algebra that you choose, but the general intuition is that free $R$-algebras are multivariate polynomial rings with coefficients from $R$. Suppose $|A| = n$. Then definition (A1) yields the ring $R\langle x_1, \ldots, x_n\rangle$ of polynomials in the $n$ noncommuting indeterminates $x_1, \ldots, x_n$ with coefficients from the ring $R$. These polynomials are a notational nightmare to write down. If we assume in the definition that the function $f : A \to S$ satisfies $\operatorname{im} f \subseteq Z(S)$ then we obtain the ring $R[x_1, \ldots, x_n]$ of polynomials in $n$ commuting indeterminates. We can express these as finite sums

$$f(x_1, \ldots, x_n) = \sum_{\alpha} r_\alpha x^\alpha$$

where $\alpha = (i_1, \ldots, i_n) \in \mathbb{N}^n$ is a multi-index and $x^\alpha := x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$. The other definitions of $R$-algebra yield various permutations of these ideas where coefficients and indeterminates are allowed or not allowed to commute among themselves or with each other. [Unfortunately, the category I defined seems not to have free objects because the putative homomorphism $R \to R\langle A\rangle$ would not map $R$ into the center of $R\langle A\rangle$.]

That was just me talking. I asked **you** to take this idea and use it to find the initial object in $R$-Alg. The punchline is that the initial object (when it exists) will be $R$ itself. Proof idea: We can think of $R$ as the ring of polynomials $R\langle\emptyset\rangle$ in zero indeterminates. Since for each ring $S$ there is a unique set function $\emptyset \to S$, the universal property of free algebras will guarantee that there is a unique $R$-algebra morphism $R\langle\emptyset\rangle \to S$. [Unfortunately this initial object does **not** exist for the definition of $R$-algebra that I gave because if $R$ is not commutative then the identity morphism $R \to R = R\langle\emptyset\rangle$ does not send $R$ into the center of itself.]

(d): Let $\iota : R \to S$ be an $R$-algebra and consider a subset $A = \{s_1, \ldots, s_n\} \subseteq S$. Choose some definition of $R$-algebra so the free algebra is isomorphic to a ring of polynomials $R\langle x_1, \ldots, x_n\rangle$ in $n$ indeterminates. In this case the canonical $R$-algebra homomorphism $i_A : R\langle x_1, \ldots, x_n\rangle \to S$ is called evaluation at $A$. For simplicity we will denote it as

$$f(x_1, \ldots, x_n) \mapsto f(s_1, \ldots, s_n).$$

Now assume that $A$ is an algebra basis, i.e., an algebraically independent algebraic generating set. To show that $A$ is maximally algebraically independent, consider any $s \in S \setminus A$. Since $A$ is algebraically generating there exists a polynomial $f(x_1, \ldots, x_n) \in R\langle x_1, \ldots, x_n\rangle$ such that

$$s = f(s_1, \ldots, s_n).$$

This nontrivial polynomial relation shows that the set $A \cup \{s\}$ is **not** algebraically independent. To show that $A$ is a minimal algebraic generating set, consider any $s_i \in A$ and assume for contradiction that $A \setminus \{s_i\}$ is also a generating set. Then there exists a polynomial $f(x_1, \ldots, x_n) \in R\langle x_1, \ldots, x_n\rangle$ such that

$$s_i = f(s_1, \ldots, s_n),$$

which is a nontrivial polynomial relation among the elements of $A$. Contradiction. □

[Remark: I'll admit that this problem was nonsense. I just wanted to get you thinking about the concept of multivariate polynomials and algebraic independence, and how these concepts are analogous to vector spaces and linear independence. The theories are formally similar and there is even an analogue of Steinitz Exchange for certain kinds of algebras, leading to the notion of "transcendence degree". It's a good exercise to try to prove Steinitz Exchange for general algebras to see how it fails. The attempt to make it work will force you to accept the tricky concept of "integral dependence".]