MATH 210A, FALL 2017
HW 3 SOLUTIONS
WRITTEN BY DAN DORE, EDITS BY PROF. CHURCH
(If you find any errors, please email ddore@stanford.edu)

Question 1. Consider a short exact sequence $0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$.
Prove that the following are equivalent.

(A) There exists a homomorphism $\sigma\colon C \to B$ such that $\beta \circ \sigma = \mathrm{id}_C$.

(B) There exists a homomorphism $\tau\colon B \to A$ such that $\tau \circ \alpha = \mathrm{id}_A$.

(C) There exists an isomorphism $\varphi\colon B \to A \oplus C$ under which α corresponds to the inclusion $A \hookrightarrow A \oplus C$ and β corresponds to the projection $A \oplus C \twoheadrightarrow C$.

When these equivalent conditions hold, we say the short exact sequence $0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$ *splits*. We can also equivalently say "$\beta\colon B \to C$ splits" (since by (i) this only depends on β) or "$\alpha\colon A \to B$ splits" (by (ii)).

Solution. (A) $\Longrightarrow$ (B): Let $\sigma\colon C \to B$ be such that $\beta \circ \sigma = \mathrm{id}_C$. Then we can define a homomorphism $P\colon B \to B$ by $P = \mathrm{id}_B - \sigma \circ \beta$. We should think of this as a *projection* onto A, in that P maps B into the submodule A and it is the identity on A (which is exactly what we're trying to prove). Equivalently, we must show $P \circ P = P$ and $\mathrm{im}(P) = A$. It's often useful to recognize the fact that a submodule $A \subseteq B$ is a direct summand iff there is such a projection.

Now, let's prove that P is a projection. We have $\beta \circ P = \beta - \beta \circ \sigma \circ \beta = \beta - \mathrm{id}_C \circ \beta = 0$. Thus, by the universal property of the kernel (as developed in HW2), P factors through the kernel $\alpha\colon A \to B$. In other words, there is a unique map $\tau\colon B \to A$ such that $\alpha \circ \tau = P$, i.e. the image of P is contained in the image of α. But then we have $\alpha \circ (\tau \circ \alpha) = P \circ \alpha = \alpha - \sigma \circ \beta \circ \alpha = \alpha$, since $\beta \circ \alpha = 0$. Thus, for all $a \in A$, $\alpha(a) = \alpha(\tau(\alpha(a)))$; since α is injective this means that $a = \tau(\alpha(a))$, or $\tau \circ \alpha = \mathrm{id}_A$..

(B) $\Longrightarrow$ (C): We define $\varphi\colon B \to A \oplus C$ by using the universal property of $A \oplus C \simeq A \times C$: a map from B to $A \times C$ is specified uniquely by specifying maps from B to A and B to C. So consider the map $\varphi = \tau \times \beta$, with $\tau\colon B \to A$ such that $\tau \circ \alpha = \mathrm{id}_A$. First, note that $p_2 \circ \varphi = \beta$, by definition of φ (see the previous homework problem on the universal property of direct sums/products), where p_1 is the projection $A \oplus C \longrightarrow\!\!\!\!\rightarrow C$. In addition, $\varphi \circ \alpha = (\tau \circ \alpha) \times (\beta \circ \alpha) = \mathrm{id}_A \times 0$: this is the map $A \longhookrightarrow A \oplus C$ given by inclusion of the first factor. So we're done once we show that φ is an isomorphism. To do this, assume that $\varphi(b) = 0$, which says exactly that $\beta(b) = 0$ and $\tau(b) = 0$. Since $\beta(b) = 0$, $b \in \ker \beta = \operatorname{im} \alpha$, so there is a unique (because α is injective) $a \in A$ such that $b = \alpha(a)$. Then, we have $0 = \varphi(b) = \varphi(\alpha(a)) = (\tau(\alpha(a)), \beta(\alpha(a))) = (a, 0)$, so $a = 0$ and thus $b = 0$ (here we used the hypothesis that $\tau \circ \alpha = \mathrm{id}_A$).

(C) $\Longrightarrow$ (A): Let $i_2\colon C \to A \oplus C$ be the inclusion of the direct summand C, i.e. $c \mapsto (0, c)$. We'll define $\sigma\colon C \to B$ as $\varphi^{-1} \circ i$. We need to show that $\beta \circ \sigma = \mathrm{id}_C$. But by assumption, $p_2 \circ \varphi = \beta$, with p_2 the canonical projection $A \oplus C \longrightarrow\!\!\!\!\rightarrow C$. Thus, $p_2 = \beta \circ \varphi^{-1}$, because φ is an isomorphism. Now, we have:

$$\beta \circ \sigma = \beta \circ \varphi^{-1} \circ i = p_2 \circ i_2 = \mathrm{id}_C$$

by definition of p_2 and i_2.

Question 2. Given an R-module, prove that the following are equivalent.

(A) Every short exact sequence $0 \to A \to B \to M \to 0$ splits.

(B) There exists some R-module N such that $M \oplus N$ is free.

When these equivalent conditions hold, we say that the R-module M is *projective*.

Solution. (A) $\implies$ (B): For *any* R-module M, there is a set I and a surjection $R^{\oplus I} \twoheadrightarrow M$ from a free module. It is important to understand why! (For example, we could take $I = M$ and map $e_m \mapsto m$ for each $m \in M$; this is obviously surjective.)

Then, letting A be the kernel of this surjection, we have a short exact sequence:

$$0 \to A \to R^I \to M \to 0$$

But by hypothesis (A), this short exact sequence splits. So in particular $M \oplus A \simeq R^I$, which is free.

(B) $\implies$ (A): Let

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r, "\alpha"] & B \arrow[r, "\beta"] & M \arrow[r] & 0 \end{tikzcd}$$

be an exact sequence, and let N be an R-module such that $M \oplus N \simeq F$, with F a free module. We want to show that the exact sequence splits, i.e. we have a map $\sigma \colon M \to B$ such that $\beta \circ \sigma = \mathrm{id}_M$. We use the following lemma, which is useful all over the place.

Lemma 1. Suppose that $0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$ and $0 \to D \xrightarrow{\delta} E \xrightarrow{\varepsilon} F \to 0$. Then

$$0 \to A \oplus D \xrightarrow{\alpha\oplus\delta} B \oplus E \xrightarrow{\beta\oplus\varepsilon} C \oplus F \to 0$$

is also a short exact sequence.

Proof. It suffices to observe that $\mathrm{im}(f \oplus g) = \mathrm{im}(f) \oplus \mathrm{im}(g)$ and $\ker(f \oplus g) = \ker(f) \oplus \ker(g)$. □

So by adding our original exact sequence to $0 \oplus 0 \oplus N \xrightarrow{\mathrm{id}_N} N \to 0$, we get an exact sequence:

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r, "\alpha\oplus 0"] & B \oplus N \arrow[r, "\beta\oplus\mathrm{id}_N"] & M \oplus N \arrow[r] & 0 \end{tikzcd}$$

Now, we have the following fact:

Lemma 2 (Free modules are projective)**.** Any exact sequence $0 \to A \to B \xrightarrow{\beta} F \to 0$ where F is a free module splits.

Proof. Let $(e_i)_{i\in I}$ be a basis for F. Since β is surjective, for each i we can choose $b_i \in B$ such that $\beta(b_i) = e_i$. Define the map $\sigma \colon F \to B$ by specifying $\sigma(e_i) = b_i$ (by the universal property of free modules, this defines a unique homomorphism $\sigma \colon F \to B$). Then, $\beta \circ \sigma(e_i) = \beta(b_i) = e_i$, so $\beta \circ \sigma$ and id_F are two R-module homomorphisms $F \to F$ which agree on the generating set $(e_i)_{i\in I}$, so they are equal (by Q1 on HW1). Thus, the exact sequence splits. □

Applying this to the current situation, using the fact that $M \oplus N$ is free, there is a homomorphism $\sigma_N \colon M \oplus N \to B \oplus N$ such that $(\beta \oplus \mathrm{id}_N) \circ \sigma_N = \beta \oplus \mathrm{id}_N$. Note that $\sigma_N(0, n) = (0, n)$ and $\sigma_N(b, 0) = (\text{something}, 0)$. Define $\sigma \colon B \to M$ by $\sigma_N(b) = (\sigma(b), 0)$. The fact that $(\beta \oplus \mathrm{id}_N) \circ \sigma_N = \beta \oplus \mathrm{id}_N$ implies $\beta \circ \sigma = \beta$, so this is the desired splitting of the original exact sequence.

Question 4. Let R be a commutative ring, and let M be a finitely generated R-module. Prove that if $\alpha\colon M \to M$ is surjective, then it is an isomorphism.

(Note the following useful consequence: any n elements that generate R^n are actually a basis of R^n.)

Solution. We first prove the seemingly-simpler statement:

Lemma 3. Let A be a commutative ring, and let M be a finitely generated A-module. Fix some $a \in A$. If multiplication by a is surjective (as a homomorphism $M \to M$), then it is injective (and thus an isomorphism).

Proof of lemma. We prove this by induction on the number of generators of M. First, assume that M is generated by a single element x. Since multiplication by a is surjective, choose y with $a \cdot y = x$. Since x generates M, we can write y as a linear combination $y = b \cdot x$ for some $b \in A$. Note that y also generates M (since $a \cdot y = x$, so linear combinations of y include those of x).

Suppose that $a \cdot z = 0$ for some $z \in M$. Since x generates M, we can write $z = c \cdot x$ for some $c \in A$. Now on the one hand we have

$$ba \cdot z = b \cdot (a \cdot z) = b \cdot 0 = 0.$$

But on the other hand, since A is commutative this is equal to

$$ba \cdot z = ba \cdot cx = bac \cdot x = c \cdot (a \cdot (b \cdot x)) = c \cdot (a \cdot y) = c \cdot x = z.$$

Therefore $z = 0$. This shows that $z \mapsto a \cdot z$ is injective, as desired. This concludes the base case.

We now assume that M is generated by $n + 1$ elements $x_1, \ldots, x_n, w$, and that the lemma is proved for all modules generated by $\leq n$ elements. Let $N \subset M$ be the submodule generated by $x_1, \ldots, x_n$.

First, we claim that multiplication by a is surjective as a homomorphism $M/N \to M/N$. Indeed, given any $\overline{m} \in M/N$, lift it to $m \in M$. By hypothesis, there exists $m' \in M$ with $a \cdot m' = m$; therefore

$$a \cdot \overline{m'} = \overline{a \cdot m'} = \overline{m}.$$

This shows that multiplication by a on M/N is surjective. Since M/N is generated by the single element $\overline{w}$, our base case implies that multiplication by a on M/N is *injective*.

We next claim that multiplication by a is surjective as a homomorphism $N \to N$. Consider $n \in N$. By hypothesis, there exists $p \in M$ with $a \cdot p = n$ (but we might worry that $p \notin N$). However, note that $a \cdot \overline{p} = \overline{a \cdot p} = \overline{n} = 0 \in M/N$. Since multiplication by a on M/N is injective, this implies $\overline{p} = 0 \in M/N$; in other words, $p \in N$. This verifies that multiplication by a on N is surjective. Since N is generated by n elements, our inductive hypothesis implies that multiplication by a on N is *injective*.

Now suppose that $a \cdot m = 0$ for some $m \in M$. We have $a \cdot \overline{m} = \overline{a \cdot m} = 0 \in M/N$. Since $\alpha_{M/N}$ is injective, this implies $\overline{m} = 0 \in M/N$; in other words, $m \in N$. But we know that multiplication by a is injective on N, so having $m \in N$ and $a \cdot m = 0$ implies that $m = 0$. Therefore multiplication by a on M is injective, as desired. □

To solve the original problem, we apply the lemma with $A = R[T]$. We define the structure of an A-module on M by $T \cdot m := \alpha(m)$; the universal property of polynomial rings means this uniquely defines an A-module structure. If M was generated by $x_1, \ldots, x_n$ as an R-module, it is certainly still generated by those elements as an A-module (since the A-linear combinations contain the R-linear combinations). So we can apply the lemma to conclude that multiplication by T is injective, i.e. that α is injective.

Question 5. Let M be a finitely generated R-module. Prove that the following are equivalent.

(A) There exists a short exact sequence $0 \to A \to F \to M \to 0$ where F is a finitely generated free module and A is finitely generated.

(B) For *every* short exact sequence $0 \to Q \to F \to M \to 0$ where F is a finitely generated free module, Q is finitely generated.

When these equivalent conditions hold, we say that the R-module M is *finitely presented.*

Solution. Since M is assumed to be finitely generated, there is always at least one short exact sequence of the form $0 \to A \to F \to M \to 0$ with F a free module, so the fact that (B) implies (A) is trivial. Let's show the converse. There are many different ways to proceed, all essentially equivalent (even if they look different).

Proof #1: (sketch) Suppose $x_1, \dots, x_n$ generate M, such that all linear dependences between the x_i are a consequence of finitely many relations, say ℓ relations (the x_i correspond to a basis for F and the relations correspond to generators for A).

Suppose we have another generating set $y_1, \dots, y_k$ for M. Since $x_1, \dots, x_n$ generate M, we can write $y_1 = a_1x_1 + \cdots + a_nx_n$, and similarly $y_2 = b_1x_1 + \cdots + b_nx_n$, and so on. Using these k relations, we can substitute to convert any dependence between the y_j into a linear combination of the x_i (which must be a linear dependence because it's equal to 0). But any dependence between the x_i is a consequence of our ℓ relations from above. Therefore we obtain $\ell + k$ relations between the y_j so that all relations among the y_j are a consequence.

(This proof is obviously sketchy, but you should keep it in mind when reading the argument below. Can you see which parts correspond to which parts?)

Proof #2: Fix a presentation $0 \to A \to F \xrightarrow{\beta} M \to 0$ with F free and A, F finitely generated. Now consider some other presentation $0 \to Q \to G \to M \to 0$ with G finitely generated and free. We must show that Q is finitely generated.

We can form a commutative diagram as below:

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r, "\alpha"] \arrow[d, "\psi"] & F \arrow[r, "\pi"] \arrow[d, "\varphi"] & M \arrow[r] \arrow[d, "="] & 0 \\
0 \arrow[r] & Q \arrow[r, "\alpha'"] & F' \arrow[r, "\pi'"] & M \arrow[r] & 0
\end{tikzcd}$$

In order to do this, we define φ by mapping each basis element e_i of F to some element $f_i \in F'$ such that $\pi'(f_i) = \pi(e_i)$. Then since $\pi' \circ \varphi = \pi$, φ maps $\ker \pi = \operatorname{im} \alpha$ into $\ker \pi' = \operatorname{im} \alpha'$, so we get the map ψ. We can also describe why ψ exists by the universal property of the kernel: $\pi' \circ (\varphi \circ \alpha) = (\pi' \circ \varphi) \circ \alpha = \pi \circ \alpha = 0$, so $(\varphi \circ \alpha)$ factors through $\alpha' \colon Q \to F$.

We can show that $Q/\operatorname{im}\psi \simeq F'/\operatorname{im}\varphi$ as follows: since $\alpha' \circ \psi = \varphi \circ \alpha$, α' maps $\operatorname{im}\psi$ into $\operatorname{im}\varphi$, so it induces a well-defined map $Q/\operatorname{im}\psi \to F'/\operatorname{im}\varphi$. Let $[q] \in Q/\operatorname{im}\psi$ be an element of the kernel of this map with $q \in Q$, so $\alpha'(q) = \varphi(f)$ for some $f \in F$. Since $\pi'(\alpha'(q)) = 0$, we get that $\pi'(\varphi(f)) = \pi(f) = 0$, so $f = \alpha(a)$ for some $a \in A$. Thus, $\alpha'(q) = \varphi(\alpha(a)) = \alpha'(\psi(a))$. Since α' is an injective homomorphism, this implies that $q = \psi(a)$, so $q \in \operatorname{im}\psi$ as desired. Thus, the map $Q/\operatorname{im}\psi \to F'/\operatorname{im}\varphi$ is injective. Now, let's see that it's also surjective. Let $f' \in F'$: we want to find some $q \in Q$ such that $\alpha'(q) = f' + \varphi(f)$ for some $f \in F$. Since π is surjective, there is some $f \in F$ such that $\pi(f) = \pi'(f')$. But $\pi(f) = \pi'(\varphi(f))$, so $\pi'(f' - \varphi(f)) = 0$. Thus, there is some $q \in Q$ such that $\alpha'(q) = f' - \varphi(f)$, which is exactly what we're looking for.

Now, $F'/\operatorname{im}\varphi$ is a quotient of the finitely generated module F', so it is finitely generated. In addition, $\operatorname{im}\psi$ is a quotient of the finitely generated module A, so it is finitely generated as well. Finally, we have an exact sequence $0 \to \operatorname{im}\psi \to Q \to Q/\operatorname{im}\psi \to 0$, so since $\operatorname{im}\psi$ and $Q/\operatorname{im}\psi$ are finitely generated, Q is finitely generated (by a previous homework exercise).

Question 7. If we set $L(f) = \frac{f}{S}$, this gives a set function

$$L\colon \operatorname{Hom}_R(M,N) \to \operatorname{Hom}_{R[\frac{1}{S}]}(S^{-1}M, S^{-1}N).$$

Observe that L is actually R-linear (you do not need to prove this).

Prove that if M is finitely presented, then L is the localization map of the R-module $\operatorname{Hom}_R(M,N)$. More precisely, for any M the universal property gives a map

$$L'\colon S^{-1}\operatorname{Hom}_R(M,N) \to \operatorname{Hom}_{R[\frac{1}{S}]}(S^{-1}M, S^{-1}N);$$

you must prove that if M is finitely presented, then L' is an isomorphism.

Solution. [1] First, we prove the theorem in the case when M is a finitely generated free module $F \cong R^k$. We can identify $\operatorname{Hom}_R(F,N)$ with the set of maps of sets from $\{e_1,\dots,e_k\}$ to N. Such a map is the same thing as an k-tuple of elements of N, so we can also identify $\operatorname{Hom}_R(F,N)$ with N^k.

If $F \cong R^k$ then $S^{-1}F \cong R[\frac{1}{S}]^k$, since S^{-1} commutes with direct sums. Furthermore, the $\frac{e_i}{1} = \ell(e_i)$ are a basis for $S^{-1}F$, so if f sends e_i to $n_i \in N$, then $\frac{f}{S}$ sends $\frac{e_i}{1}$ to $\frac{n_i}{1}$. Identifying $\operatorname{Hom}(S^{-1}F, S^{-1}N)$ with $(S^{-1}N)^k$ as above, we see that $L(n_1,\dots,n_k) = (\ell(n_1),\dots,\ell(n_k))$. Therefore L is none other than the localization map $N^k \to S^{-1}(N^k) \simeq (S^{-1}N)^k$, and L' is (under this identification) the identity.

We now want to use this to prove the theorem for a general finitely presented module M. Since M is finitely presented, there is some exact sequence:

$$F_1 \to F_2 \to M \to 0$$

with F_1, F_2 free and finitely generated (i.e. the kernel of $F_2 \twoheadrightarrow M$ is finitely generated, with generating set parametrized by a basis of F_1). By Question 3, we have an exact sequence:

$$0 \to \operatorname{Hom}(M,N) \to \operatorname{Hom}(F_2,N) \to \operatorname{Hom}(F_1,N)$$

In other words, we can identify $\operatorname{Hom}(M,N)$ with the kernel of the induced map $\operatorname{Hom}(F_2,N) \to \operatorname{Hom}(F_1,N)$. By question 6, we can apply S^{-1} to this to get an exact sequence

$$0 \to S^{-1}\operatorname{Hom}(M,N) \to S^{-1}\operatorname{Hom}(F_2,N) \to S^{-1}\operatorname{Hom}(F_1,N)$$

In other words,

$$S^{-1}\operatorname{Hom}(M,N) \text{ is the kernel of the map } S^{-1}\operatorname{Hom}(F_2,N) \to S^{-1}\operatorname{Hom}(F_1,N) \qquad (*)$$

Now back up and apply S^{-1} to our original exact sequence; by Question 6 we get:

$$S^{-1}F_1 \to S^{-1}F_2 \to S^{-1}M \to 0$$

and again by Question 3 we get:

$$0 \to \operatorname{Hom}(S^{-1}M, S^{-1}N) \to \operatorname{Hom}(S^{-1}F_2, S^{-1}N) \to \operatorname{Hom}(S^{-1}F_1, S^{-1}N)$$

[1] To make notation a little easier, I'm going to drop the subscripts on the Hom-modules; if A, B are R-modules, when I write $\operatorname{Hom}(A,B)$, I mean $\operatorname{Hom}_R(A,B)$, and when I write $\operatorname{Hom}(S^{-1}A, S^{-1}B)$ I mean $\operatorname{Hom}_{R[\frac{1}{S}]}(S^{-1}A, S^{-1}B)$

In other words,

$$\operatorname{Hom}(S^{-1}M, S^{-1}N) \text{ is the kernel of the map } \operatorname{Hom}(S^{-1}F_2, S^{-1}N) \to \operatorname{Hom}(S^{-1}F_1, S^{-1}N). \qquad (**)$$

We are now essentially done: the RHS of $(*)$ is isomorphic to the RHS of $(**)$ by applying the theorem to the free modules F_1 and F_2, so the LHS must be isomorphic too. Formally, we can fit the two "left-exact sequences" into a commutative diagram:

$$\begin{tikzcd}
0 \arrow[r] & S^{-1}\operatorname{Hom}(M,N) \arrow[r] \arrow[d, "L'"] & S^{-1}\operatorname{Hom}(F_2,N) \arrow[r] \arrow[d, equal, "L'"] & S^{-1}\operatorname{Hom}(F_1,N) \arrow[d, equal, "L'"] \\
0 \arrow[r] & \operatorname{Hom}(S^{-1}M, S^{-1}N) \arrow[r] & \operatorname{Hom}(S^{-1}F_2, S^{-1}N) \arrow[r] & \operatorname{Hom}(S^{-1}F_1, S^{-1}N)
\end{tikzcd}$$

(We could check that these all commute using the universal properties of localization.) This shows $S^{-1}\operatorname{Hom}(M,N)$ and $\operatorname{Hom}(S^{-1}M, S^{-1}N)$ are kernels of the "same map", and thus are isomorphic.

(TC: You can think about formal ways to phrase a proof of this last sentence, but that's not as important as understanding why it's true.)

Question 8. Give a counterexample to Q7 when M is not finitely presented, by exhibiting some $g\colon S^{-1}M \to S^{-1}N$ for which there do not exist $s \in S$ and $f\colon M \to N$ such that $s \cdot g = \frac{f}{S}$.
(Note: you don't have to take R to be some crazy ring for this.)

Solution. Let $R = \mathbb{Z}$, $M = \mathbb{Q}$, and $N = \mathbb{Z}$. Let $S = \mathbb{Z} \setminus \{0\}$ so $R[\frac{1}{S}] = \mathbb{Q}$. Then there is *no* nonzero homomorphism $f\colon M \to N$ (since $f(1)$ would have to be divisible by all integers). But $S^{-1}M \cong M \cong \mathbb{Q}$ and $S^{-1}N \cong \mathbb{Q}$, so we can take g to be the identity $\mathbb{Q} \to \mathbb{Q}$. □

In other words, we have

$$\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Q}, \mathbb{Z}) = 0 \qquad \text{but} \qquad \operatorname{Hom}_{\mathbb{Q}}(\mathbb{Q}, \mathbb{Q}) \cong \mathbb{Q} \neq 0.$$

Just for fun, let's see a counterexample where M is finitely generated but not finitely presented (for this we do need a rather crazy ring). Thanks to Carsten Sprunger for showing it to me.

Let R be the ring $\mathbf{Z}[x_1, \ldots, x_n, \ldots]/(2x_1, 4x_2, 8x_3, \ldots, 2^n x_n, \ldots)$.

Let I be the ideal $(x_1, x_2, \ldots, x_n, \ldots) \subseteq R$ so that $R/I \cong \mathbf{Z}$.

Let $M = R/I$, let $N = R$, and let $S = \{2, 4, 8, \ldots\}$.

Note that M is generated as an R-module by the element 1, so in particular it is finitely generated. We'll show that in this case, $L'\colon S^{-1}\operatorname{Hom}_R(M, N) \to \operatorname{Hom}_{R[\frac{1}{S}]}(S^{-1}M, S^{-1}N)$ is not surjective.

First off, note that $\ell\colon R \to R[\frac{1}{2}]$ maps x_n to 0 for each n, since $2^n x_n = 0$. In other words, $\ell(I) = 0$, so $S^{-1}(I) = 0$. Applying S^{-1} to the exact sequence $0 \to I \to N \to M \to 0$, we get $0 \to 0 \to S^{-1}N \to S^{-1}M \to 0$, so $S^{-1}N \to S^{-1}M$ is an isomorphism (even an isomorphism of rings).

Let $f \in \operatorname{Hom}_{R[\frac{1}{S}]}(S^{-1}M, S^{-1}N)$ be its inverse. This is a nonzero element of $\operatorname{Hom}_{R[\frac{1}{S}]}(S^{-1}M, S^{-1}N)$, so in particular this Hom-module is not zero. On the other hand, $\operatorname{Hom}_R(M, N) = 0$: by Question 3, a homomorphism φ of R-modules from R/I to R is the same thing as a homomorphism of R-modules from R to R which vanishes on I. In other words, $\operatorname{Hom}_R(M, N)$ is the set of $a \in R$ such that $a \cdot I = 0$, since a homomorphism of R-modules from the free module R to itself is just multiplication by some element of R. But such an a must be 0: if $a \cdot x_n = 0$, then $a = 2^n a'$ for some $a' \in R$, but this is impossible unless $a = 0$.

Note that this example can turn into an example over the ring $R = \mathbf{Z}[x_1, \ldots, x_n]$, by taking $M = R/((x_n)_{n \in \mathbf{N}})$ and $N = R/((2^n x_n)_{n \in \mathbf{N}})$; the Hom-modules we consider are exactly the same: if R is a ring, I is an ideal, and M, N are R-modules such that $I \cdot M = I \cdot N = 0$, then $\operatorname{Hom}_R(M, N) = \operatorname{Hom}_{R/I}(M, N)$.

Question 9. Given elements $r_1, \dots, r_k$ in a commutative ring R, prove the following are equivalent.

(A) These elements generate the unit ideal: $(r_1, \dots, r_k) = R$;
in other words, there exist $a_1, \dots, a_k \in R$ such that $a_1 r_1 + \cdots + a_k r_k = 1$.

(B) An R-module M is 0 $\iff$ the $R[\frac{1}{r_i}]$-module $M[\frac{1}{r_i}]$ is 0 for all $i = 1, \dots, k$.

Solution. (A) $\implies$ (B): Assume that $(r_1, \dots, r_k) = R$, and let M be an R-module. Note $M = 0 \implies M[\frac{1}{r_i}] = 0$ is trivial, so we only have to prove the other direction.

So assume that $M[\frac{1}{r_i}] = 0$ for all i, and choose an arbitrary $m \in M$. We will show that $m = 0$; since m was arbitrary this implies $M = 0$.

Our explicit definition of $M[\frac{1}{r_i}]$ tells us $\frac{m}{1} = 0$ iff $r^n \cdot m = 0$ for some n. Thus, for each i, there is some n_i such that $r_i^{n_i} m = 0$. Let's show that this implies $m = 0$.

Let $n = \sum_{i=1}^k n_i$, and choose $a_1, \dots, a_k \in R$ such that $a_1 r_1 + \cdots + a_k r_k = 1$. We have the following identity:

$$1 = 1^n = (a_1 r_1 + \cdots + a_k r_k)^n = \sum_{\substack{m_1, \dots, m_k \\ \sum_i m_i = n}} a_I \cdot r_1^{m_1} \cdot r_2^{m_2} \cdot \cdots \cdot r_k^{m_k}$$

where the a_I are some elements of R. But by the pigeonhole principle, for each term, at least one of the m_i must be at least n_i. Thus, $a_I \cdot r_1^{m_1} \cdots r_k^{m_k} \cdot m = 0$ for each such partition of n. Thus, multiplying both sides of the above identity by m, we get that $m = 0$.

(B) $\implies$ (A): Let $I = (r_1, \dots, r_k)$ be the ideal generated by $r_1, \dots, r_k$, and let M be the R-module R/I. We claim that $M[\frac{1}{r_i}] = 0$ for all i. Indeed, for all $m \in M$ we have $r_i \cdot m = 0$. Thus $\frac{m}{1} = 0 \in M[\frac{1}{r_i}]$, and so all $\frac{m}{r_i^k} = 0$.

If we now assume (B), it tells us that $R/I = 0$; in other words, $I = R$, as desired.

Question 10. Let R be a commutative ring, and let M be an R-module.
Prove that if M is **finitely presented**, the following are equivalent.

(A) M is projective. (see Q2)

(B) M is *locally free*, meaning there exist $r_1, \ldots, r_k$ in R with $(r_1, \ldots, r_k) = R$ such that $M[\frac{1}{r_i}]$ is a free $R[\frac{1}{r_i}]$-module for all $i = 1, \ldots, n$.

(C) M_P is a free R_P-module for all prime ideals P.

(D) $M_\mathfrak{m}$ is a free $R_\mathfrak{m}$-module for all maximal ideals $\mathfrak{m}$.

Solution. We'll prove (B) $\implies$ (A) $\implies$ (C) $\implies$ (D) $\implies$ (B).

(B) $\implies$ (A): Consider an exact sequence $0 \to K \to F \xrightarrow{\pi} M \to 0$ with F finitely generated and free and K finitely generated. By Question 2, in order to show that M is projective, it is necessary and sufficient to show that this short exact sequence splits, i.e. that there is some map $\sigma : M \to F$ such that $\pi \circ \sigma = \mathrm{id}_M$ (since this implies that $F \simeq M \oplus K$). In other words, the short exact sequence splits if and only if id_M is in the image of the R-module homomorphism $p = \pi_* \colon \operatorname{Hom}_R(M, F) \to \operatorname{Hom}_R(M, M)$ (where $p(f) = \pi \circ f$).

We claim this holds if and only if p is surjective. One direction is obvious: if p is surjective then id_M is in the image. Conversely, if the short exact sequence splits then $\operatorname{Hom}_R(M, F) \simeq \operatorname{Hom}_R(M, M) \oplus \operatorname{Hom}_R(M, K)$ and π_* corresponds to projection onto the first factor, which is certainly surjective.

Fix $r_1, \ldots, r_k$ with $(r_1, \ldots, r_k) = R$. We know from class (plus Question 9 for the last equivalence) that for an R-module X we have

$$X = 0 \iff X_P = 0 \,\forall P \iff X_\mathfrak{m} = 0 \,\forall \mathfrak{m} \iff X[\frac{1}{r_i}] = 0 \,\forall i.$$

Similarly, for an R-module homomorphism $f \colon Y \to Z$, we have (applying the previous equivalences to $X = \operatorname{coker}(f)$):

$$f \text{ surjective} \iff f_P \text{ surjective } \forall P \iff f_\mathfrak{m} \text{ surjective } \forall \mathfrak{m} \iff f[\tfrac{1}{r_i}] \text{ surjective } \forall i.$$

Therefore we have

$$\begin{aligned} M \text{ projective} &\iff p\colon \operatorname{Hom}_R(M, F) \to \operatorname{Hom}_R(M, M) \text{ surjective} \\ &\iff p_P\colon \operatorname{Hom}_R(M, F)_P \to \operatorname{Hom}_R(M, M)_P \text{ surjective } \forall P \\ &\iff p_\mathfrak{m}\colon \operatorname{Hom}_R(M, F)_\mathfrak{m} \to \operatorname{Hom}_R(M, M)_\mathfrak{m} \text{ surjective } \forall \mathfrak{m} \\ &\iff p[\tfrac{1}{r_i}]\colon \operatorname{Hom}_R(M, F)[\tfrac{1}{r_i}] \to \operatorname{Hom}_R(M, M)[\tfrac{1}{r_i}] \text{ surjective } \forall i \end{aligned}$$

However, our M is finitely presented, so we may **apply Question 7** which describes the localizations of $\operatorname{Hom}_R(M,F)$: we have $\operatorname{Hom}_R(M,N)_P = \operatorname{Hom}_{R_P}(M_P,N_P)$, and $\operatorname{Hom}_R(M,N)_{\mathfrak{m}} = \operatorname{Hom}_{R_{\mathfrak{m}}}(M_{\mathfrak{m}},N_{\mathfrak{m}})$, and $\operatorname{Hom}_R(M,N)[\frac{1}{r_i}] = \operatorname{Hom}_{R[\frac{1}{r_i}]}(M[\frac{1}{r_i}],N[\frac{1}{r_i}])$. Therefore

$$\begin{aligned} M \text{ projective} &\iff p\colon \operatorname{Hom}_R(M,F) \to \operatorname{Hom}_R(M,M) \text{ surjective} \\ &\iff \operatorname{Hom}_{R_P}(M_P,F_P) \to \operatorname{Hom}_{R_P}(M_P,M_P) \text{ surjective } \forall P \\ &\iff \operatorname{Hom}_{R_{\mathfrak{m}}}(M_{\mathfrak{m}},F_{\mathfrak{m}}) \to \operatorname{Hom}_{R_{\mathfrak{m}}}(M_{\mathfrak{m}},M_{\mathfrak{m}}) \text{ surjective } \forall \mathfrak{m} \\ &\iff \operatorname{Hom}_{R[\frac{1}{r_i}]}(M[\tfrac{1}{r_i}],F[\tfrac{1}{r_i}]) \to \operatorname{Hom}_{R[\frac{1}{r_i}]}(M[\tfrac{1}{r_i}],M[\tfrac{1}{r_i}]) \text{ surjective } \forall i \end{aligned}$$

But since F_P is a free module (and $F_{\mathfrak{m}}$ and $F[\frac{1}{r_i}]$ too), the argument at the beginning of this section shows

$$\begin{aligned} \operatorname{Hom}_{R_P}(M_P,F_P) \to \operatorname{Hom}_{R_P}(M_P,M_P) \text{ surjective} &\iff M_P \text{ projective} \\ \operatorname{Hom}_{R_{\mathfrak{m}}}(M_{\mathfrak{m}},F_{\mathfrak{m}}) \to \operatorname{Hom}_{R_{\mathfrak{m}}}(M_{\mathfrak{m}},M_{\mathfrak{m}}) \text{ surjective} &\iff M_{\mathfrak{m}} \text{ projective} \\ \operatorname{Hom}_{R[\frac{1}{r_i}]}(M[\tfrac{1}{r_i}],F[\tfrac{1}{r_i}]) \to \operatorname{Hom}_{R[\frac{1}{r_i}]}(M[\tfrac{1}{r_i}],M[\tfrac{1}{r_i}]) \text{ surjective} &\iff M[\tfrac{1}{r_i}] \text{ projective} \end{aligned}$$

So combining with the previous equivalences, we've showed that **when M is finitely presented**:

$$\begin{aligned} M \text{ projective} &\iff M_P \text{ projective } \forall P \\ &\iff M_{\mathfrak{m}} \text{ projective } \forall \mathfrak{m} \\ &\iff M[\tfrac{1}{r_i}] \text{ projective } \forall i \end{aligned}$$

In particular, since free modules are projective, we see that any of (B) or (C) or (D) implies (A).

(A) $\implies$ (C): Since M is finitely generated, we have a short exact sequence:

$$0 \to N \to F \to M \to 0$$

with $F \cong R^n$ finitely generated and free. Since M is projective, this implies that $M \oplus N \simeq F$. So we've shown that a finitely generated projective module is automatically a direct summand of a *finitely generated* free module.[2] This implies that $F_P \simeq M_P \oplus N_P$, and $F_P \cong R_P^n$ is free because $F \cong R^n$ is. So M_P is a finitely generated projective module over the local ring R_P. It remains to show that such an M_P is free.

Now, let $m_1, \dots, m_\ell$ be a set of generators of M_P such that ℓ is as small as possible, and $n_1, \dots, n_k$ a set of generators of N_P such that k is as small as possible. Now, let $\overline{F} = F_P/PF_P$, $\overline{M} = M_P/PM_P$, and $\overline{N} = N_P/PN_P$; these are all finitely generated modules over the field R_P/PR_P. Since $m_1, \dots, m_\ell$ generate M_P, the images of $m_1, \dots, m_\ell$ span $\overline{M}$. Thus, some subset of size $\ell' \leq \ell$ of these elements form a basis for $\overline{M}$. However, Nakayama's lemma implies that if some set of elements of the finitely generated module M_P form a basis of $\overline{M}$, then they generate M_P. Thus, since we assumed ℓ was as small as possible, $\ell' = \ell$ and the images of $m_1, \dots, m_\ell$ are linearly independent in

[2] Note that since N is a direct summand of F as well, N is also finitely generated. Thus, a finitely generated projective module is automatically finitely presented.

$\overline{M}$. Similarly, the images of $n_1, \ldots, n_k$ are linearly independent in $\overline{N}$. But since $\overline{F} = \overline{M} \oplus \overline{N}$, this says that the images of $m_1, \ldots, m_\ell, n_1, \ldots, n_k$ are linearly independent in $\overline{F}$, i.e. they form a basis of $\overline{F}$. Since $\dim \overline{F} = \operatorname{rank}(F_P)$, this says that $F_P \simeq R_P^{\ell+k}$. But the $\ell + k$ elements $m_1, \ldots, m_\ell, n_1, \ldots, n_k$ generate F_P, so they must actually be a basis by Question 4. In particular, they are linearly independent over R_P, so M_P and N_P are free.

If we pick our free module more parsimoniously, we can simplify the proof (and avoid using Q4): let $m_1, \ldots, m_k$ be a set of generators of M_P of minimal size, and let $F_P = R^k$. (There is not really an F here, but it doesn't matter.) Then the map sending the basis elements of F_P to the m_i is a surjection $F_P \to M_P \to 0$. Since M_P is projective we have $F_P \simeq M_P \oplus N_P$, and thus $k = \dim \overline{F} = \dim \overline{M} + \dim \overline{N}$. But as we saw above, since k is as small as possible, the m_i need to be linearly independent in $\overline{M}$ by Nakayama's lemma, so $\dim \overline{M} = k$, and thus $\overline{N} = 0$. Then by Nakayama's lemma again, this implies $N_P = 0$, so $M_P \cong F_P$.

(C) $\implies$ (D): Trivial, since maximal ideals are prime.

(D) $\implies$ (B): The key is the following lemma.

Lemma 4. If M is a finitely presented R-module and $\mathfrak{m}$ is a maximal ideal of R such that $M_\mathfrak{m}$ is free, then there is some $f \in R, f \notin \mathfrak{m}$ such that $M[\frac{1}{f}]$ is free.

The proof of this lemma is rather long, so we give it below. For now, we use it to prove (D) $\implies$ (B). If (D) is true, then for *every* maximal ideal $\mathfrak{m}$ of R, there is some $f_\mathfrak{m} \in R \setminus \mathfrak{m}$ such that $M[\frac{1}{f_\mathfrak{m}}]$ is free. Consider the ideal Igenerated by $(f_\mathfrak{m})$ where $\mathfrak{m}$ ranges over all maximal ideals of R. For every maximal ideal $\mathfrak{m}$, $f_\mathfrak{m} \notin \mathfrak{m}$, so $I \not\subset \mathfrak{m}$. Thus, I is not contained in any maximal ideal, so $I = (1)$. In particular, we have some equation $1 = a_1 f_{\mathfrak{m}_1} + a_2 f_{\mathfrak{m}_2} + \cdots + a_k f_{\mathfrak{m}_k}$. Thus, we can take $f_k = f_{\mathfrak{m}_k}$, and this says $(f_1, \ldots, f_k) = 1$ and $M[\frac{1}{f_k}]$ is free.

Proof of Lemma 4. [3] We have an isomorphism $\varphi_\mathfrak{m} \colon F_\mathfrak{m} \xrightarrow{\sim} M_\mathfrak{m}$, where F is a finitely generated free R-module. To prevent notation from getting out of hand, we'll prove this by repeatedly invoking the following more general claim:

[3] This is a prototypical example of a very general phenomenon, often called "spreading out". If I have a finitely presented module over a (commutative) ring R, then if a statement is true after localizing at a prime ideal P, it is already true after inverting some $f \in R - P$. In geometric language, "a property which is true at a point is true in an open neighborhood of a point". This sort of statement generalizes in many different directions. Rather than modules over a ring, we could consider some more general algebraic or algebro-geometric structures which have a notion of "finitely presented" (for example, if $A \to B$ is a ring homomorphism, we can say when B is finitely presented as an A-algebra). Also, instead of localization at a prime vs. localization at an element, we can talk about any process that is in some sense a "limit" of finite versions of the process. In our context, localizing at a prime corresponds to inverting *every* element of the (usually) infinite set $R \setminus P$, and localizing at an element corresponds to inverting some finite subset of $R \setminus P$ (using the fact that inverting finitely many elements is the same thing as inverting their product).

Claim 5. Let M, N be modules over a ring R, and let P be a prime ideal of R. Then the following statements are true:

(i) If M is finitely generated and $f, g\colon M \to N$ are two homomorphisms such that $f_P = g_P$ as homomorphisms $M_P \to N_P$, then there is some $r \notin P$ such that $f[\frac{1}{r}] = g[\frac{1}{r}]$ as homomorphisms $M[\frac{1}{r}] \to N[\frac{1}{r}]$.

(ii) If M is finitely presented and $f_P\colon M_P \to N_P$ is a homomorphism, then there is some $r \notin P$ and a homomorphism $f : M[\frac{1}{r}] \to N[\frac{1}{r}]$ such that $f_P = \frac{f}{S}$ with $S = R - P$.

Now, to prove Claim 4 from Claim 5, we can first apply part (ii) to $\varphi_{\mathfrak m}$ and $\psi_{\mathfrak m} = \varphi_{\mathfrak m}^{-1}$. This gives us some $r_0, r_0' \notin P$ and homomorphisms $\varphi_0\colon F[\frac{1}{r_0}] \to M[\frac{1}{r_0}], \psi_0\colon M[\frac{1}{r_0'}] \to F[\frac{1}{r_0'}]$ with $(\varphi_0)_{\mathfrak m} = \varphi_{\mathfrak m}$ and $(\psi_0)_{\mathfrak m} = \psi_{\mathfrak m}$. Now we can invert the element $r_1 := r_0 r_0'$ and localize φ_0, ψ_0 to get maps

$$\varphi_1 := \varphi_0[\frac{1}{r_0'}]\colon F[\frac{1}{r_1}] \to M[\frac{1}{r_1}], \qquad \psi_1 := \psi_0[\frac{1}{r_0}]\colon M[\frac{1}{r_1}] \to F[\frac{1}{r_1}]$$

Since everything we've inverted is not in $\mathfrak m$, we've preserved the property that $(\varphi_1)_{\mathfrak m} = \varphi_{\mathfrak m}$ and $(\psi_1)_{\mathfrak m} = \psi_{\mathfrak m}$.[4]

We hope that $\psi_1 = \varphi_1^{-1}$, but this might not be true yet. However, we know that $(\psi_1 \circ \varphi_1)_{\mathfrak m} = (\psi_1)_{\mathfrak m} \circ (\varphi_1)_{\mathfrak m} = \psi_{\mathfrak m} \circ \varphi_{\mathfrak m} = \mathrm{id}_{F_{\mathfrak m}} = (\mathrm{id}_{F[\frac{1}{r_1}]})_{\mathfrak m}$ and likewise $(\varphi_1 \circ \psi_1)_{\mathfrak m} = (\mathrm{id}_{M[\frac{1}{r_1}]})_{\mathfrak m}$. Now, let's rename $R[\frac{1}{r_1}]$ as R and likewise for M and F. We can invoke (i) twice, to get $r_2, r_2' \notin P$ such that $(\psi_1 \circ \varphi_1)[\frac{1}{r_2}] = (\mathrm{id}_F)[\frac{1}{r_2}]$ and $(\varphi_1 \circ \psi_1)[\frac{1}{r_2'}] = (\mathrm{id}_M)[\frac{1}{r_2'}]$. Inverting $r_3 = r_2 r_2'$, we see that $\psi_3 := \psi_1[\frac{1}{r_3}]$ and $\varphi_3 := \varphi_1[\frac{1}{r_3}]$ are inverse to each other, so $M[\frac{1}{r_3}] \simeq F[\frac{1}{r_3}]$.

Remember that we renamed our original $M[\frac{1}{r_1}]$ as M and likewise for F, so what we've actually proved is that for $r_4 = r_1 r_3$, we have $M[\frac{1}{r_4}] \simeq F[\frac{1}{r_4}]$, so $M[\frac{1}{r_4}]$ is free.

Now, let's prove Claim 5:

(i) By replacing f, g with $f - g, 0$, it suffices to prove the statement in the case $g = 0$, i.e. we want to show that if $f_P = 0$ then $f[\frac{1}{r}] = 0$ for some $r \notin P$. Let $m_1, \dots, m_n$ be generators for M. Then since $f_P = 0$, in particular, $f_P(\ell_M(m_i)) = 0 \in N_P$ for $1 \leq i \leq n$ with $\ell_M : M \to M_P$ the localization map. But $f_P(\ell_M(m_i)) = \ell_N(f(m_i))$ (by the definition of $S^{-1}f$), so for each $1 \leq i \leq n$ there is some $r_i \notin P$ such that $r_i f(m_i) = 0$. Letting $r = r_1 \cdot r_2 \cdot \dots \cdot r_n$ we see that $rf(m_i) = 0$ for each i. Thus, $f[\frac{1}{r}](m_i) = 0$ in $N[\frac{1}{r}]$. But (the images of) m_i generate $M[\frac{1}{r}]$, so $f[\frac{1}{r}] = 0$, as desired.

(ii) We already showed in Question 7 that the natural restriction map $L\colon f \mapsto \frac{f}{S}$ may be canonically identified with the localization map

$$\mathrm{Hom}_R(M, N) \xrightarrow{\ell} S^{-1}\,\mathrm{Hom}_R(M, N) \xrightarrow{L'} \mathrm{Hom}_{S^{-1}R}(S^{-1}M, S^{-1}N)$$

i.e. L' is an isomorphism. Since L' and ℓ moreover commute with varying S (i.e. if $r \notin P$, the L' sending f to f_P factors through the L' sending f to $f[\frac{1}{r}]$, and similarly for ℓ), we can see that Claim

[4] This comes from the fact that if $S_0 \subseteq S_1$, then $S_1^{-1}(S_0^{-1}M) \simeq S_1^{-1}M$, and this isomorphism takes the localization map $\ell_{1,M}\colon M \to S_1^{-1}M$ to $\ell_{1,S_0^{-1}M} \circ \ell_{0,M}$, with $\ell_{1,S_0^{-1}M}\colon S_0^{-1}M \to S_1^{-1}(S_0^{-1}M)$ and $\ell_{0,M}\colon M \to S_0^{-1}M$ the localization maps. This statement is *much* harder to state than it is to prove!

4 (ii) is equivalent to the statement that if $f_P \in \big(\mathrm{Hom}_R(M,N)\big)_P$, there is some $r \notin P$ and some $f \in \big(\mathrm{Hom}_R(M,N)\big)\,[\frac{1}{r}]$ such that the image of f in $\big(\mathrm{Hom}_R(M,N)\big)_P$ is equal to f_P.

Now, this is a perfectly general fact: if M is any module whatsoever and $m \in M_P$, there is some r such that m lifts to $M[\frac{1}{r}]$. Indeed, this is clear from the very definition of M_P: we can write $m = \frac{m_0}{r}$ with $m_0 \in M, r \notin P$, so this gives us the lift we want.

Remember that the proof of Question 7 works by using a finite presentation $F_2 \to F_1 \to M \to 0$ to identify $\mathrm{Hom}_R(M,N)$ with the set of maps from F_1 to N which vanish on the image of F_2, and similarly for $\mathrm{Hom}_{S^{-1}R}(S^{-1}M, S^{-1}N)$. So if we hadn't yet proved Question 7, we could directly prove Claim 4 this way, i.e. by considering the image of the basis elements of $(F_1)_P$ in N_P and finding an r such that they lift to $N[\frac{1}{r}]$, then finding a possibly "bigger" r' (i.e. replacing r with $r' = rr''$) which makes all of the relations coming from F_2 trivial in $N[\frac{1}{r'}]$. But this is essentially just repeating the argument we already gave!

□

(See last page for comments on what happens if we don't assume finite presentation.)

Question 11. (Hard) Extend the equivalence in Q10 to include the following equivalent condition (still under the assumption that M is finitely presented):

(E) Every linear dependence in M is trivial, in the sense below.

A linear dependence in M is a list of module elements $m_1, \ldots, m_n \in M$ and ring elements $r_1, \ldots, r_n \in R$ such that $r_1 m_1 + \cdots + r_n m_n = 0$ in M.

A *trivial* linear dependence is, colloquially, something like

$$\begin{aligned} &(10v_1 - 3v_2) \\ +2\cdot&(-3v_1 + v_2) \\ +&(-4v_1 + v_2) \\ =&(10 - 6 - 4)v_1 + (-3 + 2 + 1)v_2 \\ =&0v_1 + 0v_2 = 0. \end{aligned}$$

Formally, a linear dependence is *trivial* if there exist module elements $v^1, \ldots, v^k \in M$ and ring elements $a_i^j \in R$ such that

$$a_i^1 v^1 + a_i^2 v^2 + \cdots + a_i^k v^k = m_i \qquad \text{for all } i$$

$$r_1 a_1^j + r_2 a_2^j + \cdots + r_n a_n^j = 0 \qquad \text{for all } j$$

Solution. To see that (A) $\implies$ (E), write $M \oplus N = F$ with F free. Then we can show that (E) is true for F. Let $e_1, \ldots, e_k$ be a basis for F, and consider some $m_1, \ldots, m_n \in M$, $r_1, \ldots, r_n \in R$ such that $r_1 m_1 + \cdots + r_n m_n = 0$ in F. Now, we can define $a_i^j \in R$ uniquely by:

$$m_i = a_i^1 e_1 + \cdots + a_i^k e_k$$

i.e. the a_i^j are the components of m_i with respect to the e_j. Now, we have:

$$0 = \sum_i r_i m_i = \left(\sum_i r_i a_i^1 \right) e_1 + \cdots + \sum_i \left(r_i a_i^k \right) e_k$$

By the definition of linear independence of the e_j, this means that for each j, we have:

$$r_1 a_1^j + \cdots + r_n a_n^j = 0$$

To see that (E) for F implies (E) for M, let $0 = r_1 m_1 + \cdots + r_n m_n$ be a linear dependence in M. By replacing m_i with $(m_i, 0)$, this becomes a linear dependence in F, which must be trivial. Let $v^1, \ldots, v^k \in F$ and $a_i^j \in R$ be as in the definition of a trivial linear dependence. We can write $v^i = v_M^i + v_N^i$ uniquely. We know that, for all i, the following equation holds:

$$(m_i, 0) = a_i^1 v^1 + a_i^2 v^2 + \cdots + a_i^k v^k = a_i^1 (v_M^1 + v_N^1) + \cdots + a_i^k (v_M^k + v_N^k)$$

Thus, comparing M and N parts, we get that

$$m_i = a_i^1 v_M^1 + \cdots + a_i^n v_M^1$$

In addition, the equation

$$r_1 a_1^j + \cdots + r_n a_n^j = 0$$

still holds (this is just an equation over R, so it has nothing to do with M or F). Thus, the relation is trivial in M.

We'll prove that (E) $\Longrightarrow$ (A) by a more general fact:

Claim 6. If M is finitely presented and N is any module which satisfies the condition (E), then any homomorphism φ from M to N can be factored as $M \to F \to N$ with F a free module.

This suffices to prove that (E) $\Longrightarrow$ (A), since we can take $M = N$ and $\varphi = \mathrm{id}_M$, so this says we have maps $\sigma : M \to F$ and $\pi \colon F \to M$ such that $\pi \circ \sigma = \mathrm{id}_M$. This requires π to be surjective and σ to be a splitting of the exact sequence $0 \to \ker \pi \to F \to M \to 0$, so $M \oplus \ker \pi \simeq F$, and M is projective.

Now, let's prove the claim. Choose a finite presentation $F_2 \to F_1 \to M \to 0$ with F_1, F_2 free and finitely generated. Let $m_1, \ldots, m_k$ be the images of a basis $e_1, \ldots, e_k$ of F_1, so in particular they generate M. Now, let $\rho_j = r_{1j}e_1 + \cdots + r_{kj}e_k$, $j = 1, \ldots, \ell$ be the images of a basis of F_2 in F_1. We'll prove the claim by induction on ℓ. If $\ell = 0$, there's nothing to prove since M is free. Now, we can assume we know the claim for any finitely presented module M' which has a presentation $F_2' \to F_1' \to M' \to 0$ with F_2 generated by at most $\ell - 1$ elements. Take $M' = F_1/(\rho_1, \ldots, \rho_{\ell-1})$, so $M = M'/\rho_\ell$.

Now, we get a map $\varphi' \colon M' \to N$ by composing φ with $M' \to M$. Since $F_1 \to M$ factors through M', we can see that M' is generated by the images of $e_1, \ldots, e_k$ as well. Now, there is a free module F_0 with a map $\alpha_0 \colon M' \to F_0$ and $\beta_0 \colon F_0 \to N$ such that $\beta_0 \circ \alpha_0 = \varphi'$. We want to use this to build a free module F and maps $\alpha \colon M \to F$, $\beta : F \to N$ such that $\beta \circ \alpha = \varphi$. Suppose we can build F such that we have a map $\alpha' \colon M' \to F$ and $\beta : F \to N$ such that $\beta \circ \alpha' = \varphi'$. Then, in order to get $\alpha : M \to F$ such that $\beta \circ \alpha = \varphi$, we just need to show that $\alpha'(\rho_\ell) = 0$ (since $M = M'/\rho_\ell$). In particular, if $\alpha_0(\rho_\ell) = 0$, we're done. So let's look at $\alpha_0(\rho_\ell)$ and try to kill it.

We can write $\alpha_0(\rho_\ell)$ as $\alpha_0(\rho_\ell) = r_1 f_1 + \cdots + r_q f_q$ for $f_1, \ldots, f_q$ a basis of F_0. Now, $\beta_0(\alpha_0(\rho_\ell)) = \varphi'(\rho_\ell) = 0$, since φ' factors through $\varphi \colon M \to N$ and $\rho_\ell = 0$ in M. Thus, $\beta_0(\alpha_0(\rho(\ell)) = 0$ in N, so we have the following linear relation in N, where we let $n_i = \beta_0(f_i)$:

$$0 = \beta_0(\alpha_0(\rho_\ell)) = r_1 n_1 + \cdots + r_q f_q$$

Since N satisfies the condition (E), it follows that there are $v^1, \ldots, v^p \in N$ and for each $i = 1, \ldots, q$, we have $a_i^1, \ldots, a_i^p \in R$ such that:

$$n_i = a_i^1 v^1 + \cdots + a_i^p v^p \tag{1}$$

and for all $1 \leq p' \leq p$:

$$r_1 a_1^{p'} + \cdots + r_q a_q^{p'} = 0 \tag{2}$$

Now, let F be the free module generated by the p elements $e^1, \ldots, e^p$, and let $\beta : F \to N$ be defined by sending $e^{p'}$ to $v^{p'}$ for $1 \leq p' \leq p$. We define a map $\tau \colon F_0 \to F$ by sending f_i to $a_i^1 e^1 + \cdots + a_i^p e^p$. Then, equation (1) says exactly that $\beta \circ \tau = \beta_0$. Thus, $\varphi' = \beta_0 \circ \alpha_0 = \beta \circ \tau \circ \alpha_0$. So, let $\alpha' = \tau \circ \alpha_0$. We now need to show that $\alpha'(\rho_\ell) = 0$, or in other words that $\tau(\alpha_0(\rho_\ell)) = 0$. But this is exactly what Equation (2) says: $\rho_\ell = r_1 f_1 + \cdots + r_q f_q$ maps to the element of F whose $e^{p'}$-component is:

$$r_1 a_1^{p'} + \cdots + r_q a_1^{p'} = 0$$

This concludes the proof of (E) $\Longrightarrow$ (A).

ALTERNATE PROOF: (E) $\implies$ (C)

Instead of this direct proof that (E) $\implies$ (A), we could also show that (E) $\implies$ (C).[5] It's not hard to see that if M satisfies condition (E), then M_P does as well, since a linear dependence in M_P becomes one in M after clearing denominators by multiplying by an element $s \notin P$. Then when we get the a_i^j and the v^j, these give elements in R_P, M_P respectively, and we can divide these by s to show that the original linear dependence in M_P was trivial.

Thus, what we need to prove is that if M is a finitely generated module over a local ring R with maximal ideal $\mathfrak{m}$ and M satisfies (E), then M is free. In order to do this, we'll actually show that if $m_1, \dots, m_n \in M$ are linearly independent in $M/\mathfrak{m}$, then the submodule of M generated by $m_1, \dots, m_n$ is free. Taking $m_1, \dots, m_n$ to be a minimal set of generators of M then suffices. (Since if the $m_1, \dots, m_n$ are linearly dependent mod $\mathfrak{m}$, some subset of them generates $M/\mathfrak{m}$ and therefore generates M by Nakayama's lemma).

We can see this by induction on n. Consider a single element $m \in M$. Then the kernel of the map $R \to M$ sending 1 to m is the ideal I of elements $r \in R$ such that $r \cdot m = 0$. But by Property (E), if $r \cdot m = 0$, then there are elements $v^1, \dots, v^k \in M$ and $a^1, \dots, a^k \in R$ such that $m = a^1 v^1 + \dots + a^k v^k$ and $ra^j = 0$ for all $j = 1, \dots, k$. But $m \notin \mathfrak{m}M$, since then $\{m\}$ would not be linearly independent mod $\mathfrak{m}$. Thus, for at least one j, $a^j \notin \mathfrak{m}$. Since R i local, this implies that a^j is a unit, so $ra^j = 0$ implies that $r = 0$.

Now, consider $m_1, \dots, m_n$ which are linearly independent mod n and assume that for any smaller set of elements of M which are linearly independent mod $\mathfrak{m}$, the submodule they generate is free. We want to show that $m_1, \dots, m_n$ are linearly independent over R. So assume that $r_1 m_1 + \dots + r_n m_n = 0$. Then we have $v^1, \dots, v^k \in M$ and $a_i^j \in R$ such that $\sum_i r_i a_i^j = 0$ and $m_i = \sum_j a_i^j v^j$. If for some i, $a_i^j \in \mathfrak{m}$ for all $j = 1, \dots, k$, then $m_i \in \mathfrak{m}M$, so it is 0 mod $\mathfrak{m}$ and thus cannot be part of a linearly independent set. So, for some j such that $a_i^j \notin \mathfrak{m}$ (and thus a_i^j is a unit), we can multiply the equation $\sum_i r_i a_i^j = 0$ by $(a_i^j)^{-1}$ to solve for r_i. Thus, each r_i is an R-linear combination of the others. In particular, we have some equation $r_1 = c_2 r_2 + \dots + c_n r_n$. This lets us rearrange the equation $r_1 m_1 + \dots + r_n m_n$ as:

$$r_2(m_2 + c_2 m_1) + r_3(m_3 + c_3 m_1) + \dots + r_n(m_n + c_n m_1) = 0$$

But since $m_2, \dots, m_n$ are linearly independent mod $\mathfrak{m}$, so are the $n-1$ elements $(m_2 + c_2 m_1), \dots, (m_n + c_n m_1)$. Therefore, these are linearly independent over R, which implies that $r_2, \dots, r_n = 0$. So now, the equation $r_1 m_1 + \dots + r_n m_n = 0$ becomes $r_1 m_1 = 0$, and we already saw that this cannot happen.

[5] and this proof will actually go through for M any finitely generated module, without need for finite presentation. It's also true, and not hard to show, that (C) $\implies$ (E) for any finitely generated module. So, since (C) is strictly weaker than (A) for very crazy rings, we can't hope to prove (A) from (E) without using the finite presentation hypothesis.

Remarks from Dan on Q10:

To what extent was finite presentation crucial in our arguments here? We saw in the proof that (A) $\implies$ (C) that a finitely generated projective module is finitely presented. It turns out that if M is *locally free* in the sense of (B) and finitely generated, it is automatically finitely presented and thus projective. The proof isn't hard: take a short exact sequence $0 \to K \to F \to M \to 0$. Since $M[\frac{1}{r_i}]$ is free and therefore finitely presented, $K[\frac{1}{r_i}]$ is finitely generated. Then since there are finitely many r_i, we can throw together generators of each $K[\frac{1}{r_i}]$ and multiply them by appropriate powers of r_i to get a set of N elements of K and a map from R^N to K. This map is surjective after inverting r_i for each i, so it is surjective. So finitely generated locally free is equivalent to finitely generated projective, and both of these imply that we're already finitely presented. This is also equivalent to being locally free with all ranks finite.

However, the fact that (D) $\implies$ (B) (or even the fact that (C) $\implies$ (B)) does crucially use the finite presentation hypothesis, and it's false in general otherwise: there are finitely generated modules M such that M_P is free for each prime ideal P but M is not locally free in the sense of (B). However, such modules only occur over very crazy rings: for example, this cannot occur over a domain. Equivalently by what we said above, M is not finitely presented. It turns out that a finitely generated module M such that $M_\mathfrak{m}$ is free of rank $r(\mathfrak{m})$ for each $\mathfrak{m}$ is finitely presented (and thus projective) iff $r(\mathfrak{m})$ is a (locally) constant function on the set of maximal ideals of R. (Locally here just means that we have some $(r_1, \ldots, r_k)$ generating the unit ideal such that this function is constant after inverting each r_i).

This isn't actually so hard to see: we can use Claim 4, (i) (which only uses finite generation, not finite presented-ness) to show that we can lift an isomorphism $F_P \xrightarrow{\sim} M_P$ from R_P to a homomorphism over $R[\frac{1}{r}]$ for some $r \notin P$, and to show that M is locally free, it suffices to show that we can find some $r' \notin P$ such that this lifts to an *isomorphism.* (i.e. because then for every P there is an $r' \notin P$ such that $M[\frac{1}{r'}]$ is free, and then as before we can find some finite collection of such r' which generate the unit ideal). This is an isomorphism iff it is an isomorphism after localizing at every maximal ideal $\mathfrak{m} \ni r$, by a small variant of the argument used for (B) $\implies$ (A) (apply the same argument to the kernel of a homomorphism that we applied to the cokernel). We can replace r with some $r' \notin P$ such that the rank of $M[\frac{1}{r'}]$ is constant because the rank is locally constant. Since $M_\mathfrak{m}$ is free of the same rank as M_P, $F_\mathfrak{m}$ and $M_\mathfrak{m}$ are free modules of the same rank, so we can apply Question 4 to show that $F_\mathfrak{m} \to M_\mathfrak{m}$ is an isomorphism iff it is surjective. But if M is finitely generated and $N \to M$ is a homomorphism such that $N_P \to M_P$ is surjective, then the same thing is true for $N[\frac{1}{r}] \to M[\frac{1}{r}]$.[6]

[6] To see that the locally constant rank condition is automatically satisfied over a domain - or actually a more general ring, as we'll see - If $P \subseteq Q$ are prime ideals with M_Q free, then M_P is a localization of M_Q, so M_P is free of the same rank. Thus if $M_\mathfrak{m}$ is free for all maximal ideals $\mathfrak{m}$, M_P is free for all prime ideals P, and the rank function is constant as soon as we know that it is the same for all minimal prime ideals. In particular, if R is a domain, (0) is the unique minimal prime ideal, so this always holds. If R has finitely many minimal prime ideals, it then suffices to show that if P_1, P_2 are two minimal primes, there is some maximal ideal $\mathfrak{m}$ containing both of them (since the rank and $\mathfrak{m}$ is equal to the rank at P_1 and at P_2). This isn't actually true in general, but if no maximal ideal $\mathfrak{m}$ contains both P_1 and P_2, then the ideal $P_1 + P_2$ must be the unit ideal, so $R/(P_1 \cap P_2) \simeq R/P_1 \times R/P_2$ by the Chinese Remainder Theorem. Let $e_1, e_2 \in R$ correspond to $(1, 0)$ and $(0, 1)$ respectively under this isomorphism. Then $e_1 + e_2 = 1$, and the image of P_i in $R[\frac{1}{e_i}]$ is the unit ideal. So $R[\frac{1}{e_i}]$ has one fewer minimal prime than R does, and we can proceed by induction to see that the rank function for $M[\frac{1}{e_i}]$ is locally constant, so the rank function for M is locally constant. I found this argument in question number 1450205 on Math Stack Exchange.