MATH 210A, FALL 2017
HW 1 SOLUTIONS
WRITTEN BY DAN DORE
(If you find any errors, please email ddore@stanford.edu)

Problem 1. Given an R-module M and a subset $S \subset M$, prove that the following are equivalent.

(A) *"Every element of M is an R-linear combination of elements of S"*:
For all $m \in M$ there exist $r_1, \dots, r_k \in R$ and $s_1, \dots, s_k \in S$ such that $m = \sum_{i=1}^k r_i s_i$.

(B) *"Homomorphisms are determined by their value on elements of S"*:
For any R-module N and any homomorphisms $f : M \to N$ and $M \to N$,

$$f|_S = g|_S \implies f = g.$$

(C) *"Any homomorphism whose image contains S is a surjection"*:
For any R-module L and any homomorphism $h : L \to M$,

$$h(L) \supseteq S \implies h(L) = M.$$

When these equivalent conditions hold, we say that S *generates* M (or S *spans* M, or M *is generated by* S, or M *is spanned by* S).

Solution. (A) $\implies$ (B): We have homomorphisms $f, g : M \to N$ such that $f(s) = g(s)$ for all $s \in S$, and we want to show that this implies $f = g$, i.e. $f(m) = g(m)$ for all $m \in M$. So let $m \in M$ be arbitrary. By property (A), there are $r_1, \dots, r_k \in R, s_1, \dots, s_k \in S$ such that $m = \sum_{i=1}^k r_i s_i$. By the fact that f and g are module homomorphisms, we have:

$$\begin{aligned} f(m) &= f(r_1 s_1 + \dots + r_k s_k) \\ &= f(r_1 s_1) + \dots + f(r_k s_k) \\ &= r_1 f(s_1) + \dots + r_k f(s_k) \\ &= r_1 g(s_1) + \dots + r_k g(s_k) \\ &= g(r_1 s_1) + \dots + g(r_k s_k) \\ &= g(r_1 s_1 + \dots + r_k s_k) \\ &= g(m) \end{aligned}$$

(B) $\implies$ (C): We'll prove the contrapositive, i.e. that if (C) is false, then (B) is false. So suppose that there is an R-module L and a homomorphism $h : L \to M$ such that $h(L) \supseteq S$, but $h(L) \neq M$. Then we can form the quotient module $N := M/h(L)$, with the quotient homomorphism $\pi : M \to N$. Note that our assumption that $h(L) \subsetneq M$ means that $N = M/h(L)$ is nonzero.

Since $S \subseteq h(L)$, $\pi|_S = 0$, so π and the 0 morphism $0 : M \to N$ agree on S. However, π is not the 0 morphism, because it is surjective and N is nonzero. In particular, for any $m \in M, m \notin h(L)$, $\pi(m) \neq 0$. Thus, (B) is false.

(C) $\implies$ (A): Define R^S to be the free R-module with generators labeled by the elements of S, so it consists of formal R-linear combinations $\sum_{i=1}^k r_i e_{s_i}$ with $s_i \in S$, and e_{s_i} basis elements. Define a homomorphism $h : R^S \to M$ by sending the basis element e_s to s (this is the "universal property of free modules": there is a unique homomorphism from a free R-module to another R-module which sends the basis vectors to specified elements). By construction, S is contained in the image (since $h(e_s) = s$). Therefore, Property (C) implies that h is a surjection. This means that for any $m \in M$, there is some $\alpha \in R^S$ such that $\pi(\alpha) = m$. But an element α of R^S can be written uniquely in the form $\alpha = \sum_{i=1}^k r_i e_{s_i}$ with $r_i \in R$. Then we have:

$$m = \pi(\alpha) = \pi\left(r_1 e_{s_1} + \cdots + r_k e_{s_k}\right) = r_1 \pi(e_{s_1}) + \cdots r_k \pi(e_{s_k}) = r_1 s_1 + \cdots + r_k s_k$$

Since m was an arbitrary element of M, this shows that Property (A) is true.

[TC: Another way to think about this proof of (C) $\implies$ (A) is that the image of $h\colon R^S \to M$ is exactly the set of linear combinations of elements of S, which (in light of this question) is the submodule of M spanned by S.]

Problem 2. Here is one way to modify the converse direction to obtain an equivalence. (For the solution to the question as written on HW1, just look at (A) $\implies$ (B).)

We say an R-module M is *finitely generated* if there exists a finite set $S \subset M$ that generates M. Prove that the following are equivalent:

(A) M is finitely generated.

(B) For any infinite chain $N_1 \subseteq N_2 \subseteq \cdots \subseteq M$ of submodules of M, indexed by an arbitrary well-ordered set I, whose union $\cup_{i \in I} N_i = M$ is equal to M, there exists a finite $k \in \mathbf{N}$ such that $N_k = M$.[1]

Solution. (A) $\implies$ (B): Let $S = \{m_1, \ldots, m_n\} \subset M$ be a finite generating set. Since $\cup_{i \in \mathbf{N}} N_i = M$, for each $i = 1, \ldots, n$ there is a $j(i)$ such that $m_i \, in N_{j(i)}$. Let j be the maximum of the finitely many $j(i)$. Since $N_{j(i)} \subseteq N_j$ for each i, we must have $m_1, \ldots, m_n \in N_j$. Now, the inclusion $\iota : N_j \hookrightarrow M$ is a homomorphism of R-modules, and by construction we see that $\iota(N_j)$ contains S. Since S generates M, we may apply Property (C) from Problem 1 to conclude that $\iota : N_j \hookrightarrow M$ is surjective. Since N_j is a submodule of M, this means that $N_j = M$.

(B) $\implies$ (A): We can list *all* of the elements of M as $M = \{m_i\}_{i \in I}$ for some well-ordered set I.[2] Then, we can define submodules $N_i = \mathrm{span}\{m_j \mid j \leq i\}$, i.e. the set of all sums $\sum_{\ell=1}^{k} r_\ell m_{j_\ell}$. Since every element of M is m_i for some $i \in I$, we certainly have that $\cup_{i \in I} N_i = M$. So we can apply Property (B) and conclude that for some finite $k \in \mathbf{N}$, $N_k = M$. This says that M is the span of $m_1, \ldots, m_k$, so M is finitely generated.

[1] Here, we view $\mathbf{N}$ as an "initial segment" of I, i.e. we identify the smallest element of I with 1, the second smallest with 2, etc. This makes sense because of the definition of a well-ordered set. If you'd rather avoid such set-theoretic fuss, feel free to pretend that $I = \mathbf{N}$.

[2] via the well-ordering theorem, a consequence of the axiom of choice! If M is countable, we can take $I = \mathbf{N}$ and just enumerate the elements.

Problem 3. Prove that $\mathbf{Z}$-modules and abelian groups are the same thing. Specifically, prove that

(a) Every abelian group A admits one and only one structure of a $\mathbf{Z}$-module (i.e. there is a unique "multiplication map" $\cdot : \mathbf{Z} \times A \to A$ making A into a $\mathbf{Z}$-module).

(b) For any abelian groups A and B, the set of $\mathbf{Z}$-module homomorphisms $f : A \to B$ is exactly the set of abelian group homomorphisms $f : A \to B$.

(c) Write one sentence summarizing what makes (a) and (b) happen.

Solution. The fanciest way I can think to say this is that $\mathbf{Z}$ is the initial object in the category of (not necessarily commutative, but with a unit element) rings, so for any abelian group A, there is a unique ring homomorphism $\mathbf{Z} \to \mathrm{End}(A)$, which is equivalent to a $\mathbf{Z}$-module structure on A. (I suppose slightly more effort is needed to see that (b) holds this way).

The less fancy way to say this is that the axioms of a module require that $1 \cdot a = a, 0 \cdot a = 0$ for all $a \in A$, that $(n+m) \cdot a = n \cdot a + m \cdot a$ for all $n, m \in \mathbf{Z}, a \in A$, and that $(-n) \cdot a = -(n \cdot a)$ for all $n \in \mathbf{Z}, a \in A$. Because every element of $\mathbf{Z}$ is either 0 or a finite sum of 1's and -1's, the axioms pin down exactly what $n \cdot a$ needs to be for any $n \in \mathbf{Z}$ (i.e. $n \cdot a = a + a + \cdots + a$ with a repeated n times for $n > 0$). This argument shows that A has at most one structure of a $\mathbf{Z}$-module, and also that since an abelian group homomorphism respects addition and subtraction, it must also respect the $\mathbf{Z}$-module structure. The only remaining thing to check is that this definition of a $\mathbf{Z}$-module structure is compatible with multiplication in $\mathbf{Z}$, i.e. that $(nm) \cdot a = n \cdot (m \cdot a)$. This boils down to the *definition* of multiplication of integers: for $n > 0$, nm is $m + \cdot + m$, with m repeated n times.

Problem 4. Let R be a ring, and let $\{M_i\}_{i \in I}$ be a family of R-modules indexed by some set I.

Define the *direct product* $\prod_{i \in I} M_i$ to be the Cartesian product, i.e. the set of families $(m_i)_{i \in I}$ with $m_i \in M_i$. This becomes an R-module with the component-wise addition and multiplication:

$$(m_i)_i + (n_i)_i = (m_i + n_i)_i \qquad r \cdot (m_i)_i = (r \cdot m_i)_i$$

Define the *direct sum* $\oplus_{i \in I} M_i$ to be the submodule consisting of elements where $m_i = 0$ for all but finitely many i. (You do not have to prove this is a submodule, but you should understand why it is.) Note that when I is finite $\oplus_{i \in I} M_i$ is the same as $\prod_{i \in I} M_i$, but in general it is a proper submodule.

For readability, let $P = \prod_{i \in I} M_i$ and $S = \oplus_{i \in I} M_i$.

(a) Show that

$$\text{“a map to } P = \prod_{i \in I} M_i \text{ is the same as a family of maps to } M_i\text{”},$$

by proving the following. Let $\pi_i : P \to M_i$ be the projection taking $(m_i)_{i \in I} \mapsto m_i$. Prove that for any R-module L, given homomorphisms $f_i : L \to M_i$ there exists a unique homomorphism $f : L \to P$ such that $f_i = \pi_i \circ f$ for all i.

(b) Show that

$$\text{“a map \textit{from} } S = \oplus_{i \in I} M_i \text{ is the same as a family of maps \textit{from} } M_i\text{”},$$

by formulating and proving a separate universal property along similar lines to (a).

Solution. (a) Let L be an R-module and $f_i : L \to M_i$ homomorphisms. We define f be $f : \ell \mapsto (f_i(\ell))_i$. Since $\pi_i((m_i)_i) = m_i$, we have $(\pi_i \circ f)(\ell) = f_i(\ell)$, so $\pi_i \circ f = f_i$. Now, we need to check that f is an R-module homomorphism. So let $\ell_1, \ell_2 \in L$. Then we have:

$$f(\ell_1 + \ell_2) = (f_i(\ell_1 + \ell_2))_i = (f_i(\ell_1) + f_i(\ell_2))_i = (f_i(\ell_1))_i + (f_i(\ell_2))_i$$

Here, we used the definition of addition in $P = \prod_{i \in I} M_i$ as well as the fact that the f_i are homomorphisms. Compatibility with scalar multiplication is similar. Let $\ell \in L, r \in R$. Then we have:

$$f(r\ell) = (f_i(r \cdot \ell))_i = (r \cdot f_i(\ell))_i = r \cdot (f_i(\ell))_i$$

Again, we use the fact that the f_i are R-module homomorphisms and the definition of scalar multiplication in P.

Finally, we see that f is unique because the condition that $\pi_i \circ f(\ell) = f_i(\ell)$ for all $\ell \in L, i \in I$ implies that the i-th coordinate of $f(\ell)$ is $f_i(\ell)$. Since an element of $P = \prod_i M_i$ is determined by its coordinates, we see that this condition uniquely specifies what $f(\ell)$ must be.

(b) Mimicking the universal property for direct product, we formulate the universal property for direct sum as follows, via the canonical inclusions $j_i : M_i \to S$ which send $m \in M_i$ to the element with i-coordinate m and all other coordinates 0: for any R-module L and any family of R-module homomorphisms $f_i : M_i \to L$, there is a unique R-module homomorphism $f : S \to L$ such that $f \circ j_i = f_i$.

Let $s \in S$ be arbitrary. By the definition of S, we know that all but finitely many of the coordinates of s are 0. Let $i_1, \ldots, i_k$ be the non-zero coordinates. Then, we have:

$$s = j_{i_1}(s_{i_1}) + \cdots + j_{i_k}(s_{i_k})$$

The notation may make this statement seem harder than it is, so let's look at a quick example with $I = \{1, 2, 3\}$. Then $S = M_1 \times M_2 \times M_3 = M_1 \oplus M_2 \oplus M_3$ is the set of triples $s = (m_1, m_2, m_3)$ with $m_i \in M_i$. Given such a triple, we have:

$$s = (m_1, m_2, m_3) = (m_1, 0, 0) + (0, m_2, 0) + (0, 0, m_3) = j_1(m_1) + j_2(m_2) + j_3(m_3)$$

The point of the requirement that all but finitely many coordinates are 0 is that it ensures that even when I is infinite, such a decomposition always works. We could extend our previous example so that $I = \mathbf{N}$, but our particular s satisfies $s_i = 0$ for $i > 3$, so

$$\begin{aligned} s &= (m_1, m_2, m_3, 0, 0, 0, \ldots) \\ &= (m_1, 0, 0, 0, \ldots) + (0, m_2, 0, 0, \ldots) + (0, 0, m_3, 0, \ldots) \\ &= j_1(m_1) + j_2(m_2) + j_3(m_3) \end{aligned}$$

Now, we can define f by

$$f\left(j_{i_1}(s_{i_1}) + \cdots + j_{i_k}(s_{i_k})\right) = f_{i_1}(s_{i_1}) + \cdots + f_{i_k}(s_{i_k})$$

This is well-defined since the sum is finite and any particular s can be written *uniquely* as a sum of (appropriate j_i's of) its non-zero coordinates. Another way to write this, which makes it a bit more obvious that the definition does not depend on any arbitrary choices, is:

$$f\left((m_i)_i\right) = \sum_{i \in I} f_i(m_i)$$

since $(m_i)_i \in S$, the sum is guaranteed to have only finitely many non-zero terms.

Now, let's verify that f is an R-module homomorphism, remembering that the operations on S are defined in terms of the operations on P:

$$\begin{aligned} f\left((m_i)_i + (n_i)_i\right) &= f\left((m_i + n_i)_i\right) \\ &= \sum_{i \in I} f_i(m_i + n_i) \\ &= \sum_{i \in I} f_i(m_i) + f_i(n_i) \\ &= \left(\sum_{i \in I} f_i(m_i)\right) + \left(\sum_{i \in I} f_i(n_i)\right) \\ &= f\left((m_i)_i\right) + f\left((n_i)_i\right) \end{aligned}$$

$$\begin{aligned} f\left(r \cdot (m_i)_i\right) &= f\left((r \cdot m_i)_i\right) \\ &= \sum_{i \in I} f_i(r \cdot m_i) \\ &= \sum_{i \in I} r \cdot f_i(m_i) \\ &= r \cdot \left(\sum_{i \in I} f_i(m_i) \right) \\ &= r \cdot f((m_i)_i) \end{aligned}$$

Since all of the sums are finite, we can manipulate them without worry!

Finally, f is uniquely determined by the condition that $f \circ j_i = f_i$: this means that $f(j_i(m_i)) = f_i(m_i)$, and since f is required to be a module homomorphism,

$$f\left(\sum_{\ell=1}^{k} j_{i_\ell}(m_{i_\ell}) \right) = \sum_{\ell=1}^{k} f\left(j_{i_\ell}(m_{i_\ell})\right) = \sum_{\ell=1}^{k} f_{i_\ell}(m_{i_\ell}) = \sum_{i \in I} f_i(m_i)$$

(the last equality holds because the only non-zero coordinates of $\sum_{\ell=1}^{k} j_{i_\ell}(m_{i_\ell})$ are the i_ℓ). Since any element of S can be written in such a form, we see that the only possible definition of f is the one that we gave.