

Algorithms HW

1

■

2

■

3. In this problem, we will make good on our promise from class to show that the rank of a free module is well-defined (over a commutative ring!). Let R be a non-zero commutative ring. We are going to show that the R -modules R^n and R^m are non-isomorphic if $n \neq m$.

- Suppose that $I \trianglelefteq R$ is an ideal of a commutative ring R and let M be an R -module. Let IM be the R -submodule of M spanned by all elements ax for $a \in I$ and $x \in M$. Show that the quotient M/IM has the structure of an R/I -module. When $M = R^n$, show that M/IM is isomorphic to $(R/I)^n$ as an R/I -module.
- Show that any R -linear isomorphism $R^n \xrightarrow{\sim} R^m$ induces an R/I -linear isomorphism $(R/I)^n \xrightarrow{\sim} (R/I)^m$.
- By taking I to be a maximal ideal, deduce that R^n and R^m are isomorphic if and only if $n = m$. (Standard linear algebra results may be used without proof.)

- To show that M/IM has the structure of an R/I -module, we must show that M/IM has an underlying abelian group structure with respect to addition, and that there is a well-defined R/I scalar multiplication on M/IM .

First, we show that M/IM has a well-defined abelian group structure with respect to addition. By definition M has an abelian group structure, and so IM is a normal subgroup of M . It follows that the quotient group M/IM is well-defined and moreover is also abelian. One way to see that the quotient group is abelian is to recall that the quotient map $\pi : M \rightarrow M/IM$ is a group homomorphism and so

$$\pi(x) + \pi(y) = \pi(x + y) = \pi(y + x) = \pi(y) + \pi(x),$$

for all $x, y \in M$.

Next, we propose an R/I scalar multiplication on M/IM . If $r + I \in R/I$ and $m + IM \in M/IM$. Then I claim that scalar multiplication given by $(r + I) \cdot (m + IM) := rm + IM$ is well defined. Let $r + I = r' + I$ be equivalent elements of R/I . Then we have that there's some $a \in I$ such that $r = r' + a$. Now let $m + IM \in M/IM$ and consider

$$rm + IM = (r' + a)m + IM = r'm + IM + am + IM = r'm + IM + 0 + IM = r'm + IM,$$

since $am \in IM$ by definition. That is, our proposed scalar multiplication maps $m \in M$ to the same class mod IM , regardless of choice of representative of $r + IM$. Hence our multiplication is well defined and we have found an R/I -module structure on M/IM .

- Suppose $\phi : R^n \rightarrow R^m$ is an R -linear isomorphism. Since R^n is a free R -module, it follows that ϕ is defined exactly by its action on the basis $\{e_i\}$ where $e_i = (0, \dots, 1, \dots, 0)$ with the 1 in the i th position.

Now notice that $\bar{e}_i := \pi(e_i)$ is an R/I -basis for $(R/I)^n$. And so maps out of $(R/I)^n$ can be defined by their action on \bar{e}_i . We define a map $\bar{\phi} : (R/I)^n \rightarrow (R/I)^m$ by $\bar{\phi}(\bar{e}_i) = (\pi \circ \phi)(e_i)$. This map is R/I linear by construction, we claim that it is also a bijection.

Suppose $(\bar{b}_1, \bar{b}_2, \dots, \bar{b}_m) \in (R/I)^m$. Since $\pi : R \rightarrow R/I$ is a surjection, there is an element $(b_1, b_2, \dots, b_m) \in R^m$ such that $\pi(b_1, b_2, \dots, b_m) = (\bar{b}_1, \bar{b}_2, \dots, \bar{b}_m)$. Moreover, ϕ is an isomorphism and so there also exists an element $(a_1, a_2, \dots, a_n) \in R^n$ such that $\phi(a_1, \dots, a_n) = (b_1, \dots, b_m)$. It then follows that $\bar{\phi}(\bar{a}_1, \bar{a}_2, \dots, \bar{a}_n) = (\bar{b}_1, \bar{b}_2, \dots, \bar{b}_m)$. Thus, $\bar{\phi}$ is surjective.

Now consider $0 \in (R/I)^m$. Tuples of the form $(b_1, \dots, b_m) \in R^m$ with $b_i \in I$ map to 0 under π . Since ϕ is an isomorphism from R^n to R^m , only elements $(a_1, \dots, a_n) \in R^n$ with $a_i \in I$ satisfy $\phi(a_1, \dots, a_n) = (b_1, \dots, b_m)$ with $b_i \in I$. Then, only elements of the form $(\bar{a}_1, \bar{a}_2, \dots, \bar{a}_n) \in (R/I)^n$ map to $0 \in (R/I)^m$ under $\bar{\phi}$. However, since $a_i \in I$ we have $(\bar{a}_1, \dots, \bar{a}_n) = 0 \in (R/I)^n$. And so $\bar{\phi}$ is injective.

We have found a bijective R/I -linear map $\bar{\phi} : (R/I)^n \rightarrow (R/I)^m$ and so we have found an induced R/I -linear isomorphism $(R/I)^n \rightarrow (R/I)^m$.

- Suppose $n = m$, then $R^n = R^m$ and so $R^n \cong R^m$ as R -modules.

Now suppose that $R^n \cong R^m$. Since R is a non-zero commutative ring we have (the axiom of choice (or perhaps Zorn's lemma)) gives that there exists a maximal ideal $I \trianglelefteq R$. Now by part (b) we have an induced isomorphism on the R/I modules $(R/I)^n \cong (R/I)^m$. However, since I is maximal, it follows that R/I is a field and

so $(R/I)^n$ and $(R/I)^m$ are in fact R/I -vector spaces. Vector spaces are characterized by their dimension and so it follows that $(R/I)^n \cong (R/I)^m$ as R/I vector spaces implies $n = m$.

Hence the rank of a free module over a non-zero commutative ring is a well defined notion.

■

4. Prove the following identities for tensor products (where M, N, L are arbitrary R -modules):

- $M \otimes_R N \cong N \otimes_R M$ (“commutativity”)
- $R \otimes_R M \cong M$ (“identity”)
- $M \otimes_R (N \oplus L) \cong (M \otimes_R N) \oplus (M \otimes_R L)$ (“distributivity”)
- (harder) $M \otimes_R (N \otimes_R L) \cong (M \otimes_R N) \otimes_R L$ (“associativity”)

[Hint: the universal property of tensor products is a handy way of defining R -linear maps out of tensor products]

- Consider the map $M \times N \rightarrow N \otimes_R M$ given by $((m, n) \mapsto n \otimes m)$. Notice that this map is R -bilinear on $M \times N$ since $\otimes : M \times N \rightarrow M \otimes_R N$ is. Then by the universal property of tensor products we have a unique R -linear map $f : M \otimes_R N \rightarrow N \otimes_R M$ such that $f \circ \otimes = ((m, n) \mapsto n \otimes m)$. The same argument on the R -bilinear map $N \times M \rightarrow N \otimes_R M$ given by $((n, m) \mapsto (m \otimes n))$ gives a unique R -linear map $\tilde{f} : N \otimes_R M \rightarrow M \otimes_R N$ such that¹ $\tilde{f} \circ \times = ((n, m) \mapsto m \otimes n)$.

Notice now that $f \circ \tilde{f} = id_{N \otimes_R M}$ and $\tilde{f} \circ f = id_{M \otimes_R N}$. Indeed $(f \circ \tilde{f})(m \otimes n) = f(n \otimes m) = m \otimes n$. And likewise for the other direction.

That is, we have found a bijective R -linear map $M \otimes_R N \rightarrow N \otimes_R M$ and so in fact $M \otimes_R N$ is isomorphic to $N \otimes_R M$.

- Consider the following map $M \times N \rightarrow M$ via $((r, m) \mapsto rm)$ given by the module structure on M . Notice that this map is bilinear **come back and write the computation out** And so by the universal property of tensor products we have a unique R -linear map $f : R \otimes_R M \rightarrow M$ such that $r \otimes n \mapsto rm$.

I claim that this map is bijective and so is an isomorphism of R -modules. First notice that f is surjective. Indeed, if $m \in M$ then $f(1 \otimes m) = 1 \cdot m = m$, so long as R is not the zero ring. If R is the zero ring, then M must be the zero module, and then our desired isomorphism trivially holds.

Next we show that f is injective. Suppose we have $r \cdot m' = m$ for some $m, m' \in M$

¹The “ \otimes ” in the following phrase now refers to the R -bilinear map $N \times M \rightarrow N \otimes_R M$, whereas earlier it referred to the R -bilinear map $M \times N \rightarrow M \otimes_R N$.

and $r \in R$. Then notice

$$r \otimes m' = 1 \cdot r \otimes m' = r \otimes r \cdot m' = 1 \otimes m,$$

And so $rm' = m$ implies $r \otimes m' = 1 \otimes m$. This suffices to show that f is injective because if generally we have $r_1m_1 = r_2m_2$ then by definition $r_1m_1 = m'$ for some $m' \in M$ and then we have $m' = r_2m_2$.

Overall we have a bijective R -linear map $R \otimes_R M \rightarrow M$, and so $R \otimes_R M \cong M$.

- First we acquire an R -linear map $M \otimes_R (N \oplus L) \rightarrow (M \otimes_R N) \oplus (M \otimes_R L)$ by leveraging the universal property of tensor products. And then we show that this map is in fact an isomorphism.

First define a map $h : M \times (N \oplus L) \rightarrow (M \otimes_R N) \oplus (M \otimes_R L)$ by $h(m, (n, l)) = (m \otimes n, m \otimes l)$. Note that in R -Mod finite coproducts are also products, and so the domain of the function h is the R -module $M \oplus N \oplus L$. We claim that this map is R -bilinear. Consider

$$\begin{aligned} h(r_1m_1 + r_2m_2, (n, l)) &= ((r_1m_1 + r_2m_2) \otimes n, (r_1m_1 + r_2m_2) \otimes l) \\ &= (r_1(m_1 \otimes n) + r_2(m_1 \otimes n), r_1(m \otimes l) + r_2(m_2 \otimes n)) \\ &= r_1(m_1 \otimes n, m_1 \otimes l_1) + r_2(m_2 \otimes n, m_2 \otimes l). \end{aligned}$$

By the definition of the tensor product relations, and of the R -module structure on the direct sum of two R -modules. In other words, we have shown that h is R -linear in the first argument. Now consider the second argument

$$\begin{aligned} h(m, r_1(n_1, l_1) + r_2(n_2, l_2)) &= (m \otimes r_1n_1 + r_2n_2, m \otimes r_1l_1 + r_2l_2) \\ &= (r_1(m \otimes n_1) + r_2(m \otimes n_2), r_1(m \otimes l_1) + r_2(m \otimes l_2)) \\ &= r_1(m \otimes n_1, m \otimes l_1) + r_2(m \otimes n_2, m \otimes l_2), \end{aligned}$$

using the bilinearity of the tensor product, and by using the definition of the R -module structure on the direct sum of R -modules. That is, we've shown h is R -linear in the second argument also. And so h is an R -bilinear map.

We are now free to use the universal property of tensor products to acquire a new R -linear map $f : M \otimes_R (N \oplus L) \rightarrow (M \otimes_R N) \oplus (M \otimes_R L)$. where $f(m \otimes (n, l)) = (m \otimes n, m \otimes l)$. If we can verify that this map is bijective then we are done.

First we show f is surjective. Let $(m \otimes n, m \otimes l) \in (M \otimes_R N) \oplus (M \otimes_R L)$ then we have $m \otimes (n, l) \in M \otimes_R (N \oplus L)$ maps to the desired element.

Now suppose $f(m \otimes (n, l)) = 0$ that is $m \otimes n = 0$ and $m \otimes l = 0$. We want to show that $m \otimes (n, l) = 0$. [come back to this. There might be another way to do this using the universal property of tensor products](#)

■

4

■

6. Suppose that $f: M \rightarrow M'$ and $g: N \rightarrow N'$ are homomorphisms of R -modules. Use f and g to define a homomorphism

$$M \otimes_R N \rightarrow M' \otimes_R N'.$$

(This homomorphism is usually denoted by $f \otimes g$.)

We define the desired map by using the universal property of tensor products. Consider the following composition

$$M \oplus N \xrightarrow{(f,g)} M' \oplus N' \xrightarrow{\otimes} M' \otimes_R N',$$

via

$$(m, n) \mapsto (f(m), g(n)) \mapsto f(m) \otimes g(n).$$

We claim that this composition $\phi: M \oplus N \rightarrow M' \otimes_R N'$ is R -bilinear. Indeed, first let $n \in N$ be fixed and then consider

$$\begin{aligned} \phi(r_1 m_1 + r_2 m_2, n) &= (r_1 f(m_1) + r_2 f(m_2)) \otimes g(n) \\ &= (r_1 f(m_1)) \otimes g(n) + (r_2 f(m_2)) \otimes g(n) \\ &= r_1 (f(m_1) \otimes g(n)) + r_2 (f(m_2) \otimes g(n)) \\ &= r_1 \phi(m_1, n) + r_2 \phi(m_2, n), \end{aligned}$$

by the relations on the elements of the tensor product. In other words, we have shown that $\phi(-, n)$ is R -linear for each $n \in N$. A very similar calculation will show that $\phi(m, -)$ is R -linear for each $m \in M$. That is, ϕ is R -bilinear.

By the universal property of the tensor product we then have an R -linear map $\psi: M \otimes_R N \rightarrow M' \otimes_R N'$ given by $m \otimes n \mapsto f(m) \otimes g(n)$, as desired.

■

4

■