Math 542 HW2

Hongtao Zhang

1 Chinese Remainder

1.1 10.3.16

For any left ideal I of R define

$$IM = \left\{ \sum_{\text{finite}} a_i m_i \mid a_i \in I, m_i \in M \right\}$$

to be the collection of all finite sums of elements of the form am where $a \in I$ and $m \in M$. This is a submodule of M.

For any ideal I of R let IM be the submodule defined above. Let $A_1, ..., A_k$ be any ideals in the ring R. Prove that the map

$$\varphi : M \to \frac{M}{A_1 M} \times ... \times \frac{M}{A_k M} \text{ defined by } m \mapsto (m + A_1 M, ..., m + A_k M)$$

is an R-module homomorphism with kernel $A_1 M \cap A_2 M \cap ... \cap A_k M$.

Proof: Want to check $\forall x, y \in M : \varphi(x + y) = \varphi(x) + \varphi(y)$ and
$\forall x \in M, r \in R : \varphi(rx) = r\varphi(x)$.
$$\begin{aligned}\forall x, y \in M : \varphi(x + y) &= (x + y + A_1 M, ..., x + y + A_k M) \\ &= (x + A_1 M, ..., x + A_k M) + (y + A_1 M, ..., y + A_k M) \\ &= \varphi(x) + \varphi(y)\end{aligned}$$

$\forall r \in R, x \in M : \varphi(rx) = (rxA_1 M, ..., rxA_k M) = r(xA_1 M, ..., xA_k M)$ because submodule is invariant under the ring R.

To become the kernel, it need to satisfy that $\forall i \in [1, k] : x + A_i M = A_i M$, which implies that $x \in \bigcap_i A_i M$.

□

1.2 10.3.17

In the notation of the Section 1.1, assume further that the ideals $A_1, ..., A_k$ are pairwise comaximal $(i.e. \forall i \neq j : A_i + A_j = R)$. Prove that

$$\frac{M}{(A_1 ... A_k) M} \cong \frac{M}{A_1 M} \times ... \times \frac{M}{A_k M}$$

[See proof of the Chinese Remainder Theorem for rings in Section 7.6.]

Proof: Based on the proof of Chinese Remainder Theorem for rings in Section 7.6, it suffices to check the case when $k = 2$.

Consider a map $\varphi : M \to \frac{M}{AM} \times \frac{M}{BM}$ by sending $x \mapsto (a + AM, a + BM)$.

φ is a module homomorphism based on Section 1.1.

The kernel is clearly $(AM \cap BM)$, and similar to the proof in Ring, it suffices to check when A, B are comaximal, $(AB)M = (A \cap B)M$

Because $A + B = R$, $\exists x \in A, y \in B : x + y = 1$

$$\forall (r_1 \bmod A, r_2 \bmod B) \in \frac{M}{AM} \times \frac{M}{BM}$$

$$\begin{aligned} \varphi(r_2 x + r_1 y) &= \varphi(r_2)\varphi(x) + \varphi(r_1) y \\ &= (r_2 \bmod A, r_2 \bmod B)(0, 1) + (r_1 \bmod A, r_1 \bmod B)(1, 0) \\ &= (0, r_2 \bmod B) + (r_1 \bmod A, 0) \\ &= (r_1 \bmod A, r_2 \bmod B) \end{aligned}$$

Therefore φ is surjective.

It's clear that $(AB)M \subset (A \cap B)M$

Because $A + B = R$, $\exists x \in A, y \in B : x + y = 1$

Thus $\forall c \in (A \cap B)M : \exists x' \in A, y' \in B : c = cx + cy \in (AB)M$

□

2 Fractions

Suppose that R is an integral domain and let M be an R-module. Let S be a multiplicatively closed subset of R that includes 1 and does not include 0 (for instance complemenets of prime ideals). Let $S^{-1}M$ be the collection of symbols of the form $\frac{m}{s}$ where $m \in M$ and $s \in S$ and where we insist that $\frac{s' \cdot m}{s' s} = \frac{m}{s}$ for any $s' \in S$. This is an abelian group where we define addition by $\frac{m_1}{s_1} + \frac{m_2}{s_2} := \frac{s_2 \cdot m_1 + s_1 \cdot m_2}{s_1 s_2}$ for $m_1, m_2 \in M$ and $s_1, s_2 \in S$. Note that $S^{-1}R$ is a ring if we additionally define multiplication by $\frac{r_1}{s_1} \cdot \frac{r_2}{s_2} := \frac{r_1 r_2}{s_1 s_2}$ for $r_1, r_2 \in R$ and $s_1, s_2 \in S$. Finally, we note that $S^{-1}M$ is an $S^{-1}R$-module where $\frac{r}{s_1} \cdot \frac{m}{s_2} := \frac{r \cdot m}{s_1 s_2}$.

2.1

Show that if $f : M_1 \to M_2$ is a homomorphism of R-modules, then the map $S^{-1}f : S^{-1}M_1 \to S^{-1}M_2$ sending $\frac{m}{s} \mapsto \frac{f(m)}{s}$ is a homomorphism of $S^{-1}R$ modules.

Proof: Given that f is a homomorphism of R-module, this question is automatically right when checking addition and multiplication.

$$\forall \frac{m}{s} \in S^{-1}M_1, r \in R : S^{-1}f\left(r\frac{m}{s}\right) = \frac{f(rm)}{s} = \frac{rf(m)}{s}$$

addition is similar and omitted.

□

2.2

If $S = R - \{0\}$, then note that $S^{-1}R$ is a field. Use this to show that R^n and R^m are not isomorphic if n and m are distinct positive integers.

Proof: Note $S^{-1}R^n$ and $S^{-1}R^m$ are $S^{-1}R$ module, and because $S^{-1}R$ is a field, this is a vector space, and thus the dimension will match.

Thus it suffices to see that $S^{-1}R^m \cong S^{-1}R^n$ if and only if $R^m \cong R^m$, which is clear.

□

2.3

Let $S = R - \{0\}$ and consider the map $M \to (S^{-1}R) \otimes M$ that sends m to $1 \otimes m$. Show that its kernel is the torsion submodule of M.

Proof: Consider a map φ from $S^{-1}R \oplus M$ to $S^{-1}R$ by sending $\left(\frac{r}{s}, m\right) \mapsto \frac{rm}{s}$. Given the universal property of $\otimes$, there must exists a unique f that maps from $S^{-1}R \otimes M$ to $S^{-1}R$ which factor through φ.

□

3 Tensor

3.1 10.4.2

Show that the element "$2 \otimes 1$" is $0 \in \mathbb{Z} \otimes_{\mathbb{Z}} \frac{\mathbb{Z}}{2\mathbb{Z}}$ but is nonzero in $2\mathbb{Z} \otimes_{\mathbb{Z}} \frac{\mathbb{Z}}{2\mathbb{Z}}$.

Proof: We have $2 \otimes 1 = 2 \times (2 \otimes 1) = 1 \otimes 2 = 1 \otimes 0 = 0$ in $\mathbb{Z} \otimes_{\mathbb{Z}} \frac{\mathbb{Z}}{2}\mathbb{Z}$.

However, in $2\mathbb{Z}$, we cannot pull out the 2 out of 2 because $1 \notin 2\mathbb{Z}$.

□

3.2 10.4.20

Let $I = (2, x)$ be the ideal generated by 2 and x in the ring $R = \mathbb{Z}[x]$. Show that the element $2 \otimes 2 + x \otimes x$ in $I \otimes_R I$ is not a simple tensor, i.e. cannot be written as $a \otimes b$ for some $a, b \in I$.

Proof: From the old school we have $(a+b)(a-b) = a^2 - b^2$, and since $\otimes$ also satisfy distributive rule we shall have $a = 2, b = ix$. However, we don't have $i \in \mathbb{Z}[x]$, and thus this is impossible.

□

4 Duality

Suppose that R is commutative. Let M, N, and U be R-modules. The *dual module* of M is defined to be $M^* := \mathrm{Hom}_R(M, R)$.

4.1

Suppose that $(e_1, ..., e_n)$ is a bisis, i.e. linearly independent spanning set for M. Define $e_i^* \in M^*$ to be the homomorphism that sends e_i to 1 and all other $e_j (j \neq i)$ to 0. Show that $(e_1^*, ..., e_n^*)$ is a basis for M^*.

Proof: A homomorphism can be uniquely determined by sending the basis of M to R.

Because $\forall x \in M : x = \sum a_i e_i$, then by defining the map from $M \to M^*$ by sending $\sum a_i e_i \mapsto \sum a_i e_i^*$ is a surjective. Therefore $(e_1^*, ..., e_n^*)$ is a basis for M^*.

□

4.2

Show that if M is a free R-module of rank n, where n is a positive integer, then $(M^*)^*$ is isomorphic to M. (Hint: Consider the map $M \longrightarrow (M^*)^*$ that sends $m \in M$ to ev_m where $\mathrm{ev}_m : M^* \to R$ sends a homomorphism $\varphi : M \to R$ to $\varphi(m)$. To establish that this map is a surjection show that, in the notation of the preceding part, $((e_i)^*)^* = \mathrm{ev}_{e_i}$.)

Proof: Consider the map $\psi : M \to (M^*)^*$ by sending $m \mapsto ev_m$ where $ev_m : M^* \to R$ by sending $(\varphi : M \to R) \mapsto \varphi(m)$ as an evaluation map.

Then ev_{e_i} will send $e_i^* \mapsto e_i^*(e_i) = e_i$ and every other $e_j^* : j \neq i$ will send e_i to 0, which is exactly e_i^{**}.

The only thing left checking is that ψ is a homomorphism, which is automatically true given that this is an evaluation map from a homomorphism $\varphi : M \to R$.

□

4.3

Show that if R is a field and M and N are finitely generated, then $\mathrm{Hom}_R(M, N) \cong M^* \otimes N$ as R-modules. Show that this is not necessarily such an isomorphism when $R = \mathbb{Z}$ and M and N are finitely generated $\mathbb{Z}$-modules.

Proof: Suppose (e_i) are a finite set of elements that finitely generate M. Then by the same construction of part (4.1), we will have (e_i^*) that finitely generate M^*.

If R is a field, then M, N are vector spaces, and thus free.

We have $\mathrm{Hom}_R(M, N)$ equivalent to a matrix that has dimension $m \times n$, where m, n are the number of basis of M, N.

On the other hand, we have any bilinear map from $M \oplus N$ can be written as $m^T A n$, where the A has dimension $m \times n$. Thus this is an isomorphism of set.

Since in the expression we have m^T, and thus this is a map from $M \to R$, and thus we need the left hand side to be M^* of the tensor.

This is not necessary true under $\mathbb{Z}$ module because we can have different basis representation of the same element in $\mathbb{Z}$ module. Thus the dimension of the matrix may vary given different finitely generated set, and thus the tensor may be larger than the homomorphism.

□

5 Counterexample

Do one of the following two problems: 10.3.24 or 10.3.26.

5.1 10.3.24

For each positive integer i let M_i be the free $\mathbb{Z}$-module $\mathbb{Z}$, and let M be the direct product $\prod_{i \in Z^+} M_i$. Each elements of M is in the uniquely determined form $(a_1, a_2, a_3, \ldots)$ with $a_i \in \mathbb{Z}$ for all i. Let N be the submodule of M consisting of all such tuple with only finitely many nonzero a_i. Assume M is a free $\mathbb{Z}$-module with basis $\mathcal{B}$.

5.1.1

Show that N is countable.

Proof: It suffices to prove that the diagnoal argument that proves $\mathbb{R}$ is uncountable does not work here.

Because all elements in N contains only finitely many nonzero entries, the new element we retrieve from the diagonal plus 1 can only contain finitely many nonzero entries. However, this is not possible unless we have 9 on the diagonal after some finitely many terms.

However, that contradicts to how we enumerate the elements in N. Thus the diagnol plus 1 is not in N.

□

5.1.2

Show that there is some countable subset $\mathcal{B}_1$ of $\mathcal{B}$ such that N is contained in the submodule, N_1, generated by $\mathcal{B}_1$. Show also that N_1 is countable.

Proof: Because $\mathcal{B}$ is a basis,

$$\forall n \in N : \exists c_i \in \mathbb{Z} : \sum_{b_i \in \mathcal{B}} c_i b_i = n$$

such that the number of b_i used to represent n is finite.

Thus we takes the union of such b_i that's required to cover N, we will have a countable union of finite subsets which is still countable.

□

5.1.3

Proof: By definition of quotient, $\overline{M}$ can be generated by $\mathcal{B} \setminus \mathcal{B}_1$, and thus is a free module.

As a free module, every element in $\overline{M}$ can be represented by a finite sum of elements in $\mathcal{B} \setminus \mathcal{B}_1$, and thus is a multiple of other elements if and only if k divides all the coefficients of the basis.

□

5.1.4

Proof: The diagonal arguments works here by flipping the sign of each diagonal element.

Since $\mathcal{S}$ is uncountable, it is not possible that $\mathcal{S} \subset N_1$.

□

5.1.5

Proof: Given that $\overline{s} \in \frac{M}{N_1}$, and $N \in N_1$, we can add linear combination of any element that have finitely many nonzero entries.

Consider an integer k, it suffices to use N to fill the gap for any entries in $\overline{s}$ that has index less than k. Beyond that, every element will have a factor of k.

Thus $\forall k \in \mathbb{Z}, \exists m \in M : \overline{s} = k\overline{m}$.

□