Algebra III Fall 2024 Problem Set 5
Amin Zolfagharian - 610002072

Problem 1.

(i) Let $x, y \in Tor(M)$ and $r \in R$. We need to show that $rx + y \in Tor(M)$ in order to show that $Tor(M)$ is a submodule of M. Since both $x, y \in Tor(M)$, then there exists nonzero $r_x, r_y \in R$ such that $r_x x = 0$ and $r_y y = 0$. Now we show that $r_x r_y(rx+y) = 0$:

$$\begin{aligned}
r_x r_y(rx + y) &= r_x r_y rx + r_x r_y y \\
&= r_x r_y rx + r_x(r_y y) \\
&= r_x r_y rx \\
&= r_y r(r_x x) = 0
\end{aligned}$$

And since both r_x and r_y are nonzero therefore $r_x r_y$ is nonzero as well. This proves that $rx + y \in Tor(M)$ and thus $Tor(M)$ is a submodule of M.

(ii) Consider $\mathbb{Z}_6$ as a $\mathbb{Z}_6$ module. By definition we have:

$$Tor(\mathbb{Z}_6) = \{2, 3, 4\}$$

Which doesn't even form a group, let alone a submodule of M.

(iii) Let $m \neq 0 \in M$, where M is a R-module. And let $r_1 r_2 = 0$ where $r_1, r_2 \in R$ and $r_1, r_2 \neq 0$. If $r_2 m = 0$ then we are done since $m \in Tor(M)$. Otherwise consider $(r_1 r_2)m = r_1(r_2 m) = 0$ Since $r_2 m \neq 0$ then $r_2 m \in Tor(M)$. This completes the proof.

Problem 2.

Let $x, y \in \bigcup\limits_{k=1}^{\infty} N_k$ and $r \in R$. Therefore there exists $i, j \in \mathbb{N}$ such that $x \in N_i$ and $y \in N_j$. WLOG we can assume $i \leq j$. Since $N_i \subseteq N_j$ therefore we have $x, y \in N_j$. Since N_j is a submodule of M then we have:

$$\begin{aligned}
rx + y \in N_j \subseteq \bigcup_{k=1}^{\infty} N_k \\
\implies rx + y \in \bigcup_{k=1}^{\infty} N_k
\end{aligned}$$

Which shows that it is a submodule of M.

Problem 3.

Let M be an R-module, where scalar product is non-trivial. Now consider the $M \times M$ as a R-module. With componentwise addition and multiplication.

$$\begin{aligned}
M_1 = \{(m, 0) | m \in M\} \\
M_2 = \{(0, m) | m \in M\}
\end{aligned}$$

M_1 and M_2 are both sub-modules of $M \times M$ since:

$$\begin{aligned}\forall x, y \in M_1, \forall r \in R : rx + y &= r(m_x, 0) + (m_y, 0)\\ &= (rm_x, 0) + (m_y, 0)\\ &= (rm_x + m_y, 0) \in M_1\end{aligned}$$

Last lines is a direct result of M being a R-module. Now consider $M_1 \cup M_2$. And $x \neq 0 \in M_1$, $y \neq 0 \in M_2$ and $r \in R$ such that $rx \neq 0$:

$$rx + y = r(m_x, 0) + (0, m_y) = (rm_x, m_y)$$

Since both $rm_x \neq 0$ and $m_y \neq 0$, then $(rm_x, m_y) \neq M_1 \cup M_2$. This shows that $M_1 \cup M_2$ is not a sub-module of $M \times M$.

Problem 4.

Again consider $M = \mathbb{Z}_6$ as a $\mathbb{Z}_6$-module. And let $I = N = M$ We have $Tor_I(N) = \{2, 3, 4\}$ and $Ann_I(N) = \{0\}$ Thus $Tor_I(N) \neq Ann_I(N)$.

Problem 5.

(a) Let $r \in Ann_{\mathbb{Z}}(M)$. Then for any $(a, b, c) \in M$ we have $r(a, b, c) = (0, 0, 0)$. Let $a = 1_{\mathbb{Z}_{24}}, b = 1_{\mathbb{Z}_{15}}, c = 1_{\mathbb{Z}_{50}}$. Therfore we have:

$$r(a, b, c) = (r, r, r) = (0, 0, 0)$$

This shows that:

$$\left.\begin{aligned}24 &\mid r\\ 15 &\mid r\\ 50 &\mid r\end{aligned}\right\} \implies 2^3 \times 3 \times 5^2 = 600 \mid r \implies r \in 600\mathbb{Z}$$

And since for any $r \in 600\mathbb{Z}$ we have:

$$600(a, b, c) = (600a, 600b, 600c) = (0, 0, 0)$$

Which implies $r \in Ann_{\mathbb{Z}}(M)$, then we have $Ann_{\mathbb{Z}}(M) = 600\mathbb{Z}$.

(b) If $(a, b, c) \in Ann_M(2\mathbb{Z})$ then we have:

$$\begin{aligned}2 \in 2\mathbb{Z} : 2(a, b, c) = (2a, 2b, 2c) &= (0, 0, 0)\\ \implies a &\in \{0, 12\} \cong \mathbb{Z}_2\\ b &\in \{0\} \cong \mathbb{Z}_1\\ c &\in \{0, 25\} \cong \mathbb{Z}_2\end{aligned}$$

This shows that $Ann_M(2\mathbb{Z}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. It is easy to see that for any $2i \in 2\mathbb{Z}$ it works.

Problem 6.

Let $\varphi \in Hom_{\mathbb{Z}}(\mathbb{Z}_{30}, \mathbb{Z}_{21})$. Then φ is a group homomorphism from $\mathbb{Z}_{30}$ to $\mathbb{Z}_{21}$. Let r be the generator of $\mathbb{Z}_{30}$ having order 30. Then it must mapped to an element with order s where $s \mid 30$. And since $s \mid 21$ then we can only have $s = 1, 3$. If $s = 3$, there are only two elements with order 3 in $\mathbb{Z}_{21}$, namely 7 and 14. Also since $R = \mathbb{Z}$ then if φ is a homomorphism we have:

$$\varphi(rm) = \varphi(m + \cdots + m) = r\varphi(m)$$

Thus φ is also a module homomorphism. Therefore any module homomorphism from $\mathbb{Z}_{30}$ to $\mathbb{Z}_{21}$ is uniquely identified with $\varphi(1)$. And we have only 3 such homomorphism:

$$\begin{gathered}\varphi(1) = 7 \implies \varphi(m) = 7m \pmod{21}\\ \varphi(1) = 14 \implies \varphi(m) = 14m \pmod{21}\\ \varphi(1) = 0 \implies \varphi(m) = m \pmod{21}\end{gathered}$$

Which form a group of order 3, $\mathbb{Z}_3$.
Now since any $\mathbb{Z}$-module homomorphism is uniquely identifined with $\varphi(1)$, and we have:

$$\left.\begin{array}{l} Ord_{\mathbb{Z}_n}(\varphi(1)) \mid n \\ Ord_{\mathbb{Z}_n}(\varphi(1)) \mid Ord_{\mathbb{Z}_m}(1) = m \end{array}\right\} \implies Ord_{\mathbb{Z}_n}(\varphi(1)) \mid (n, m)$$

We only need to show that homomorphisms that map 1 to a members with order r in $\mathbb{Z}_n$ where $r \mid (n, m)$ form the group $\mathbb{Z}_{(m,n)}$. Let $\sigma \in Hom_{\mathbb{Z}}(\mathbb{Z}_m, \mathbb{Z}_n)$, where $\sigma(1) = s$ and $Ord(s) = (m, n)$. Now it is easy to see that $\sigma^r(1) = \sigma^{r-1}(s) = \cdots = s^r$. This shows that $Ord(\sigma) = Ord(s) = (m, n)$. On the otherhand the number of elements in $\mathbb{Z}_n$ such as s where $Ord_{\mathbb{Z}_n}(s) \mid (n, m)$ is exactly (m, n). This proves that σ generates the whole group and thus we have:

$$Hom_{\mathbb{Z}}(\mathbb{Z}_m, \mathbb{Z}_n) \cong \mathbb{Z}_{(m,n)}$$

Problem 7.

First we show that eM and $(1 - e)M$ is submodule of M:

$$\begin{gathered}x, y \in M \implies ex, ey \in eM, r \in R\\ r(ex) + ey = rex + ey = erx + ey = e(rx + y) \in eM\end{gathered}$$

Note that we used $re = er$ and also that since M is module then $rx + y \in M$. Similarly for $(1 - e)M$ we have:

$$\begin{aligned} r((1 - e)x) + (1 - e)y &= rx - rex + y - ey \\ &= rx + y - (erx - ey) \\ &= rx + y - e(rx - y) \in (1 - e)M \end{aligned}$$

It is obvious that since both eM and $(1-e)M$ are R module, so is $eM \oplus (1-e)M$. It remains to show an isomorphism:

$$\begin{aligned}
\varphi : M &\to eM \oplus (1-e)M \\
m &\mapsto (em, (1-e)m) \\
\varphi(m+m') &= (e(m+m'), (1-e)(m+m')) \\
&= (em, (1-e)m) + (em', (1-e)m') \\
&= \varphi(m) + \varphi(m'). \\
\varphi(rm) &= (erm, (1-e)rm) \\
&= (rem, (r-re)m) \\
&= (rem, r(1-e)m) \\
&= r(em, (1-e)m) = r\varphi(m).
\end{aligned}$$

This shows that φ is a homomorphism. Now to show that it is an isomorphism we have to show that it is both surjective and injective. Suppose $em+(1-e)m' \in eM \oplus (1-e)M$. For any $m, m' \in M$ we know $em + (1-e)m' \in M$. Thus we have:

$$\begin{aligned}
\varphi(em + (1-e)m') &= \big(e(em + (1-e)m'), (1-e)(em + (1-e)m')\big) \\
&= \big((e^2 m + (e - e^2)m'), (e - e^2)m + (1 - 2e + e^2)m'\big)
\end{aligned}$$

Sicne $e^2 = e$:

$$= \big(em, (1-e)m'\big)$$

This gives us that φ is surjective. For injective suppose $m, m' \in M$ where $m \neq m'$:

$$\begin{gathered}
\varphi(m) = \varphi(m') \\
\implies (em, (1-e)m) = (em', (1-e)m') \\
\implies em = em', (1-e)m = (1-e)m' \\
\implies e(m-m') = 0, (1-e)(m-m') = 0 \\
\implies e(m-m') + (1-e)(m-m') = 0 \\
\implies m - m' = 0 \implies m = m'
\end{gathered}$$

Which is a contradiction. This gives us that φ is bijective as well. Therefore φ is an isomorphism and thus we have:

$$M \cong eM \oplus (1-e)M$$

Problem 8.

(i) Suppose that R/I is free module with basis $E \subseteq R/I$ and I is non-trivial. Let $r+I \in E$. And let $s_1, s_2 \in I$ such that $s_1 \neq s_2$ and $s_1 r + I = s_2 r + I$. This always exists since I is non-trivial. Since $r + I \in E$ then we must have: $s_1(r+I) \neq s_2(r+I)$. But we have:

$$s_1(r+I) = s_1 r + I = s_2 r + I = s_2(r+I)$$

Which is a contradiction. Thus R/I is not a free module.

(ii) ($\Leftarrow$) If I is a principal ideal of R then we have $I = \langle a \rangle$ for some $a \in R$. Since I is an ideal of R then it's also a submodule of R. We show that $\{a\}$ is a basis for I over R. Any element in I is of the form ra for some $r \in R$. We have to show that this is unique. Since $\{a\}$ is linearly independent. Suppose there exists some $r_1 \neq r_2 \in R$ such that $r_1 a = r_2 a$:

$$r_1 a = r_2 a \implies a r_1 = a r_2 \implies a(r_1 - r_2) = 0$$

And since R is a integral domain then either $a = 0$ or $r_1 = r_2$. And since $a = 0$ makes a trivial ideal I then we have $r_1 = r_2$. Therefore I is a free module over R.
($\Rightarrow$) If I is a free module over R with basis E. If E has more than 1 element such a and b, then we have:

$$ba + (-a)b \in R$$

Since R is integral domain then we have: $ba - ab = 0$. And since $a, b \in E$ then they are linearly independent. Which means that $b = -a = 0$. Which is a contradiction supposing a and b are different elements in E. This shows that E has exactly 1 element a. And each element in I can be expressed as ra for some $r \in R$. This shows that $I = \langle a \rangle$. And thus I is a principal ideal of R.

Problem 9.

We prove that it is a module homomorphism. Consider φ:

$$\begin{aligned} \varphi : Hom_R(M_1 \times M_2, N) &\to Hom_R(M_1, N) \times Hom_R(M_2, N) \\ \sigma(-,-) &\mapsto \big(\sigma(-,0), \sigma(0,-)\big) \end{aligned}$$

It is obvious that both $\sigma(-,0)$ and $\sigma(0,-)$ are homomorphism. It remains to show that φ is a homomorphism:

$$\begin{aligned} \varphi(\sigma + \delta)(a, b) &= \big((\sigma + \delta)(a, 0), (\sigma + \delta)(0, b)\big) \\ &= \big(\sigma(a, 0) + \delta(a, 0), \sigma(0, b) + \delta(0, b)\big) \\ &= \big(\sigma(a, 0), \sigma(0, b)\big) + \big(\delta(a, 0), \delta(0, b)\big) \\ &= \varphi(\sigma)(a, b) + \varphi(\delta)(a, b) \end{aligned}$$

Also

$$\begin{aligned} \varphi(r\sigma)(a, b) &= \big(r\sigma(a, 0), r\sigma(0, b)\big) \\ &= r\big(\sigma(a, 0), \sigma(0, b)\big) \\ &= r\varphi(\sigma)(a, b) \end{aligned}$$

Thus φ is homomorphism. To show that it is an isomorphism we show that φ has an inverse.

$$\begin{aligned} \psi : Hom_R(M_1, N) \times Hom_R(M_2, N) &\to Hom_R(M_1 \times M_2, N) \\ \big(\sigma, \delta\big) &\mapsto \pi \end{aligned}$$

Where $\pi(a,b) = (\sigma(a), \delta(b))$. It is obvious that $\varphi^{-1} = \psi$. First we have to show that π is a homomorphism.

$$\begin{aligned}
\pi((a_1,b_1)+(a_2,b_2)) &= \pi(a_1+a_2, b_1+b_2) \\
&= (\sigma(a_1+a_2), \delta(b_1+b_2)) \\
&= (\sigma(a_1)+\sigma(a_2), \delta(b_1)+\delta(b_2)) \\
&= (\sigma(a_1), \delta(b_1)) + (\sigma(a_2), \delta(b_2)) \\
&= \pi(a_1,b_1) + \pi(a_2,b_2). \\
\pi(r(a_1,b_1)) &= \pi((ra_1, rb_1)) \\
&= (\sigma(ra_1), \delta(rb_1)) \\
&= (r\sigma(a_1), r\delta(b_1)) \\
&= r(\sigma(a_1), \delta(b_1)) \\
&= r\pi(a_1,b_1).
\end{aligned}$$

This shows that π is a homomorphism. Now to show that ψ is homomorphism.

$$\begin{aligned}
\psi((\sigma_1,\delta_1)+(\sigma_2,\delta_2))(a,b) &= \psi(\sigma_1+\sigma_2, \delta_1+\delta_2)(a,b) \\
&= ((\sigma_1+\sigma_2)(a), (\delta_1+\delta_2)(b)) \\
&= (\sigma_1(a)+\sigma_2(a), \delta_1(b)+\delta_2(b)) \\
&= (\sigma_1(a), \delta_1(b)) + (\sigma_2(a), \delta_2(b)) \\
&= \psi(\sigma_1,\delta_1)(a,b) + \psi(\sigma_2,\delta_2)(a,b)
\end{aligned}$$

Also:

$$\begin{aligned}
\psi(r(\sigma,\delta))(a,b) &= \psi(r\sigma, r\delta)(a,b) \\
&= (r\sigma(a), r\delta(b)) \\
&= r(\sigma(a), \delta(b)) \\
&= r\psi(\sigma,\delta)(a,b)
\end{aligned}$$

This shows that ψ is a homomorphism. And since it is the inverse of φ, therefore φ is an module isomorphism. Thus we have:

$$Hom_R(M_1 \times M_2, N) \cong_R Hom_R(M_1, N) \times Hom_R(M_2, N)$$

The second part is really similar and quite long.

Problem 10.

(i) Let $\psi_1(a_1, a_2, \dots) = (a_1, 0, a_2, 0, \dots)$, and $\psi_2(a_1, a_2, \dots) = (0, a_1, 0, a_2, \dots)$. Now we have:

$$\begin{aligned}
\varphi_1\psi_1(a_1, a_2, a_3, \dots) = \varphi_1(a_1, 0, a_2, 0, \dots) &= (a_1, a_2, a_3, \dots) \\
\implies \varphi_1 \circ \psi_1 &= 1
\end{aligned}$$

Similarly $\varphi_2\psi_2 = 1$. And also:

$$\begin{aligned}\varphi_2\psi_1(a_1, a_2, \dots) &= \varphi_2(a_1, 0, a_2, \dots) = (0, 0, 0, \dots) \\ &\implies \varphi_2 \circ \psi_1 = 0\end{aligned}$$

And similarly we $\varphi_1\psi_2 = 0$. And also:

$$\begin{aligned}(\psi_1\varphi_1 + \psi_2\varphi_2)(a_0, a_1, a_2, \dots) &= \psi_1(a_0, a_2, a_4, \dots) + \psi_2(a_1, a_3, a_5, \dots) \\ &= (a_0, 0, a_2, 0, a_4, \dots) + (0, a_1, 0, a_3, 0, \dots) \\ &= (a_0, a_1, a_2, \dots)\end{aligned}$$

Thus we have $\psi_1\varphi_1 + \psi_2\varphi_2 = 1$. With this we can generate any element in R. Consider $\sigma \in R$:

$$\sigma = \sigma(\psi_1\varphi_1 + \psi_2\varphi_2) = (\sigma\psi_1)\varphi_1 + (\sigma\psi_2)\varphi_2$$

To show that this representation is unique suppose that $\sigma_1\varphi_1 + \sigma_2\varphi_2 = \delta_1\varphi_1 + \delta_2\varphi_2$, then we have:

$$\begin{aligned}\sigma_1\varphi_1\psi_1 + \sigma_2\varphi_2\psi_1 &= \delta_1\varphi_1\psi_1 + \delta_2\varphi_2\psi_1 \\ \implies \sigma_1(1)\sigma_2(0) &= \delta_1(1) = \delta_2(0) \implies \sigma_1 = \delta_1\end{aligned}$$

Similarly with ψ_2 we can conclude that $\sigma_2 = \delta_2$. Which proves the uniqueness of representation. And since for $0\varphi_1 + 0\varphi_2 = 0$, the uniqueness of representation shows that if for some $\sigma_1, \sigma_2 \in R$ we have $\sigma_1\varphi_1 + \sigma_2\varphi_2 = 0$ then $\sigma_1 = \sigma_2 = 0$. Which proves that φ_1 and φ_2 are linearly independent. This proves that $\{\varphi_1, \varphi_2\}$ is a basis for R.

(ii) Let us define a homomorphism from $R \times R$ to R:

$$\begin{aligned}\phi : R \times R &\to R \\ (f, g) &\mapsto f\varphi_1 + g\varphi_2\end{aligned}$$

Since φ_1, φ_2 form a basis, thus ϕ is both injective and surjective. Checking the homomorphism is easy:

$$\begin{aligned}\phi((f_1, g_1) + (f_2, g_2)) &= \phi(f_1 + f_2, g_1 + g_2) \\ &= (f_1 + f_2)\varphi_1 + (g_1 + g_2)\varphi_2 \\ &= f_1\varphi_1 + g_1\varphi_2 + f_2\varphi_1 + g_2\varphi_2 \\ &= \phi(f_1, g_1) + \phi(f_2, g_2)\end{aligned}$$

Therefore ϕ is a homomorphism. This proves that $R \times R \cong R$. And by induction we can see that $R^n \cong R$.