MATH 830 FALL 2025: HOMEWORK 2 SOLUTIONS

Almost all mathematics papers written today are co-authored by two or more authors. For this assignment, you will work in groups of two. There are ten students currently enrolled in the class. Please choose your partner to work with and let me know who that is. You will work together as a team on this assignment and each team will turn in one set of solutions. These solutions should be **typeset using LaTex**. If you have not used LaTex before, this is a good opportunity to learn. Typically one learns by looking at a source file created by someone else and mimicking what they have done by cutting and pasting. One can also look online for any instructions for creating the math expressions you would like to use. Each member of the team must contribute both to the solutions and the typesetting. As before, for this assignment, you may use your notes, the Daily Summary, and any daily homework you have done. You may not consult outside sources, including, any algebra textbook, the internet, graduate students not in this class, or any professor except your Math 830 instructor. You may not cite any facts not covered in class or the homework. To receive full credit, all proofs must be complete and contain the appropriate amount of detail. Hard copies of each team's solutions are due in pdf format, Monday, October 13.

Throughout R will denote a commutative ring.

1.This problem shows that two of the facts established in class for finitely generated modules over a PID fail if the module is not finitely generated. In particular, these show: (i) If M is not finitely generated over the PID R, then $T(M)$ need not be a direct summand of M and (ii) An arbitrary torsion-free module over a PID need not be free. We take the case $R := \mathbb{Z}$. Let $\mathcal{P}$ denote the set of prime numbers in $\mathbb{Z}$ and set $M := \prod \mathbb{Z}_{p\in\mathcal{P}}$, the *direct product* of all $\mathbb{Z}_p$.

(i) Show that $T(M) = \bigoplus_{p\in\mathcal{P}} \mathbb{Z}_p$.
(ii) Show that $\bigcap_{p\in\mathcal{P}} pM = 0$, and thus $\bigcap_{p\in\mathcal{P}} pN = 0$, for any submodule $N \subseteq M$.
(iii) Set $x := (1, 1, 1, 1, \cdots) \in M$. Show that the image of x in $M/T(M)$ is not zero.
(iv) Show that the image of x in $M/T(M)$ belongs to $\bigcap_{p\in\mathcal{P}} p(M/T(M))$.
(v) Conclude: (i) $T(M)$ is not a direct summand of M and (ii) $M/T(M)$ is torsion-free, but not free.

Solution. (i) We first show $T(M) = \bigoplus_{p\in\mathcal{P}} \mathbb{Z}_p$. Suppose $x = (a_p)_{p\in\mathcal{P}} \in \bigoplus_p \mathbb{Z}_p$. Then only finitely many a_p are no-zero. If $p_1, \ldots, p_r$ are the primes for which $a_{p_i} \neq 0$, then for $0 \neq c := p_1 \cdots p_r$, we have $cx = 0$ in M, so that $x \in T(M)$. Conversely, suppose $0 \neq z = (b_p)_{p\in\mathcal{P}}$ and $rz = 0$, for $0 \neq r$ in $\mathbb{Z}$. Then $rb_p \equiv 0$ module $p\mathbb{Z}$, for all p. If $b_p \not\equiv 0$ in $\mathbb{Z}_p$, then $p \mid r$. Thus, we can only have finitely many primes p for which $b_p \not\equiv 0$ in $\mathbb{Z}_p$, so that $z \in T(M)$, which gives what we want.

(ii) Next we show that $\bigcap_{p\in\mathcal{P}} pM = 0$, and thus $\bigcap_{p\in\mathcal{P}} pN = 0$, for any submodule $N \subseteq M$. For this, notice that for primes $p \neq q$, $p\mathbb{Z}_q = \mathbb{Z}_q$ and for $q = p$, $p\mathbb{Z}_p = 0$. Thus, pM is the set of $\mathcal{P}$-tuples in M that are zero in the pth coordinate. Intersecting these as p varies over all primes gives the zero module.

(iii) Now set $x := (1, 1, 1, 1, \ldots) \in M$. Note that by the first step, $x \notin T(M)$, since it has infinitely many non-zero coordinates, and thus the image of x in $M/T(M)$ is not zero.

(iv) We next show that that the image of x in $M/T(M)$ belongs to $\bigcap_{p\in\mathcal{P}} p(M/T(M))$. Fix $p \in \mathcal{P}$ and note that the image of x in $M/T(M)$ belongs to $p(M/T(M)$ if and only if $x \in pM + T(M)$ in M. Let e_p denote the element of M that is 1 in the pth coordinate and 0 elsewhere. Then $e_p \in T(M)$ and by the description of pM above, $x \in pM + Re_p \subseteq pM + T(M)$. Since this is true for all p, the image of x in $M/T(M)$ belongs to $\bigcap_{p\in\mathcal{P}} p(M/T(M))$.

(v) Finally, we show that $T(M)$ is not a direct summand of M and $M/T(M)$ is torsion-free, but not free. For this, we first note that if $T(M)$ were a summand of M, we would have $M = T(M) \oplus K$, for some submodule $K \subseteq M$. But then $K \cong M/T(M)$. By part (ii), $\bigcap_{p\in\mathcal{P}} pK = 0$, while on the other hand, by parts (iii) and (iv) x is a non-zero element of $\bigcap_{p\in\mathcal{P}} pK$, a contradiction. Thus, $T(M)$ is not a summand of M. For all modules M, $M/T(M)$ is torsion-free. However, in the present case, if $M/T(M)$ were free, the canonical exact sequence $0 \to T(M) \to M \to M/T(M) \to 0$ would split and $T(M)$ would be a summand of M, contradicting what we just proved. Therefore, $M/T(M)$ is a non-free, torsion-free module over the PID $\mathbb{Z}$. □

2. Suppose R is a PID and $M = \langle x\rangle \oplus \langle y\rangle$ with non-zero x, y satisfying $\text{ann}(x) = aR$, $\text{ann}(y) = bR$, and GCD $(a, b) = 1$.

(i) Show that $\text{ann}(x + y) = abR$.
(ii) Show that $M = \langle x + y\rangle$. Hint: Adapt the proof of the Chinese remainder theorem.

Solution. For (i), suppose $t \in R$. Clearly $t \in \text{ann}(x + y)$ if $t \in abR$. Conversely, suppose $t \in \text{ann}(x + y)$. Then $tx + ty = 0$, and the direct sum decomposition implies $tx = 0$ and $ty = 0$. Thus in R, $a \mid t$ and $b \mid t$. Since $\text{GCD}(a, b) = 1$, $ab \mid t$, showing $t \in abR$. Thus, $\text{ann}(x + y) = abR$. □

For (ii), we have to show the following, for $r, s \in R$, $rx + sy = c(x + y)$, for some $c \in R$. We can write $ua + vb = 1$ in R. It follows that $x = vbx$ and $y = uay$. Thus, Thus, $rx + sy = rvbx + suay = (rvb + sua) \cdot (x + y)$, which gives what we want. □

3. Prove the following variation of Nakayama's lemma: Let M be a finitely generated R-module and $J \subseteq R$ a proper ideal. If $JM = M$, then there exists $j \in J$ such that $(1+j) \cdot M = 0$.

Solution. We start with two easy observations. The first is that it suffices to find $j \in J$ such that $(1-j) \cdot M = 0$ and the second is that any product of the form $(1-c_1)\cdots(1-c_r)$ with each $c_i \in J$ is of the form $1-j$, for some $j \in J$. . We proceed by induction on the number of generators of M. If $M = \langle x \rangle$, then by hypothesis we have $x = jx$, for some $j \in J$, so that $(1-j)x = 0$, and hence $(1-j)M = 0$.

Now suppose $M = \langle x_1, \ldots, x_n \rangle$, with $n > 1$. We first note that we can write $x_1 = j_1x_1 + \cdots + j_nx_n$, so that $(1-j_1)x_1 \in JN$, for $N := \langle x_2, \ldots, x_n \rangle$. Suppose we could show $JN = N$, then by induction, $(1-j') \cdot N = 0$, for some $j' \in J$. Thus, from the inclusion $(1-j_1)x_1 \subseteq JN$, we have $(1-j_1)(1-j')x_1 = 0$. Thus, $(1-i)x_1 = 0$, for some $i \in J$. Therefore,

$$\begin{aligned}(1-i)(1-j)' \cdot M &= (1-i)(1-j') \cdot \langle x \rangle + (1-i)(1-j') \cdot N \\ &= 0 + 0 = 0,\end{aligned}$$

which gives what we want by the second observation. To see that $JN = N$, for $2 \leq i \leq n$, write $x_i = c_1x_1 + \cdots + c_nx_n$, with each $c_i \in J$. Thus,

$$(1-c_i)x_i = c_1x_1 + \cdots + c_{i-1}x_{i-1} + c_{i+1}x_{i+1} + \cdots + c_nx_n.$$

Multiplying by $(1-j_1)$ we get

$$\begin{aligned}(1-j_1)(1-c_i)x_i &= c_i(j_2x_2 + \cdots j_nx_n) + (1-j_1)c_2x_2 + \cdots + (1-j_1)c_{i-1}x_{i-1} + (1-j_1)c_{i+1}x_{i+1} + \cdots + (1-j_1)c_nx_n. \\ &= d_2x_2 + \cdots + d_nx_n,\end{aligned}$$

for $d_i \in J$. Writing $(1-j_1)(1-c_i) = 1-e$, for $e \in J$, we have $x_i = ex_i + d_2x_2 + \cdots + d_nx_n$, showing that $x_i \in JN$. Doing this for each $2 \leq i \leq n$ gives $N \subseteq JN$, which is what we want.

4. Let $R := \mathbb{Z}[\sqrt{-5}] := \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ and let I denote the ideal of R generated by 3 and $2+\sqrt{-5}$. This problem shows that I is a non-free, projective R-module.

(i) Let $x := a3 + b(2+\sqrt{-5})$, with $a, b \in R$ be an element of I. Show that there exist *unique* $u, v \in R$ such that $(2-\sqrt{-5})x = 3u$ and $(1+\sqrt{-5})x = 3v$.

(ii) Define $\phi : R^2 \to I$ as follows: $\phi(\begin{pmatrix} u \\ v \end{pmatrix}) = u3 + v(2+\sqrt{-5})$. For each x as in (i), define $j(x) = \begin{pmatrix} u \\ v \end{pmatrix}$. Observe that $j : I \to R^2$ is a well-defined R-module homomorphism, and then prove $\phi j = 1_I$.

(iii) Conclude that I is a projective R-module.

(iv) Recall the norm $N : R \to \mathbb{Z}$ defined by $N(a+b\sqrt{-5}) = a^2+5b^2$. Show that N is multiplicative, i.e., $N(xy) = N(x)N(y)$, for $x, y \in R$

(v) Show that I is not a principal ideal and conclude that I is not a free R-module.

Solution. For (i), it is easy to check that $u = 2a + 3b - a\sqrt{-5}$ and $v = a - b + (a+b)\sqrt{-5}$ satisfy the requirements and are unique. For (ii), the uniqueness of u and v show that j is well defined, and it is straight forward to check that j is an R-module homomorphism. A quick check shows that

$$\begin{aligned}\phi(\begin{pmatrix} u \\ v \end{pmatrix}) &= u \cdot 3 + v \cdot (2+\sqrt{-5}) \\ &= (2a + 3b - a\sqrt{-5}) \cdot 3 + (a - b + (a+b)\sqrt{-5}) \cdot (2+\sqrt{-5}) \\ &= a \cdot 3 + b(2+\sqrt{-5}),\end{aligned}$$

so that $\phi j = 1_I$, as required. Finally, from class we have that $R^2 = j(I) \oplus K$, where K is the kernel of ϕ showing that I is a projective R-module (since $I \cong j(I)$). □

Part (iv) is a straight forward calculation. For part (v) we first note that since $N(xy) = N(x)N(y)$, for $x, y \in R$, $a + b\sqrt{-5}$ is a unit in R if and only if $a = \pm 1$ and $b = 0$. Now suppose that I is a principal ideal. Then there exists $f \in I$ such that $I = R \cdot f$. Let us first eliminate the case that f is a unit in R, i.e., $I = R$. Suppose, by way of contradiction, that $I = R$. If we note that $R = \mathbb{Z}[X]/(X^2+5)$ (you should check this), then I corresponds to the ideal $(3, 2+X)/(X^2+5)$ so that if $I = R$, it would follow that $(3, X+2) = \mathbb{Z}[X]$. Write $1 = g(X) \cdot 3 + h(X) \cdot (2+X)$, for $g(X), h(X) \in \mathbb{Z}[X]$. If we set $X = -2$, then we have $1 = g(-2) \cdot 3$ in $\mathbb{Z}$, which is a contradiction. It follows that $I \neq R$, so f is not a unit in R.

Now write $3 = r \cdot f$, for $r \in R$. Then $9 = N(3) = N(r) \cdot N(f)$. Since $N(f) \neq 1$, either $N(r) = 3$ or $N(r) = 1$. The first case can never hold, since the equation $3 = a^2 + 5b^2$ has no solutions in $\mathbb{Z}$. If $N(r) = 1$, then $r = \pm 1$, so that $I = 3 \cdot R$. But then we may write $2 + \sqrt{-5} = (a + b\sqrt{-5}) \cdot 3$ in R, and this clearly cannot hold. Thus, it follows that I is not a principal ideal, and therefore, is not a free R-module. □

5. Let $S \subseteq R$ be a multiplicatively closed subset and M an R-module. For $(s, m), (s', m')$ in $S \times M$, defined $(s, m) \sim (s', m')'$ if there exists $s'' \in S$ such that $s''(s'm - sm') = 0$.

(i) Show the relation defined above is an equivalence relation.

(ii) Writing m/s for the equivalence class of (s, m) let M_S denote the set of all such equivalence classes and prove that M_S has a well-defined structure as an R_S-module.

Solution. Very straight forward.

6. Given an exact sequence $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ of R-modules and a multiplicatively closed set $S \subseteq R$, prove that the induced sequence of R_S-modules $0 \to A_S \xrightarrow{f_S} B_S \xrightarrow{g_S} C_S \to 0$ is exact.

Solution. Suppose $f_S(a/s) = 0/1$, for $a/s \in A_S$. Then $f(a)/s = 0/1$ in A_S, so $s'f(a) = 0$ in A, for some $s' \in S$. Thus $f(s'a) = 0$, so $s'a = 0$, since f is 1-1. It follows that $a/s = 0$ in A_S, so f_S is 1-1.

Let $a/s \in A_S$. Then $g_S(f_S(a/s)) = g(f(a))/s = 0/s = 0/1$, showing that the image of f_S is in the kernel of g_S. Conversely, suppose $g_S(b/s)) = 0/1$. Then $s'g(b) = 0$ in C, for some $s' \in S$. Thus, $g(s'b) = 0$, so $s'b = f(a)$, for some $a \in A$. Thus, $f(a)/s' = b/1$ in B_S, so $f(a)/ss' = b/s$ in B_S, and it follows that $f_S(a/ss') = b/s$, so that the kernel of g_S is contained in the image of f_S. Therefore exactness holds at B_S.

Finally, suppose $c/s \in C_S$. Then $c = g(b)$, for some $b \in B$ and thus, $g_S(b/s) = c/s$, showing that g_S is onto. Thus, the induces sequence over R_S is exact. □

7. Given a short exact sequence $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ of R-modules, show that there are exact sequences

(i) $0 \to \mathrm{Hom}_R(C, M) \xrightarrow{g^*} \mathrm{Hom}_R(B, M) \xrightarrow{f^*} \mathrm{Hom}_R(A, M)$

(ii) $0 \to \mathrm{Hom}_R(M, A) \xrightarrow{\hat{f}} \mathrm{Hom}_R(M, B) \xrightarrow{\hat{g}} \mathrm{Hom}_R(M, C)$.

for appropriately defined maps $f^*, g^*, \hat{f}, \hat{g}$.

Solution. One notes that $g^*(\alpha) := \alpha g$, for $\alpha \in \mathrm{Hom}_R(C, M)$ and $\hat{g}\beta = g\beta$, for $\beta \in \mathrm{Hom}_R(M, B)$, with f^* and $\hat{f}$ defined similarly. It is easy to check that the starred and hatted induced maps are R-module homomorphisms.

We show (i) as the proof of (ii) is similar. Suppose $g^*(h) = 0$, for $h \in \mathrm{Hom}_R(C, M)$. Then $hg = 0$ as a map from B to M. Take $c \in C$. Then, $c = g(b)$, for some $b \in B$, so that $h(c) = hg(b) = 0$, showing $h = 0$, so that g^* is injective.

Take $h \in \mathrm{Hom}_R(C, M)$, Then,

$$f^*g^*(h)) = f^*(hg) = (hg)(f) = hgf = 0,$$

since $gf = 0$. Thus the image of g^* is contained in the kernel of f^*. Conversely, suppose $j \in \mathrm{Hom}_R(B, M)$ and $f^*(j) = 0$. Then $jf = 0$. Then $jf(a) = 0$, for all $a \in A$. Thus, j maps the kernel of g to zero, so there is an induced map $j' : B/\ker(g) \to M$, where $j'(\bar{b}) := j(b)$, and $\bar{b}$ is the class of b in $B/\ker(g)$. Now, $B/\ker(g) \cong C$, the isomorphisms being given by the induced map $g' : B/\ker(g) \to C$. We define $l : C \to M$ by $l = j'(g')^{-1}$. We now note that $g^*(l) = j$, i.e., $lg = j$. Take $b \in B$. Then, $lg(b) = l(g(b)) = j'(g')^{-1}(g(b)) = j'(\bar{b}) = j(b)$, which gives what we want. Thus, exactness in the sequence 2(i) holds at $\mathrm{Hom}_R(B, M)$. □

8. Assume the short exact sequence $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ splits. Prove that f^* in 7(i) and $\hat{g}$ in 7(ii) are surjective. In other words, the given exact sequence remains exact upon applying $\mathrm{Hom}_R(-, M)$ and $\mathrm{Hom}_R(M, -)$.

Solution. We just show f^* is surjective, the proof that $\hat{g}$ is surjective is similar. Suppose $j : C \to B$ is the splitting, so that $B = f(A) \oplus j(C)$. Let $h \in \mathrm{Hom}_R(A, M)$ and define $t : B \to M$ as follows. For $b \in B$, write $b = f(a) + j(c)$, for $a \in A$ and $c \in C$. Then $f(a)$ is unique, by the directness of the sum, and a is unique, since f is 1-1. Set $t(b) := h(a)$. Then it is easy to check that $t \in \mathrm{Hom}_R(B, M)$, and by definition, $tf(a) = h(a)$, for all $a \in A$. Thus, $f^*(t) = h$, showing that f^* is surjective. □

9. Fix a prime $p \in \mathbb{Z}$ and let $\mathbb{Z}_{p^\infty}$ denote the set of elements in $\mathbb{Q}/\mathbb{Z}$ annihilated by some power of p. Show (i) $\mathbb{Z}_{p^\infty}$ is an injective $\mathbb{Z}$-module and (ii) $\mathbb{Q}/\mathbb{Z}$ is the internal direct sum of $\mathbb{Z}_{p^\infty}$, as p ranges over the set of prime integers.

Solution. For (i),it suffices to show that $\mathbb{Z}_{p^\infty}$ is a divisible $\mathbb{Z}$-module. Take $n \in \mathbb{Z}$ and $x \in \mathbb{Z}_{p^\infty}$. It is straight forward to check that $x = [\frac{a}{p^i}]$ is the class of a fraction of the form $\frac{a}{p^i}$, with $a \in \mathbb{Z}$. Suppose $n = p^e n_o$, with p not dividing n_0. Then we can write $1 = up^i + vn_0$, for $u, v \in \mathbb{Z}$. Thus, $p^e = up^{i+e} + vn$, so $\frac{a}{p^i} = au + \frac{avn}{p^{i+e}}$. Thus, in $\mathbb{Z}_{p^\infty}$, $x = [\frac{a}{p^i}] = n[\frac{av}{p^{i+e}}]$, which is what we want.

For (ii), take $x := [\frac{a}{b}] \in \mathbb{Q}/\mathbb{Z}$. We may assume $b > 0$. Write $b = p_1^{e_1} \cdots p_r^{e_r}$, for primes $p_1, \ldots, p_r \in \mathbb{Z}$. We want to show that x is a sum of elements from $\mathbb{Z}_{p_i^\infty}$, for $1 \le i \le r$. For each $1 \le i \le r$, set $n_i := \prod_{j \neq i} p_j^{e_j}$. Since $\mathrm{GCD}(n_1, \ldots, n_r) = 1$, the ideal generated by $n_1, \ldots, n_r$ is $\mathbb{Z}$. Thus, there exist $a_i \in \mathbb{Z}$ such that $1 = a_1 n_1 + \cdots + a_r n_r$. It follows that $\frac{1}{b} = \frac{1}{p_1^{e_1} \cdots p_r^{e_r}} = \frac{a_1}{p_1^{e_1}} + \cdots + \frac{a_r}{p_r^{e_r}}$. Thus, $[x] = [\frac{aa_1}{p_1^{e_1}}] + \cdots + [\frac{aa_r}{p_r^{e_r}}]$ in $\mathbb{Q}/\mathbb{Z}$. Thus $\mathbb{Q}/\mathbb{Z}$ is the sum of the submodules $\mathbb{Z}_{p^\infty}$ as p ranges over the primes in $\mathbb{Z}$.

For directness of the sum, it suffices to show that if we have sum

$$(*) \qquad [\frac{a_1}{p_1^{e_1}}] + \cdots + [\frac{a_r}{p_r^{e_r}}] = 0$$

in $\mathbb{Q}/\mathbb{Z}$, then each $[\frac{a_i}{p_i^{e_i}}] = 0$. To see this, set $n_i := \prod_{j \neq i} p_j^{e_j}$ so that

$$0 = [\frac{a_1}{p_1^{e_1}}] + \cdots + [\frac{a_r}{p_r^{e_r}}] = [\frac{a_1 n_1 + \cdots + a_r n_r}{p_1^{e_1} \cdots p_r^{e_r}}]$$

in $\mathbb{Q}/\mathbb{Z}$. Thus, there exists $t \in \mathbb{Z}$ such that $a_1 n_1 + \cdots + a_r n_r = t \cdots p_1^{e_1} \cdots p_r^{e_r}$ in $\mathbb{Z}$. Thus, $p_1^{e_1}$ divides the left side of this last equation, and hence divides $a_1 n_1$. This forces $p_1^{e_1} \mid a_1$. Writing $a_1 = a_1' p_1^{e_1}$, we have $[\frac{a_1}{p_1^{e_1}}] = [\frac{a_1' p_1^{e_1}}{p_1^{e_1}}] = [\frac{a_1'}{1}] = 0$ in $\mathbb{Q}/\mathbb{Z}$. A similar argument shows that $[\frac{a_i}{p_i^{e_i}}] = 0$, for $2 \leq i \leq r$, which gives what we want, and completes the proof. □

10. Assume R is an integral domain and M is a torsion-free, divisible R-module. Show that M is an injective R-module. Conclude that K is an injective R-module for any field K containing R.

Solution. Given an ideal $I \subseteq R$, we must find ρ that completes the diagram

$$\begin{array}{ccccc} 0 & \longrightarrow & I & \xrightarrow{i} & R \\ & & \downarrow{\scriptstyle g} & \swarrow{\scriptstyle \rho} & \\ & & M & & \end{array} .$$

Take $0 \neq j \in I$. Since M is divisible, there exists $m_j \in M$ such that $jm_j = g(j)$. We claim that m_j is independent of $j \in J$. If so, then there exists $m \in M$ such that $jm = g(j)$, for all $j \in J$. In this case, we define $\rho : R \to M$ by $\rho(r) = rm$. Then, for $j \in J$, we have $\rho i(j) = \rho(j) = jm = g(j)$, which shows that M is an injective R-module.

For the claim, take $j_1, j_2 \in J$. On the one hand, we have $j_1 m_{j_1} = g(j_1)$ and $j_2 m_{j_2} = g(j_2)$. On the other hand $j_1 g(j_2) = g(j_1 j_2) = j_2 g(j_1)$, so it follows that $j_1 j_2 m_{j_1} = j_1 j_2 m_{j_2}$. Since $j_1 j_2 \neq 0$ and M is torsion-free, we have $m_{j_1} = m_{j_2}$, which proves the claim.

For the second statement, if K is a field containing R, then clearly K is a torsion-free, divisible R-module, and hence K is an injective R-module. □