MATH 500
Problem Set 10

Anthony D'Arienzo

apd6@illinois.edu

4 April 2022

Exercise 1 (DF 12.1.6): Let R be an integral domain and M any non-principal ideal of R such that $M \neq (0)$, considered as an R-module. Show that (i) M is torsion free and (ii) $\operatorname{rank} M = 1$, but (iii) M is not a free module.

Proof of (i). Let x be an element of M. Suppose $rx = 0$, where $r \neq 0$. Since R is an integral domain, this implies $x = 0$ (M is an ideal of R, so x is an element of R). Thus, if $x \in M$ is torsion, then $x = 0$: $M_{\text{tors}} = \{0\}$. ■

Proof of (ii). Let x, y be any two elements of M. Then yx and xy are elements of M. Integral domains are commutative, so $yx - xy = yx - yx = 0$, so x and y are linearly dependent. Since x and y are arbitrary, this shows that $\operatorname{rank} M < 2$. Since $M \neq (0)$, $\operatorname{rank} M > 0$, so $\operatorname{rank} M = 1$. ■

Proof of (iii). Suppose, for the purpose of deriving a contradiction, that M were a free module. Since the basis of a free module is always linearly independent, and $\operatorname{rank} M = 1$, the basis of M must be a single element $x_0 \in M$. That is, every element y of M is uniquely equal to an expression of the form rx_0 for some $r \in R$. M is an ideal of R, so this implies $M = (x_0)$. Since M is not principal, we have a contradiction. Therefore M is not free. ■

* * * * *

Exercise 2 (DF 12.1.7): Let R be any ring, $A_1, \ldots, A_m$ be R-modules, and $B_k \subseteq A_k$ submodules. Show that there is an isomorphism $(A_1 \oplus \ldots \oplus A_m)/(B_1 \oplus \ldots \oplus B_m) \cong (A_1/B_1) \oplus \ldots \oplus (A_m/B_m)$ of modules.

Proof. Let $M \overset{\text{def}}{=} (A_1 \oplus \ldots \oplus A_m)/(B_1 \oplus \ldots \oplus B_m)$ and $N \overset{\text{def}}{=} (A_1/B_1) \oplus \ldots \oplus (A_m/B_m)$. Then N is the coproduct of the modules A_i/B_i. Therefore it suffices to show that M satisfies the universal property of this coproduct. Suppose we have a family of morphishms $f_i : A_i/B_i \to X$ for $i \in \{1, \ldots, m\}$, where X is some R-module. Let $\pi_i : A_i \to A_i/B_i$ be the quotient morphism. Then $f_i \circ \pi_i : A_i \to X$ is a morphism of R-modules. The universal property of $A_1 \oplus \ldots \oplus A_m$ tells us that there exists a unique morphism $\hat{f} : A_1 \oplus \ldots \oplus A_m \to X$ such that the following diagram commutes for all $i \in \{1, \ldots, m\}$.

$$\begin{tikzcd}
A_i \arrow[r, "\pi_i"] \arrow[dr, "\iota_i"'] & A_i/B_i \arrow[r, "f_i"] & X \\
& A_1 \oplus \ldots \oplus A_m \arrow[ur, dashed, "\hat{f}"'] &
\end{tikzcd} \tag{2.1}$$

where $\iota_i : A_i \to A_1 \oplus \ldots \oplus A_m$ is the canonical inclusion morphism. Furthermore $\iota_i(B_i)$ is contained in the kernel of the map $A_i \to A_1 \oplus \ldots \oplus A_m \to M$ since $\iota_i(B_i)$ is a submodule of $B_1 \oplus \ldots \oplus B_m$. Therefore the universal property of the quotient gives us a unique map $\rho_i : A_i/B_i \to M$ fitting into the following diagram.

$$\begin{tikzcd}
A_i \arrow[r, "\pi_i"] \arrow[dr, "\iota_i"'] & A_i/B_i \arrow[dd, dashed, bend left, "\exists! \rho_i"] \\
& A_1 \oplus \ldots \oplus A_m \arrow[d] \\
& M
\end{tikzcd} \tag{2.2}$$

Lastly, we show that $B_1 \oplus \ldots \oplus B_m$ is contained in the kernel of $\hat{f}$. Note that it suffices to show that $\iota_i(B_i)$ is contained in the kernel of $\hat{f}$, because (by definition) $B_1 \oplus \ldots \oplus B_m = \iota_1(B_1) \oplus \ldots \oplus \iota_m(B_m)$. Since B_i is contained in $\ker \pi_i \circ f_i$, Diagram $\boxed{2.1}$ shows that $\iota_i(B_i)$ is contained in $\ker \hat{f}$, as desired. Therefore $B_1 \oplus \ldots \oplus B_m \leqslant \ker \hat{f}$; hence $\hat{f}$ itself induces a unique morphism $\bar{f} : M \to X$ making the following diagram commute.

$$\begin{tikzcd}
A_i \arrow[r, "\pi_i"] \arrow[dr, "\iota_i"'] & A_i/B_i \arrow[r, "f_i"] & X \\
& A_1 \oplus \ldots \oplus A_m \arrow[ur, "\hat{f}"'] \arrow[d] & \\
& M \arrow[uur, dashed, "\exists! \bar{f}"'] &
\end{tikzcd} \tag{2.3}$$

Using Diagram $\boxed{2.2}$, we can replace the left side with ρ_i:

$$\begin{tikzcd}
A_i/B_i \arrow[r, "f_i"] \arrow[d, "\rho_i"'] & X \\
M \arrow[ur, dashed, "\exists! \bar{f}"'] &
\end{tikzcd}$$

This is the universal property for the coproduct N. Therefore $M \cong N$. ■

* * * * *

Exercise 3 (DF 12.1.8): Let R be a PID, B a torsion R-module, and p a prime element in R. Prove that if $pb = 0$ for some $b \in B, b \neq 0$, then $\mathrm{Ann}(B) \subseteq (p)$. (Recall that $\mathrm{Ann}(B) \overset{\text{def}}{=} \{r \in R \mid rB = 0\}$).

Proof. Rb is a submodule of B, so it is a module in its own right. Since $pb = 0$, $p \in \mathrm{Ann}(Rb)$; hence $\mathrm{Ann}(Rb) \neq (0)$. Since $b \neq 0$, $1 \cdot b \neq 0$, so $\mathrm{Ann}(Rb)$ is not the unit ideal.

Therefore Ann(Rb) is a nontrivial ideal in the PID R, so Ann(Rb) is a principal ideal. Since p is prime, (p) is maximal amoung principal ideals, therefore Ann(Rb) $=$ (p). Any element $r \in R$ which annihilates all of B will annihilate b in particular. Thus $\mathrm{Ann}(B) \subseteq \mathrm{Ann}(Rb)$; hence $\mathrm{Ann}(B) \subseteq (p)$. ■

* * * * *

Exercise 4 : Let R be a ring with 1, not necessarily commutative. Show that if $I, J \subseteq R$ are left ideals such that $J = Ia$ for some $a \in R^{\times}$, then $R/I \cong R/J$ as modules.

Proof. We will show that R/I satisfies the universal property of R/J. Let $\phi : R \to N$ be a morphism of R-modules such that $J \subseteq \ker\phi$. We define a new morphism $\overline{\phi} : R/I \to N$ of R-modules by setting:

$$\overline{\phi}(\overline{x}) \overset{\text{def}}{=} \phi(xa).$$

To show that this is well-defined, suppose $y \in I$, so there exists an element $z \in J$ such that $y = za^{-1}$. Then $ya) = \phi(z) = 0$ since $z \in \ker\phi$; hence $\overline{\phi}$ is a well-defined (set)-function from R/I to N. We now show that $\overline{\phi}$ is linear:

$$\overline{\phi}(r\overline{x} + s\overline{y}) = \phi((rx+sy)a) = \phi(rxa + sya) = r\phi(xa) + s\phi(ya) = r\overline{\phi}(\overline{x}) + s\overline{\phi}(\overline{y}).$$

Furthermore we can define an R-module morphism $\pi' : R \to R/I$ by setting $\pi'(x) \overset{\text{def}}{=} \overline{xa^{-1}}$. Since $J = Ia$, $\ker\pi'$ contains J (in fact, $J = Ia$ implies $\ker\pi' = J$). Moreover, $\overline{\phi}(\pi'(x)) = \phi(xa^{-1}a) = \phi(x)$, so the following triangle commutes.

$$\begin{tikzcd} R \arrow[r, "\phi"] \arrow[d, "\pi'"'] & N \\ R/I \arrow[ur, dotted, "\overline{\phi}"'] & \end{tikzcd}$$

All that is left to check is that $\overline{\phi}$ is unique. Since π' is surjective, the requirement that $\overline{\phi} \circ \pi' = \phi$ forces a unique definition for $\overline{\phi}$.

Thus $\pi' : R \to R/I$ satisfies the universal property of the quotient R/J. Since quotients are unique up to isomorphism, $R/I \cong R/J$. ■

* * * * *

Exercise 5 : Let $R \overset{\text{def}}{=} M_{2\times 2}(F)$ with F a field. Find examples of left ideals $I, J \subseteq R$ such that $R/I \cong R/J$ as modules but $I \neq J$.

Proof. Let I denote the collection of all matrices $A \in R$ such that $A\binom{1}{0} = 0$, and let J denote the collection of all matrices $B \in R$ such that $B\binom{0}{1} = 0$.

I is a left-ideal: for any $M_1, M_2 \in R$ and $A_1, A_2 \in I$,

$$(M_1A_1 - M_2A_2)\begin{pmatrix}1\\0\end{pmatrix} = M_1\left(A_1\begin{pmatrix}1\\0\end{pmatrix}\right) - M_2\left(A_2\begin{pmatrix}1\\0\end{pmatrix}\right) = 0.$$

A similar argument shows that J is also a left-ideal. Furthermore, the matrix

$$\sigma \stackrel{\text{def}}{=} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

is an element of $R^\times$ (it is its own inverse). Since $I\sigma = J$, Exercise $\boxed{4}$ implies $R/I \cong R/J$. However, $I \neq J$: $\left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ is an element of I but not an element of J. ■

* * * * *

Exercise 6 (DF 12.2.10): Find all similarity classes of 6×6 matrices over $\mathbb{Q}$ with minimal polynomial $(x+2)^2(x-1)$.

***

It suffices to give all lists of invariant factors and write out some of their corresponding matrices.

***

Proof. Let $P \stackrel{\text{def}}{=} (x+2)^2(x-1)$. Let $V \stackrel{\text{def}}{=} \mathbb{Q}^6$ and $T : V \to V$ be a matrix with minimal polynomial P. Then V_T decomposes into a sum

$$V_T \cong \mathbb{Q}[x]/(f_1) \oplus \ldots \oplus \mathbb{Q}[x]/(f_k),$$

where $f_1 \mid f_2 \mid \ldots \mid f_k$ are all monic polynomials. Since the minimal polynomial is the largest invariant factor, $f_k = P$. Furthermore $\dim_{\mathbb{F}} V_T = \deg f_1 + \ldots + \deg f_k$. $\deg f_k = 3$, so $\deg f_1 + \ldots + \deg f_{k-1} = 3$, leaving the following possibilities:

- $k = 4$ and $\deg f_1 = \deg f_2 = \deg f_3 = 1$,
- $k = 3$ and $\deg f_1 = 1$ and $\deg f_2 = 2$,
- $k = 2$ and $\deg f_1 = 3$.

Since the invariant factors must divide P, this yields six classes.

1. $f_1 = f_2 = P$;
2. $f_1 = f_2 = f_3 = x-1$ and $f_4 = P$;
3. $f_1 = f_2 = f_3 = x+2$ and $f_4 = P$;
4. $f_1 = x+2$, $f_2 = (x+2)^2$, and $f_3 = P$;
5. $f_1 = x+2$, $f_2 = (x+2)(x-1)$, and $f_3 = P$;
6. $f_1 = x-1$ and $f_2 = (x+2)(x-1)$, and $f_3 = P$.

Any matrix is similar to its rational canonical form, so these six classes correspond bijectively to the collection of similarity classes of $M_{6\times 6}(\mathbb{Q})$. The invariant factors determine the rational canonical form of the representative of each similarity class. In the order enumerated above, the following six matrices represent the six similarity classes.

$$\begin{pmatrix} 0 & 0 & 4 & & & \\ 1 & 0 & 0 & & & \\ 0 & 1 & -3 & & & \\ & & & 0 & 0 & 4 \\ & & & 1 & 0 & 0 \\ & & & 0 & 1 & -3 \end{pmatrix}, \begin{pmatrix} 1 & & & & & \\ & 1 & & & & \\ & & 1 & & & \\ & & & 0 & 0 & 4 \\ & & & 1 & 0 & 0 \\ & & & 0 & 1 & -3 \end{pmatrix}, \begin{pmatrix} -2 & & & & & \\ & -2 & & & & \\ & & -2 & & & \\ & & & 0 & 0 & 4 \\ & & & 1 & 0 & 0 \\ & & & 0 & 1 & -3 \end{pmatrix},$$

$$\begin{pmatrix} -2 & & & & & \\ & 0 & -4 & & & \\ & 1 & -4 & & & \\ & & & 0 & 0 & 4 \\ & & & 1 & 0 & 0 \\ & & & 0 & 1 & -3 \end{pmatrix}, \begin{pmatrix} -2 & & & & & \\ & 0 & 2 & & & \\ & 1 & -1 & & & \\ & & & 0 & 0 & 4 \\ & & & 1 & 0 & 0 \\ & & & 0 & 1 & -3 \end{pmatrix}, \begin{pmatrix} 1 & & & & & \\ & 0 & 2 & & & \\ & 1 & -1 & & & \\ & & & 0 & 0 & 4 \\ & & & 1 & 0 & 0 \\ & & & 0 & 1 & -3 \end{pmatrix}.$$

$\blacksquare$

* * * * *

Exercise 7 (DF 12.3.5): Compute the Jordan canonical form (over $\mathbb{C}$) of the matrix

$$A \overset{\text{def}}{=} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -2 \\ 0 & 1 & 3 \end{pmatrix}.$$

Solution. The characteristic polynomial $\det(\lambda I - A)$ is $\lambda^2 - 3\lambda + 2 = (\lambda-2)(\lambda-1)$, so the eigenvalues of A are 2 and 1. We can directly solve the system $A - 2I = 0$ and $A - I = 0$ to find an eigenbasis

$$\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ -2 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ -1 \end{pmatrix}.$$

Therefore these three vectors form a basis of V_A; hence the Jordan canonical form of A is

$$J(A) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}.$$

■

* * * * *

Exercise 8 : Let $R \stackrel{\text{def}}{=} \mathbb{Z}[i]$. Classify all finitely generated R-modules M with the property that $5M = 0$.

Proof. R is a PID, so due to the elementary divisor composition, any finitely generated R-module M is isomorphic to a direct sum of the form:

$$M \cong R/\left(p_1^{k_1}\right) \oplus \ldots \oplus R/\left(p_m^{k_m}\right),$$

where each p_i is a prime element of R. This decomposition is unique in the sense that m is unique and the $p_i^{k_i}$ are unique up to reordering and multiplication by units. Therefore it suffices to classify R-modules M' of the form $R/(p^k)$, where p is a prime element of R such that $5M' = 0$. Since R is a PID, $\mathrm{Ann}(M') = (r_0)$ for some $r_0 \in R$. Since (p^k) is an ideal, (p^k) is contained in $\mathrm{Ann}(M')$, so r_0 divides p^k. That is, r_0 is a power of p. On the other hand $5M' = 0$, so $5 \in \mathrm{Ann}(M') = (r_0)$. This shows that r_0 is a nontrivial power of p. Furthermore, $5 = (2+i)(2-i)$; both of these factors are prime (they are irreducible in a PID). So we have $(2+i)(2-i) = p^d a$, where $0 < d \leqslant k$ and $a \in R$. Thus $d = 1$ and $p = 2+i$ or $p = 2-i$. In other words, $M' \cong R/(2+i)$ or $M' \cong R/(2-i)$.

Returning to the direct sum M, this tells us that M is a direct sum of copies of $M_1 \stackrel{\text{def}}{=} R/(2+i)$ and $M_2 \stackrel{\text{def}}{=} R/(2-i)$. This proves the following classification.

Proposition 8.1. For any finitely generated $\mathbb{Z}[i]$-module M such that $5M = 0$, there exist $d_1, d_2 \in \mathbb{Z}_{\geqslant 0}$ such that

$$M \cong M_1^{d_1} \oplus M_2^{d_2}.$$

■