The last Home-work

Gandhar Kulkarni (mmat2304)

1

1. Since R is a PID, we know that $(a, b) = (d)$, for some $d, a, b \in R$. Then we have $d = am + bn$, for some $m, n \in R$. Now we have a vector $v = [a, b]^T \in R^2 \backslash \{0\}$. Then we show that there exists a $2x2$ matrix that does what we want by constructing one. Let the desired matrix by be given by $X = \begin{pmatrix} x_{11} & x_{21} \\ x_{12} & x_{22} \end{pmatrix}$. Now we have $Xv = [x_{11}a + x_{21}b, x_{12}a + x_{22}b]^T = [d, 0]^T$. Comparing terms, we have $x_{12}a + x_{22}b = 0$. Then we have $x_{12}a = -x_{22}b$, which implies that $x_{12}| - b$, and $x_{22}|a$. It is easy to see that $x_{12} = -a/d$ and $x_{22} = b/d$ does the trick. For $x_{11}a + x_{21}b = d$, see that $x_{11} = m$ and $x_{21} = n$ are good choices, since their linear combination produces d. Thus see that

$$X = \begin{pmatrix} m & n \\ -b/d & a/d \end{pmatrix}$$

is a matrix that achieves the intended result.

2. The above result shall be of much use to us. We see that we want to send a_{11} to d, that is the gcd of a_{11} and a_{i1}, and a_{i1} to 0. Let $m, n \in R$ such that $d = a_{11}m + a_{i1}n$. Define the matrix $\tilde{X} = (x_{kl})$ thus— $x_{11} = m, x_{1i} = n, x_{i1} = -a_{i1}/d, x_{ii} = a_{11}/d$. Also we have $x_{kk} = 1$ if $k \neq 1, i$. All other elements are 0. Then we have $A' = \tilde{X}A = (a'_{kl})$, where $a'_{11} = a_{11}m + a_{i1}n$, $a'_{i1} = (-a_{i1})a_{11} + (a_{11})a_{i1} = 0$, and $a'_{kl} = a_{kl}$ for $k \neq 1, i$. We need to see that this here matrix is invertible. For $\tilde{X}$ a $m \times m$ matrix, we want $\det \tilde{X}$. We expand the determinant along the first row. Then we have $\det \tilde{X} = m \det \tilde{X}[1|1] + (-1)^{i+1}((-1)^{i+1} \det \tilde{X}[1|i])$. $\tilde{X}[1|1]$ is a diagonal matrix with a_{11} on the a_{ii}th entry, and 1 otherwise on the diagonal. Thus $\det \tilde{X}[1|1] = a_{11}$. $\tilde{X}[1|i]$) is a matrix with x_{i1} at the $(i-1, 1)$th entry, with every element below and above it zero. We take the determinant along this column, we have $(-1)^{i-1+1}x_{i1} \cdot \det I_{m-2} = (-1)^i x_{i1}$. Thus see that $\det \tilde{X} = ma_{11} + (-1)^{2i+1}(-a_{i1}) = 1$, means that $\tilde{X}$ is invertible.

3. The above result and the result above that shall be of much use to us. If $A = 0$, then there is nothing to do. We then have $A \neq 0$. Without loss of generality, we take $a_{11} \neq 0$. This is because we can shift the row with a non-zero element to the top, then send the column with that element to the first column. Now using the above result, there is a $\tilde{X}_1$ such that $a_{21} = 0$. The value of a_{11} changes. Now we have $\tilde{X}_2$ that sends a_{31} to 0. We repeat this process till $a_{i1} = 0$ for all $i > 1$. Now we have the first column all zero except for a_{11}. Let $X_1 := \tilde{X}_{i-1} \dots \tilde{X}_1$. Let us denote X_1A by A'. Then consider A'^T. The first row now becomes the first column, and we can do the same thing that we did earlier, to reduce all elements below a_{11} in A'^T to 0. Let that operation be given by the matrix Y_1. Naturally, this matrix is the product of matrices obtained from $j - 1$ operations as given in the previous part. Then we take the transpose of the matrix $Y_1A'^T$ to have

$$A'' = (Y_1A'^T)^T = (Y_1(X_1A)^T)^T = X_1^T A Y_1^T.$$

The matrix we have obtained has no non-zero elements below a_{11} or to its right.

Now note that we can modify our previous result to the second row. Earlier, we reduced all the leading terms of rows other than the first row to zero, then we did the same with columns. Here we reduce the second terms of the ith rows for $i > 2$, then do the same for the columns. We can find a X_2 and Y_2 both invertible such that $X_2A''Y_2$ has all elements of the type a_{2j} and a_{i2} zero, for $i, j \neq 2$. Now we have a matrix where a_{11} and a_{22} may or may not be zero, but all elements sharing the same row or column with them is zero. We continue this process for the entire matrix, which gives us at every stage two invertible matrices that do the above reduction. To be precise, we have $X_1, \ldots, X_t, Y_1, \ldots, Y_t$ where $t = \min(m, n)$. We say $X = X_1 \ldots X_t$, and $Y = Y_t^{-1} \ldots Y_q^{-1}$. Then putting all of these results together, we get $D = XAY^{-1}$.

We do not know a priori if $a_{11}|a_{22}|\ldots|a_{tt}$, but we can ensure this. We first make sure that $a_{11}|a_{22}$, then the general case is easy to see. We execute the elementary column operation $C_1 \mapsto C_1 + C_2$. Now using the previous result we can change a_{11} to $\gcd(a_{11}, a_{22},)$ and a_{21} goes to 0. All other terms remain unchanged. We know that $d|a_{22}$. We repeat this procedure for d_{ii} and $d_{(i+1)(i+1)}$, to get the desired result.

2

3

We have M a $R-$module which has itself as a generating set. Then $\pi : R^{\oplus M} \twoheadrightarrow M$ is the surjective map sending e_m to m. We see that $\pi(e_{rm} - re_m) = \pi(e_{rm}) - r\pi(e_m) = rm - rm = 0$. Also, $\pi(e_{m_1+m_2} - e_{m_1} - e_{m_2}) = \pi(e_{m_1+m_2}) - \pi(e_{m_1}) - \pi(e_{m_2}) = (m_1 + m_2) - m_1 - m_2 = 0$. Therefore we have $e_{rm} - re_m \in \ker \pi$, and $e_{m_1+m_2} - e_{m_1} - e_{m_2} \in \ker \pi$. Thus we have

$$(e_{rm} - re_m, e_{m_1+m_2} - e_{m_1} - e_{m_2}) \subseteq \ker \pi.$$

To see the other inclusion, let there be some $re_m \in \ker \pi$. Then we have $\pi(re_m) = rm = 0$. See that we can write re_m as

$$re_m = -((e_{rm} - re_m) + (e_{0+0} - e_0 - e_0)),$$

as $e_{rm} = e_0$. Thus for any general element $\sum re_m \in \ker \varphi$, we can write the term as a linear combination of terms in $(e_{rm} - re_m, e_{m_1+m_2} - e_{m_1} - e_{m_2})$. Thus

$$(e_{rm} - re_m, e_{m_1+m_2} - e_{m_1} - e_{m_2}) = \ker \pi,$$

as required.

4

1. By the structure theorem for finitely generated modules, we have $N \cong \frac{\mathbb{Z}}{(a_1)} \oplus \cdots \oplus \frac{\mathbb{Z}}{(a_k)} \oplus \mathbb{Z}^d$, where $a_1|a_2|\ldots|a_k$ and N is a finitely generated submodule in $\mathbb{Q}$. Since no element in $\mathbb{Q}$ is a torsion element, we must have $T(N) = \{0\}$. Thus $N \cong \mathbb{Z}^d$. Let $d > 1$, say $d = 2$. Then we have a map $f : \mathbb{Z}^2 \to N$ from $\mathbb{Z}^2$ to N, where $f(1, 0) = \frac{p_1}{q_1}$ and $f(0, 1) = \frac{p_2}{q_2}$, for some $\frac{p_1}{q_1}, \frac{p_2}{q_2} \in \mathbb{Q}$. Then we have $f(q_1p_2, -q_2p_1) = 0$, which contradicts the linear independence of $\mathbb{Z}$. Then $d = 0, 1$, which means N is either zero or a cyclic module.

2. We have N_1, N_2, two non-zero submodules of $\mathbb{Q}$. We have $\frac{p_1}{q_2} \in N_1, \frac{p_2}{q_2} \in N_2$. See that $\frac{p_1}{q_1}(q_1p_2) = \frac{p_2}{q_2}(q_2p_1)$, thus $p_1p_2 \in N_1 \cap N_2$. Thus for any non-zero submodule we can find a non-zero element they have in common.

3. Let $f : \mathbb{Q} \to M \cong \bigoplus_{i=1}^{k} \frac{\mathbb{Z}}{(a_i)} \oplus \mathbb{Z}^d$ be a $\mathbb{Z}-$linear map. By the structure theorem, we can write M as given. Then we have $f(1) = (m_1, \ldots, m_k, n_1, \ldots, n_d)$, where $m_1 \in \frac{\mathbb{Z}}{(a_1)}, \ldots, m_k \in \frac{\mathbb{Z}}{(a_k)}$, and $n_1, \ldots, n_d \in \mathbb{Z}^d$.

5

$R^{\oplus X}$ is a free module, for some indexing set X. M is some submodule of $R^{\oplus X}$. We find a subset $Y \subseteq X$ such that $M \cap R^{\oplus Y}$ is free and B is a basis for this free module. Let (B, Y) be such a pair with the given partial order. $\mathbb{T}$ is the poset of all such submodules in $R^{\oplus X}$.

1. X is non-empty. Then we can pick a singleton subset $\{x\} \subseteq X$. $R^{\oplus Y}$ must be a finitely generated module (hence the free module generated by a singleton must be R), and hence so must $M \cap R$, as this is merely an ideal in R, which is an ideal generated by one element. Thus the ideal is isomorphic to R as a module. Thus $R \cong Ra$, where $(a) = I$. Thus this is an element of $\mathbb{T}$, which means that $\mathbb{T}$, where this above example corresponds to the element $(R, \{1\})$.

6

1. Let $f \in \mathrm{Hom}_{\mathbb{Z}}\left(\frac{\mathbb{Z}}{(n)}, \frac{\mathbb{Q}}{\mathbb{Z}}\right)$. Then we have an abelian group, as $\mathrm{Hom}_{\mathbb{Z}}\left(\frac{\mathbb{Z}}{(n)}, \frac{\mathbb{Q}}{\mathbb{Z}}\right)$ is a $\mathbb{Z}-$module ($\mathbb{Z}-$modules and abelian groups are the same). Elements in $\frac{\mathbb{Q}}{\mathbb{Z}}$ are precisely the elements of $\mathbb{Q}\cap[0,1)$. Then due to the $\mathbb{Z}-$linearity of f, we only need to ask where 1 is sent to. Let us say that $f(1) = \frac{p}{q}$. We see that $n \cdot f(1) = f(n) = f(0) = 0$, thus $n \cdot \frac{p}{q} = 0$. This then means that $\frac{np}{q} \in \mathbb{Z} \implies q|n$. This means that $f(1) = \frac{p}{n}$, for some $p < n$, which means that we have n choices at most. Now note that any map of the form $f_i : \frac{Z}{(n)} \to \frac{\mathbb{Q}}{\mathbb{Z}}$ where $f_i(k) = \frac{ik}{n}$, where $i = 0, 1, \ldots, n-1$ is in $\mathrm{Hom}_{\mathbb{Z}}\left(\frac{\mathbb{Z}}{(n)}, \frac{\mathbb{Q}}{\mathbb{Z}}\right)$, which means that it must have at least n elements. Since the only number that is at least n but is at most n is n, we are done.

2. Since M is a finite $\mathbb{Z}-$module, it is finitely generated, hence it must be of the form $\bigoplus_{i=1}^{k} \frac{\mathbb{Z}}{(a_i)} \oplus \mathbb{Z}^d$, for some $d \geq 0$. Note that since the module is finite, we must have $d = 0$. Then we have $M = \bigoplus_{i=1}^{k} \frac{\mathbb{Z}}{(a_i)}$, where $(a_1) \supseteq (a_2) \supseteq \cdots \supseteq (a_k)$. Let us denote $M_i := \frac{\mathbb{Z}}{(a_i)}$, so we have $M = \bigoplus_{i=1}^{k} M_i$. See that $\mathrm{Hom}_{\mathbb{Z}}\left(M_i, \frac{\mathbb{Q}}{\mathbb{Z}}\right)$ is a cyclic group of order a_i as given in the previous result. Moreover, we know explicitly what those maps are. Also see that in $\mathrm{Hom}_{\mathbb{Z}}\left(M_i, \frac{\mathbb{R}}{\mathbb{Z}}\right)$, the map is determined solely by where 1 is taken to. If it is taken to an irrational number, then this map cannot be a cyclic group, as it will not have a period. Therefore these maps must be rational, and hence we defer to the rational case to see that the module $\mathrm{Hom}_{\mathbb{Z}}\left(M_i, \frac{\mathbb{R}}{\mathbb{Z}}\right)$ must have the same maps as $\mathrm{Hom}_{\mathbb{Z}}\left(M_i, \frac{\mathbb{Q}}{\mathbb{Z}}\right)$, giving us the isomorphism.

   We will state a few facts that will make proving that $M \cong \mathrm{Hom}_{\mathbb{Z}}\left(M, \frac{\mathbb{Q}}{\mathbb{Z}}\right)$ easier. Note that $\mathrm{Hom}_{\mathbb{Z}}\left(M, \frac{\mathbb{Q}}{\mathbb{Z}}\right) \cong \bigoplus_{i=1}^{k} \mathrm{Hom}_{\mathbb{Z}}\left(M_i, \frac{\mathbb{Q}}{\mathbb{Z}}\right)$, and that for modules $M_1, \ldots, M_k$ and $N_1, \ldots, N_k$ where $M_i \cong N_i$ for all $1 \leq i \leq k$, we have $\oplus_{i=1}^{k} M_i \cong \oplus_{i=1}^{k} N_i$. By the universal property of direct sums, we know that the composition of isomorphic maps shall also be an isomorphic map.

   We want to show that $M_i \cong \mathrm{Hom}_{\mathbb{Z}}\left(M_i, \frac{\mathbb{Q}}{\mathbb{Z}}\right)$, the required result should follow directly. We know that $M_i = \{0, 1, \ldots, a_i - 1\}$, and $\mathrm{Hom}_{\mathbb{Z}}\left(M_i, \frac{\mathbb{Q}}{\mathbb{Z}}\right) = \{\varphi_0^i, \ldots, \varphi_{a_i-1}^i\}$, where $\varphi_m^i(1) = \frac{m}{a_i}$. Now define the map $\sigma : M_i \to \mathrm{Hom}_{\mathbb{Z}}\left(M_i, \frac{\mathbb{Q}}{\mathbb{Z}}\right)$, where $\sigma(m_i) = \varphi_{m_i}^i$. Our map is a $\mathbb{Z}-$module homomorphism. We define $\theta : \mathrm{Hom}_{\mathbb{Z}}\left(M_i, \frac{\mathbb{Q}}{\mathbb{Z}}\right) \to M_i$, where $\theta(\varphi_{m_i}^i) = m_i$. Then see that $\sigma \circ \theta = \iota_{\mathrm{Hom}_{\mathbb{Z}}\left(M_i, \frac{\mathbb{Q}}{\mathbb{Z}}\right)}$, and $\theta \circ \sigma = \iota_{M_i}$. Thus we see that $M_i \cong \mathrm{Hom}_{\mathbb{Z}}\left(M_i, \frac{\mathbb{Q}}{\mathbb{Z}}\right)$.

   Since $\mathrm{Hom}_{\mathbb{Z}}\left(M, \frac{\mathbb{Q}}{\mathbb{Z}}\right) \cong \bigoplus_{i=1}^{k} \mathrm{Hom}_{\mathbb{Z}}\left(M_i, \frac{\mathbb{Q}}{\mathbb{Z}}\right)$, we have

$$M \cong \bigoplus_{i=1}^{k} M_i \cong \bigoplus_{i=1}^{k} \mathrm{Hom}_{\mathbb{Z}}\left(M_i, \frac{\mathbb{Q}}{\mathbb{Z}}\right) \cong \mathrm{Hom}_{\mathbb{Z}}\left(M, \frac{\mathbb{Q}}{\mathbb{Z}}\right),$$

   as required.

3. We have the map $\delta : M \to \mathrm{Hom}_R\left(\mathrm{Hom}_R\left(M, N\right), N\right)$ where $\delta(m) = (\varphi \mapsto \varphi(m))$. Let us denote by $f_m \in \mathrm{Hom}_R\left(\mathrm{Hom}_R\left(M, N\right), N\right)$, where $f_m(\varphi) = \varphi(m)$. So $\delta(m) = f_m$. We want to see if δ is a $R-$linear map.

   We will check the behaviour of δ with respect to addition and scalar multiplication. We have $\delta(m+n) = f_{m+n}$, which means that $f_{m+n}(\varphi) = \varphi(m+n) = \varphi(m) + \varphi(n)$. We know that $f_m(\varphi) = \varphi(m)$ and $f_n(\varphi) = \varphi(n)$, so we have $f_{m+n} = f_m + f_n$. Also we know that $\delta(m) = f_m$ and $\delta(n) = f_n$, so putting all this together we have $\delta(m+n) = \delta(m) + \delta(n)$. For scalar multiples, see that $\delta(rm) = f_{rm}$, where $f_{rm}(\varphi) = \varphi(rm) = r\varphi(m)$. See that $f_m(\varphi) = \varphi(m)$, so $r\varphi(m) = rf_m$. We know that $r\delta(m) = rf_m$, which is the required result. Thus we have that δ is a $R-$linear map.

   To see that δ commutes with finite direct sums, we note that since finite direct sums in the first slot and Hom commute, we can see that

$$\mathrm{Hom}_R\left(\mathrm{Hom}_R\left(\oplus_{i=1}^{k} M_i, N\right), N\right) \cong \oplus_{i=1}^{k} \mathrm{Hom}_R\left(\mathrm{Hom}_R\left(M_i, N\right), N\right).$$

   We specify an isomorphism between the two using the terminology defined earlier. For the ease of typing and the eyes of the reader, let

$$H_1 = \mathrm{Hom}_R\left(\mathrm{Hom}_R\left(\oplus_{i=1}^{k} M_i, N\right), N\right),$$

and

$$H_2 = \oplus_{i=1}^k \mathrm{Hom}_R\left(\mathrm{Hom}_R\left(M_i, N\right), N\right).$$

We have $\delta_{\oplus_{i=1}^k M_i} : \oplus_{i=1}^k M_i \to H_1$, where $\delta_{\oplus_{i=1}^k M_i}(m_1, \ldots, m_k) = (\varphi \mapsto \phi(m_1, \ldots, m_k))$. Denote the map on the right by $f_{m_1,\ldots,m_k}$. We have $\delta_{M_i} \to \mathrm{Hom}_R\left(\mathrm{Hom}_R\left(M, N\right), N\right)$, where $\delta_{M_i}(m_i) = (\varphi \mapsto \varphi(m_i))$. We denote the map on the right by $f^i_{m_i}$. We extend this map to H_2, where $\delta|_{M_i} = \delta_{M_i}$. Here, we abuse notation since more accurately δ_{M_i} acts on M_k, while δ acts on $\oplus_{i=1}^k M_i$. This product of maps is denoted by $\oplus_{i=1}^k \delta_{M_i}$.

Now we wish to show that the given diagram in the problem commutes. Define $\psi_1 : H_1 \to H_2$, and $\psi_2 : H_2 \to H_1$, two module maps. We know a map between the two exists such that their composition is the identity maps for H_1 and H_2. Then we have $\psi_1 \circ \delta_{\oplus_{i=1}^k M_i} : \oplus_{i=1}^k M_i \to H_2$, where $\psi_1 \circ \delta_{\oplus_{i=1}^k M_i}(m_1, \ldots, m_k) = \psi_1(f_{(m_1,\ldots,m_k)}) = (f^1_{m_1}, \ldots, f^k_{m_k})$. Similarly, we have the map $\psi_2 \circ \oplus_{i=1}^k \delta_{M_i} : \oplus_{i=1}^k M_i \to H_1$ where $\psi_2 \circ \oplus_{i=1}^k \delta_{M_i}(m_1, \ldots, m_k) = \psi_2(f^1_{m_1}, \ldots, f^k_{m_k}) = f_{(m_1,\ldots,m_k)}$. See that this diagram commutes, which is the desired result.

4. We will use the previous two results liberally to get our result. We know $M \cong \mathrm{Hom}_{\mathbb{Z}}\left(M, \frac{\mathbb{Q}}{\mathbb{Z}}\right)$, Thus $\mathrm{Hom}_{\mathbb{Z}}\left(\mathrm{Hom}_{\mathbb{Z}}\left(M, \frac{\mathbb{Q}}{\mathbb{Z}}\right), \frac{\mathbb{Q}}{\mathbb{Z}}\right) \cong \mathrm{Hom}_{\mathbb{Z}}\left(M, \frac{\mathbb{Q}}{\mathbb{Z}}\right) \cong M$. Now we need to check that $\delta_{\oplus_{i=1}^k M_i}$ is an isomorphism. Previously we established a correspondence between the elements of each M_i with its Hom module, we extend it to all of M. A general element of M is $(m_1, \ldots, m_k)$, and a general map from M to $\frac{\mathbb{Q}}{\mathbb{Z}}$ is $(\phi^1_{m_1}, \ldots, \phi^k_{m_k})$, where $\phi^i_{m_i} : M_i \to \frac{\mathbb{Q}}{\mathbb{Z}}$ is the map where $\phi^i_{m_i}(1) = \frac{m_i}{a_i}$.

   Now see that $\delta_{\oplus_{i=1}^k M_i}(m_1, \ldots, m_k) = f_{m_1,\ldots,m_k}$. This map takes any map in $\mathrm{Hom}_{\mathbb{Z}}\left(M, \frac{\mathbb{Q}}{\mathbb{Z}}\right)$ and sends it to that map evaluated at $(m_1, \ldots, m_k)$. That is, $\delta_{\oplus_{i=1}^k M_i}(m_1, \ldots, m_k) = (f_{m_1}, \ldots, f_{m_k})$, which is the map where each component sends any map in $\mathrm{Hom}_{\mathbb{Z}}\left(M_i, \frac{\mathbb{Q}}{\mathbb{Z}}\right)$ to that map evaluated at m_i, for $i = 1, \ldots, k$. We wish to have a map from $\mathrm{Hom}_{\mathbb{Z}}\left(\mathrm{Hom}_{\mathbb{Z}}\left(M, \frac{\mathbb{Q}}{\mathbb{Z}}\right), \frac{\mathbb{Q}}{\mathbb{Z}}\right)$ to M, such that their composition is the identity map. Any element of $\mathrm{Hom}_{\mathbb{Z}}\left(M_i, \frac{\mathbb{Q}}{\mathbb{Z}}\right)$ is of the form ϕ^i_ℓ, where $\ell = 0, 1, \ldots, a_i - 1$. As mentioned before, it can be mapped to $\ell \in M_i$. Then we specify a map from M_i to $\frac{\mathbb{Q}}{\mathbb{Z}}$, which sends ℓ to $\phi^i(\ell)$. Thus any element of $\mathrm{Hom}_{\mathbb{Z}}\left(\mathrm{Hom}_{\mathbb{Z}}\left(M, \frac{\mathbb{Q}}{\mathbb{Z}}\right), \frac{\mathbb{Q}}{\mathbb{Z}}\right)$ can be represented by $(\phi^1_{\ell_1}, \ldots, \phi^k_{\ell_k})$. We naturally see that we can send this to $(\ell_1, \ldots, \ell_k) \in M$, which is the required inverse map.