MATH 7752 Homework 5

James Harbour

February 25, 2022

Problem 1

Let $F = \mathbb{Z}^3$ be the free $\mathbb{Z}$-module of rank 3. Let N be the submodule of F generated by $v_1 = (1, 2, 3), (5, 4, 6)$, and $(7, 8, 9)$.

(1) Find compatible bases for F and N, that is, bases satisfying the submodule theorem 1.

Proof.

$$\begin{bmatrix} 1 & 2 & 3 \\ 5 & 4 & 6 \\ 7 & 8 & 9 \end{bmatrix} \xrightarrow{\mathcal{E}_{21}(-5), \mathcal{E}_{31}(-7)} \begin{bmatrix} 1 & 2 & 3 \\ 0 & -6 & -9 \\ 0 & -6 & -12 \end{bmatrix} \xrightarrow{\mathcal{E}'_{21}(-2), \mathcal{E}'_{31}(-3)} \begin{bmatrix} 1 & 0 & 0 \\ 0 & -6 & -9 \\ 0 & -6 & -12 \end{bmatrix} \xrightarrow{\mathcal{E}_{32}(-1)} \begin{bmatrix} 1 & 0 & 0 \\ 0 & -6 & -9 \\ 0 & 0 & -3 \end{bmatrix} \xrightarrow{\mathcal{E}_{23}(-3)} \begin{bmatrix} 1 & 0 & 0 \\ 0 & -6 & 0 \\ 0 & 0 & -3 \end{bmatrix}$$

Then the desired matrix B has the form

$$B = E_{12}(-2)^{-1} E_{13}(-3)^{-1} = E_{12}(2) E_{13}(3) = \begin{bmatrix} 1 & 2 & 3 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

so our new basis $\{y_1, y_2, y_3\}$ of F is given by

$$\begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} e_1 \\ e_2 \\ e_3 \end{bmatrix}$$

and our new basis of N is $\{y_1, -6y_2, -3y_3\}$. □

(2) Describe the quotient F/N in the IF form.

Proof. The quotient is given by

$$F/N \cong (y_1\mathbb{Z} \oplus y_2\mathbb{Z} \oplus y_3\mathbb{Z})/(y_1\mathbb{Z} \oplus -6y_2\mathbb{Z} \oplus -3\mathbb{Z}) \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$$

□

(3) Describe in IF form the abelian group given by the presentation

$$\langle a, b, c \mid a + 2b + 3c = 0, 5a + 4b + 6c = 0, 7a + 8b + 9c = 0 \rangle.$$

Proof. By definition,

$$\langle a, b, c \mid a + 2b + 3c = 0, 5a + 4b + 6c = 0, 7a + 8b + 9c = 0 \rangle = F/N$$

as above, and F/N has IF form $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$. □

Problem 2

Let R be a PID. For an R-module M define $\mathrm{rk}(M)$ to be the minimal size of a generating set of M.
(a) Let M be a finitely generated R-module and $R/a_1R \oplus \cdots \oplus R/a_mR \oplus R^s$ be its invariant factor decomposition. That is, $s \geq 0$ and the elements $a_1, \ldots, a_m$ are non-zero, non-units such that $a_1|a_2|\cdots|a_m$. Prove that $\mathrm{rk}(M) = m + s$. **Warning:** It is not true in general that $\mathrm{rk}(P \oplus Q) = \mathrm{rk}(P) \oplus \mathrm{rk}(Q)$.

Proof. As M has a generating set of size $m + s$, we have that $n = rk(M) \leq m + s$. Then there exists a surjective R-module homomorphism $\varphi : R^n \to M$ such that $\varphi(e_i) = x_i$. Letting $K := \ker(\varphi)$, as $\{e_1, \ldots, e_n\}$ is a basis for R^n, there exist nonzero $b_1, \ldots, b_k \in R$ with $k \leq n$ and $b_1|\cdots|b_k$ such that $\{b_1e_1, \ldots, b_ne_n\}$ is a basis for K. Suppose that $1 \leq l \leq k$ is such that $b_1 \cdots b_l$ are units and $b_{l+1}, \ldots, b_k$ are non-units. Then

$$\begin{aligned} M &\cong \left(\bigoplus_{i=1}^{n} e_iR\right) \Big/ \left(\bigoplus_{i=1}^{k} b_ie_iR\right) \cong R/b_1R \oplus \cdots \oplus R/b_kR \oplus R^{n-k} \\ &\cong R/b_{l+1}R \oplus \cdots \oplus R/b_kR \oplus R^{n-k} \end{aligned}$$

which is in invariant factor form, so $n - k = s$ and $k - l = m$, so

$$n = k + s = l + m + s \geq m + s$$

and thus $rk(M) = m + s$. □

(b): Let F be a free R-module of rank n with basis $e_1, \ldots e_n$. Let N be the submodule of F generated by some elements $v_1, \ldots, v_n \in F$. Let $A \in Mat_n(R)$ be the matrix such that

$$\begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} = A \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix}.$$

Find a simple condition on the entries of A which holds if and only if $\mathrm{rk}(F/N) = n$.

Proof. If any entry in A is a unit, then we could apply row and column operations alongside flips to have the element appear in smith normal form, whence $\mathrm{rk}(F/N) \leq n - 1 < n$, so we must first have that all entries of the matrix are nonunits.

We claim that the simple condition on A is that every entry of A is divisible by some nonunit $a \in R$.

$\underline{\Longrightarrow}$: Write $A = CDB$ where D is the SNF of A and $B, C \in \mathrm{GL}_n(R)$. Then $D = C^{-1}AB^{-1}$, so each nonzero element in the SNF of A is a linear combination of elements of A, and is thus divisible by a. Hence, each nonzero element of the SNF is a nonunit, so by part (a), the rank of F/N is $m + (n - m) = n$.

$\underline{\Longleftarrow}$: Suppose that $\mathrm{rk}(F/N) = n$. Then by the above comment, every entry of A is a nonunit. As before, write $A = CDB$ where D is the SNF of A. Let $a_1 \in R$ be the first nonzero entry of D. Then a_1 divides every entry in D, and every entry of A is a linear combination of entries of D and are thus divisible by a_1. If a_1 were a unit, then part (a) would imply that $rk(F/N) \neq n$, so it follows that a_1 is a nonunit that divides every entry of A. □

Problem 3

In this problem R will be a commutative domain. An R-module P is called *projective* if it is a direct summand of a free R-module. That is, if there exist a free R-module F and a submodule Q of F such that $F = P \oplus Q$.

(1) Let P, M, N be R-modules and suppose $f : M \to N$ is a surjective R-module homomorphism. The map f induces a homomorphism of R-modules,

$$\begin{aligned} f_\star : \quad & \mathrm{Hom}_R(P, M) \to \mathrm{Hom}_R(P, N) \\ & [\varphi : P \to M] \mapsto [f \circ \varphi : P \to N]. \end{aligned}$$

Prove that if P is finitely generated and projective, then $f_\star$ is surjective.
Hint: The universal property of free R-modules will be useful.

Proof. We first show that such $f_\star$ is surjective when $P = F$ is a free R-module. Suppose that $\varphi \in \mathrm{Hom}_R(F, N)$. Let F be free over some subset $X \subseteq F$. By surjectivity of f, for all $x \in X$, there exists an $m_x \in M$ such that $f(m_x) = \varphi(x)$. Then, by the universal property of free modules, there exists a unique $\psi \in \mathrm{Hom}_R(P, M)$ such that $\psi(x) = m_x$ for all $x \in X$. It follows then that, for $x \in X$,

$$f(\psi(x)) = f(m_x) = \varphi(x)$$

whence by linearity $f_\star(\psi) = f \circ \psi = \varphi$.

Now we treat the general case. Let P be a finitely generated projective R-module. Then by definition there exists a free module F and a submodule $Q \subseteq F$ such that $F = P \oplus Q$. Take $\pi : F \to P$ to be the natural projection and $\iota : P \to F$ the natural inclusion. Then, appealing to the previous case, there exists an R-module homomorphism $\psi : F \to M$ such that $f \circ \psi = \varphi \circ \pi$. Deine a new $\widetilde{\psi} \in \mathrm{Hom}_R(P, M)$ by $\widetilde{\psi} := \psi \circ \iota$. Now, for $p \in P$, we have that

$$(f \circ \widetilde{\psi})(p) = (f \circ \psi)((p, 0))) = (\varphi \circ \pi)((p, 0)) = \varphi(p)$$

so $\varphi = f \circ \widetilde{\psi} = f_\star(\widetilde{\psi})$. $\square$

(2) Show that if R is a PID and P is finitely generated, then P is projective if and only if P is free.

Proof.
The reverse direction follows from the fact that $P = P \oplus 0$, so it suffices to show the forward direction. Let P be a finitely generated projective module. Then there exists a surjective R-module homomorphism $f : R^n \to P$ for some $n \in \mathbb{N}$. Consider the identity map $1_P \in \mathrm{Hom}_R(P, P)$. By part (1), there exists a $\psi \in \mathrm{Hom}_R(P, R^n)$ such that $f \circ \psi = f_\star(\psi) = 1_P$. Then $\psi(P)$ is a submodule of a finitely generated free module and is thus free (as R is a PID). Moreover, as ψ has a left inverse, it is injective whence $P \cong \psi(P)$ is free. $\square$

Problem 4

Determine the number of possible RCF's of 8×8 matrices A over $\mathbb{Q}$ with $\chi_A(x) = x^8 - x^4$. Explain your argument in detail.

Proof. The IF decomposition for V_A is of the form

$$V_A \cong \frac{\mathbb{Q}[x]}{(\alpha_1(x))} \oplus \cdots \oplus \frac{\mathbb{Q}[x]}{(\alpha_m(x))}$$

where $\alpha_1|\alpha_2|\cdots\alpha_m$ are all monic polynomials in $\mathbb{Q}[x]$

We first factor the desired χ_A into irreducibles over $\mathbb{Q}$, i.e. $x^8 - x^4 = x^4(x^2+1)(x+1)(x-1)$. We require that $\alpha_m(x) = \mu_A(x)$, $\alpha_1(x)\cdots\alpha_m(x) = \chi_A(x) = x^4(x^2+1)(x+1)(x-1)$, and $\sum_i \deg(\alpha_i) = 8$.

First observe that, if any of the $x, (x^2+1)$, $(x+1)$, or $(x-1)$ are missing from $\mu_A(x)$, then it would be impossible to have $\alpha_1(x)\cdots\alpha_m(x) = \chi_A(x)$. Thus, $\mu_A(x) = x^k(x^2+1)(x+1)(x-1)$ for some $k \in \{1, \dots, 4\}$. Moreover, if any of the α_i for $i < m$ contain a factor of (x^2+1), $(x+1)$, or $(x-1)$, then we would again violate $\alpha_1(x)\cdots\alpha_m(x) = \chi_A(x)$. Thus, every α_i must be a unit or a power of x.

k=1: In this case, we are forced to take $m = 4$ and $\alpha_i = x$ for $1 \le i < 4$ as this is the only way to partition 8 with one 4 and remaining ones.

k=2: In this case, we either have $m = 2$ and $\alpha_1 = x^2$, or $m = 3$ and $\alpha_1, \alpha_2 = x$. These are the only possible partitions of 8 given the restrictions.

k=3: In this case, we are forced to take $m = 2$ and $\alpha_1 = x$, this is clearly the only allowed partition.

k=4: In this case, take $m = 1$ and $\alpha_1 = \mu_A(x) = \chi_A(x)$.

$\square$