Peize Liu
St. Peter's College
University of Oxford

Problem Sheet 4

A3: Rings and Modules

April 15, 2020

Question 1

Give examples of the following.

(i) A free module over a PID and a linearly independent subset that cannot be extended to a basis.

(ii) A free module over a PID and a minimal generating subset that is not a basis.

(iii) A free module over a PID and a proper submodule of the same rank.

Proof.

1. $\mathbb{Z}$ itself is a $\mathbb{Z}$-module. It is a free module of rank 1. Consider $\{2\} \subseteq \mathbb{Z}$. Clearly $\{2\}$ is linearly independent because $\mathbb{Z}$ is an integral domain. $\{2\}$ is not a basis of $\mathbb{Z}$ because it cannot generate $1 \in \mathbb{Z}$. Suppose that it can be extended to a basis B. Pick $n \in B$ such that $n \neq 2$. We have $2 \cdot n + (-n) \cdot 2 = 0$, contradicting that B is linearly independent.
2. Again we consider $\mathbb{Z}$ as a $\mathbb{Z}$-module. $\{2, 3\} \subseteq \mathbb{Z}$ is a minimal generating set because $1 = 1 \cdot 3 + (-1) \cdot 2$, and $\{2\}, \{3\}$ cannot generate $\mathbb{Z}$. $\{2, 3\}$ is linearly dependent as $0 = 2 \cdot 3 + (-3) \cdot 2$, so it is not a basis.
3. Once more we consider $\mathbb{Z}$ as a $\mathbb{Z}$-module. It is a free module of rank 1. $2\mathbb{Z}$ is a proper submodule of $\mathbb{Z}$ of rank 1 as $\{2\}$ is a basis of it.

□

Question 2

Both the conclusions below from the Structure Theorem in the lectures notes. The point of this question is to see how the proof simplifies in each case.

(i) Suppose that R is a PID and M is a finitely generated $R-$module such that $\mathrm{Ann}_R(x) = \{0\}$ for all $x \neq 0_M$, Show that M is free.

(ii) Suppose that G is a finitely generated Abelian group. Show that G is isomorphic to a direct sum of cyclic groups.

Proof. We begin our proof with stating a general theorem.

Theorem 1

If R is a PID and M is a finitely generated free R-module, then any submodule N of M is also free and finitely generated.

Instead of proving the theorem, we shall prove a stronger lemma:

Lemma 2

Suppose that R is a PID and M is a free R-modules with basis $\{v_1, ..., v_n\}$. Let N be a submodule of M. Then there exists $a_1, ..., a_m \in R$ ($m \leqslant n$) such that $\{a_1 v_1, ..., a_m v_m\}$ is a basis of N and $a_1 \mid \cdots \mid a_m$.

Proof of Lemma 2. We use induction on the rank n.

Base case: If $n = 0$, then both M and N are the zero module. The result holds trivially.

Induction case: Suppose the result holds for $\mathrm{rank}\, M < n$. For $\mathrm{rank}\, M = n$: we consider the family of submodules of R:

$$\{\varphi(N) \lhd R : \varphi \in \mathrm{Hom}_R(M, R)\}$$

Since R is a PID, it is Noetherian. The family has a maximal element $\rho(N)$. Suppose that it is generated by a_1. There exists $w_1 \in N$ such that $\rho(w_1) = a_1$. We claim that a_1 divides $\varphi(w_1)$ for all $\varphi \in \mathrm{Hom}_R(M, R)$.

$\langle a_1, \varphi(w_1)\rangle$ is a principal ideal in R. Let b be a generator of it and $b = ra_1 + s\varphi(w_1)$ for some $r, s \in R$. Consider $\psi := r\rho + s\varphi \in \mathrm{Hom}_R(M, R)$. Since $a_1 \in \langle b\rangle$, $\rho(N) = \langle a_1\rangle \subseteq \langle b\rangle$. On the other hand, $\psi(w_1) = b \in \psi(N) \implies \langle b\rangle \subseteq \psi(N) \subseteq \rho(N) = \langle a_1\rangle$ by maximality of $\rho(N)$. Hence $\langle a_1\rangle = \langle b\rangle$ and in particular a_1 divides $\varphi(w_1)$.

Since M is free, there is an isomorphism $\sigma : M \to R^n$. Let $\sigma(w_1) = (r_1, ..., r_n) \in R^n$. Let $\pi_i : R^n \twoheadrightarrow R$ be the projection onto the i-th coordinate. Since $\pi_i \circ \sigma \in \mathrm{Hom}_R(M, R)$, $a_1 \mid \pi \circ \sigma(w_1)$. There exists $s_1, ..., s_n \in R$ such that $r_i = a_1 s_i$. Let $v_1 := \sigma^{-1}(s_1, ..., s_n) \in M$ so that $w_1 = a_1 v_1$.

Note that $a_1 = \rho(w_1) = \rho(a_1 v_1) = a_1\rho(v_1)$. As $a_1 \neq 0$, $\rho(v_1) = 1$. Let $M' := \ker\rho$ and $N' = N \cap M'$. Clearly $N' \subseteq N$ and $N' \subseteq M' \subseteq M$. We claim that $M = \langle v_1\rangle \oplus M'$ and $N = \langle w_1\rangle \oplus N'$.

For $m \in M$, $m = \rho(m)v_1 + (m - \rho(m)v_1)$. Note that

$$\rho(m - \rho(m)v_1) = \rho(m) - \rho(m)\rho(v_1) = 0$$

Therefore $m - \rho(m)v_1 \in \ker\rho$. We have $M = \langle v_1\rangle + \ker\rho$. On the other hand, for $m \in \langle v_1\rangle \cap \ker\rho$, $m = rv_1$ for some $r \in R$. $0 = \rho(rv_1) = r\rho(v_1) = r \implies m = 0$. Hence $\langle v_1\rangle \cap \ker\rho = \{0\}$. Hence $M = \langle v_1\rangle \oplus \ker\rho$ as claimed.

For $m \in N$, as $\langle a_1\rangle = \rho(N)$, $a_1 \mid \rho(m)$. Let $\rho(m) = a_1 c$ for some $c \in R$. Write

$$m = \rho(m)v_1 + (m - \rho(m)v_1) = a_1 c v_1 + (m - a_1 c_1 v_1) = cw_1 + (m - cw_1).$$

Note that $\rho(m - cw_1) = \rho(m) - c\rho(w_1) = a_1 c - a_1 c = 0$. Therefore $m - cw_1 \in \ker\rho \cap N$ and $N = \langle w_1\rangle + N'$. The direct sum part is analgous to above. We have proven the claim.

We have $\mathrm{rank}\, M' < n$. By induction hypothesis, let $\{v_2, ..., v_n\}$ be a basis of M' and $a_2 v_2, ..., a_m v_m$ be a basis of N', where $a_2 \mid \cdots \mid a_n$. Then $\{v_1, ..., v_n\}$ is a basis of M and $\{a_1 v_1, ..., a_m v_m\}$ is a basis of N.

Finally, we shall conclude the proof by showing that $a_1 \mid a_2$. (This part is not used in the question but I mention it for completeness.) Consider any mapping $f : \{v_1, ..., v_n\} \to R$ such that $f(v_1) = f(v_2) = 1$. By universal property of free modules, it lifts to $\varphi \in \mathrm{Hom}_R(M, R)$ such that $\varphi(v_1) = \varphi(v_2) = 1$. Since $\varphi(a_1 v_1) = a_1$, $\langle a_1\rangle \subseteq \varphi(N)$. By maximality of $\langle a_1\rangle$ we have $\langle a_1\rangle = \varphi(N)$. But then $\varphi(a_2 v_2) = a_2 \in \varphi(N) = \langle a_1\rangle$. Hence $a_1 \mid a_2$. □

Theorem 1 follows from Lemma 2 immediately.

Proof of (1). If $M = \{0\}$ then it is trivially a free module. Suppose that $M \neq \{0\}$.

Let $x_1, ..., x_n$ generates M. Since M is torsion-free, $\{x_i\}$ is linearly independent for each $i \in \{1, ..., n\}$. As $\{x_1, ..., x_n\}$ is finite, it contains a maximal linearly independent subset $\{x_1, ..., x_r\}$. Then for each $r < j \leqslant m$, there exists a non-trivial relation:

$$b_1 x_1 + \cdots + b_r x_r + a_j x_j = 0$$

where $b_1, ..., b_r, a_j \in R$ and $a_j \neq 0$ by maximality.

Let $\{x_1, ..., x_r\}$ generates a submodule N of M, which is free by definition. Notice that $a_{r+1} \cdots a_m x_i \in N$ for $i \in \{1, ..., n\}$, as $a_j x_j \in \langle x_1, ..., x_m\rangle$ for $r < j \leqslant m$ via the above relation. Hence $x \mapsto a_{r+1} \cdots a_n x$ defines a R-module homomorphism $\varphi : M \to N$. It is injective because $a_{r+1} \cdots a_n \neq 0$ and M is torsion-free. By First Isomorphism Theorem, $M \cong \mathrm{im}\,\varphi \subseteq N$. Since $\mathrm{im}\,\varphi$ is a submodule of the free module N, by Theorem 1 it is free. Hence M is a free module. □

Proof of (2). G is a finitely generated $\mathbb{Z}$-module and $\mathbb{Z}$ is a PID. There exists an epimorphism $\pi : \mathbb{Z}^n \twoheadrightarrow G$ for some $n \in \mathbb{N}$. By First Isomorphism Theorem, $G \cong \mathbb{Z}^n / \ker\pi$. We apply Lemma 2 to $\ker\pi$: there exists a basis $\{v_1, ..., v_n\}$ of $\mathbb{Z}^n$ and a basis $\{a_1 v_1, ..., a_m v_m\}$ of $\ker\pi$ for some $a_1, ..., a_m \in R\backslash\{0\}$. In order words, $\ker\pi \cong a_1\mathbb{Z} \oplus \cdots \oplus a_m\mathbb{Z}$. Hence:

$$G = \frac{\mathbb{Z}^n}{\ker\pi} \cong \frac{\mathbb{Z}^n}{a_1\mathbb{Z} \oplus \cdots \oplus a_m\mathbb{Z}} \cong \frac{\mathbb{Z}}{a_1\mathbb{Z}} \oplus \cdots \oplus \frac{\mathbb{Z}}{a_m\mathbb{Z}} \oplus \mathbb{Z}^{n-m}$$

G is the direct sum of some cyclic groups. □

□

Question 3

Suppose that R is a commutative ring with identity. Show that if every submodule of R (considered as a left $R-$module) is free then R is PID.

Proof. We know that $I \subseteq R$ is a submodule of R if and only if it is an ideal of R. Suppose that I is an ideal. Since it is a free module, it has a basis B. B is linearly independent. It cannot have more than one element, because for any $b_1, b_2 \in B$, $0 = b_1 \cdot b_2 + (-b_1) \cdot b_2$. Hence I is generated by a single element (both as a submodule and as an ideal). R is a PID. □

Question 4

Suppose that $M = \mathbb{C}^3$ is the left $\mathbb{C}[x]-$module endowed with scalar multiplication $\mathbb{C}[x] \to \mathrm{End}(M)$; $p \mapsto (M \to M, v \mapsto p(A)v)$ where

$$A = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

(i) Show that M is cyclic.

(ii) Show that M is isomorphic to the direct sum of three submodules.

(iii) Is M isomorphic to $\mathbb{C}[A]$ as a $\mathbb{C}[x]-$module?

(iv) How do your answers above change if we replace $\mathbb{C}$ by $\mathbb{R}$? with $\mathbb{F}_7$?

Proof. (i) We shall obtain the invariant factors of A by putting $xI - A$ into Smith normal form. Since $\mathbb{C}$ is a field, $\mathbb{C}[x]$ is a Euclidean domain and we can do this by a sequence of elementary operations:

$$xI - A = \begin{pmatrix} x & 0 & -1 \\ -1 & x & 0 \\ 0 & -1 & x \end{pmatrix} \sim \begin{pmatrix} -1 & x & 0 \\ 0 & -1 & x \\ x & 0 & -1 \end{pmatrix} \sim \begin{pmatrix} -1 & x & 0 \\ 0 & -1 & x \\ 0 & x^2 & -1 \end{pmatrix}$$
$$\sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & x \\ 0 & x^2 & -1 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & x \\ 0 & 0 & x^3 - 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & x^3 - 1 \end{pmatrix}$$

Hence the A has the unique invariant factor $x^3 - 1$. By applying to the $\mathbb{C}[x]$-module Structure Theorem $\mathbb{C}^3$, we obtain $\mathbb{C}^3 = \mathbb{C}[x]/\langle x^3 - 1 \rangle$. In particular $\mathbb{C}^3$ is a cyclic $\mathbb{C}[x]$-module.

(ii) $x^3 - 1 = (x-1)(x-\omega)(x-\omega^2)$ splits over $\mathbb{C}[x]$, where $\omega = \dfrac{-1+\sqrt{3}\mathrm{i}}{2}$. By Chinese Remainder Theorem:

$$\mathbb{C}^3 \cong \frac{\mathbb{C}[x]}{\langle x^3 - 1 \rangle} \cong \frac{\mathbb{C}[x]}{\langle x - 1 \rangle} \oplus \frac{\mathbb{C}[x]}{\langle x - \omega \rangle} \oplus \frac{\mathbb{C}[x]}{\langle x - \omega^2 \rangle}$$

(iii) By universal property of the polynomial ring $\mathbb{C}[x]$, the evaluation $x \mapsto A$ induces the epimorphism $\sigma : \mathbb{C}[x] \to \mathbb{C}[A]$ with kernel $\ker \sigma = \langle m_A(x) \rangle$. The minimal polynomial m_A is the largest invariant factor $x^3 - 1$. By First Isomorphism Theorem for rings, $\mathbb{C}[A] \cong \mathbb{C}[x]/\langle x^3 - 1 \rangle$. This is also an isomorphism of $\mathbb{C}[x]$-modules. By part (i) we see that $\mathbb{C}[A] \cong \mathbb{C}^3$ as $\mathbb{C}[x]$-modules.

(iv) The Smith normal form of the matrix is the same regardless of the base field, so the results in part (i) and (iii) will be unchanged. For part (ii), $x^3 - 1$ has different factorizations on different polynomial rings.

On $\mathbb{R}[x]$, $x^3-1=(x-1)(x^2+x+1)$. Hence $\mathbb{R}^3 \cong \dfrac{\mathbb{R}[x]}{\langle x-1\rangle} \oplus \dfrac{\mathbb{R}[x]}{\langle x^2+x+1\rangle}$.

On $\mathbb{F}_7[x]$, $x^3-1=(x-1)(x^2+x+1)=(x-1)(x^2+x-6)=(x-1)(x-2)(x+3)=(x-1)(x-2)(x-4)$.
Hence $\mathbb{F}_7^3 \cong \dfrac{\mathbb{F}_7[x]}{\langle x-1\rangle} \oplus \dfrac{\mathbb{F}_7[x]}{\langle x-2\rangle} \oplus \dfrac{\mathbb{F}_7[x]}{\langle x-4\rangle}$. □

Question 5

Let G be the Abelian group with generators a, b, and c and relations $2a-16b-8c=0$ and $4a+24b+8c=0$. Find $s, r \in \mathbb{N}$, natural numbers $d_r \mid \cdots \mid d_1$, and an isomorphism $G \to (\mathbb{Z}/d_r\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/d_1\mathbb{Z}) \oplus \mathbb{Z}^s$.

Proof. Consider G as a $\mathbb{Z}$-module. It is finitely presented as suggested by the question. Hence there exists an exact sequence:

$$\mathbb{Z}^2 \xrightarrow{\varphi} \mathbb{Z}^3 \xrightarrow{\pi} G \longrightarrow 0$$

where $G \cong G/\ker\pi = G/\operatorname{im}\varphi = \operatorname{coker}\varphi$. φ sends the generators of $\mathbb{Z}^2$ to $(2,-16,-8),(4,24,8) \in \mathbb{Z}^3$, which correspond to the relations in G. Therefore it has a matrix representation:

$$\varphi = \begin{pmatrix} 2 & 4 \\ -16 & 24 \\ -8 & 8 \end{pmatrix}$$

We can use a sequence of elementary operations to transform it into Smith normal form:

$$\left(\begin{array}{cc|c} 2 & 4 & a \\ -16 & 24 & b \\ -8 & 8 & c \end{array}\right) \sim \left(\begin{array}{cc|c} 2 & 0 & a \\ -16 & 56 & b \\ -8 & 24 & c \end{array}\right) \sim \left(\begin{array}{cc|c} 2 & 0 & a \\ 0 & 8 & b \\ -8 & 24 & 2b+c \end{array}\right) \sim \left(\begin{array}{cc|c} 2 & 0 & a-8b-4c \\ 0 & 8 & 7b+3c \\ 0 & 0 & 2b+c \end{array}\right)$$

Hence $\operatorname{im}\varphi = \langle (2,0,0),(0,8,0)\rangle \cong 2\mathbb{Z} \oplus 8\mathbb{Z}$ and $G \cong \dfrac{\mathbb{Z}^3}{2\mathbb{Z}\oplus 8\mathbb{Z}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}$.
The isomorphism $G \to \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}$ is given by

$$a-8b-4c \mapsto (1,0,0) \qquad 7b+3c \mapsto (0,1,0) \qquad 2b+c \mapsto (0,0,1)$$

or

$$a \mapsto (1,0,4) \qquad b \mapsto (0,1,-3) \qquad c \mapsto (0,-2,7)$$ □

Question 6

(i) Show that the matrix A below has characteristic polynomial $(x-1)^4$ and minimal polynomial $(x-1)^2$.

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

(ii) What are the possible rational canonical forms of a matrix with characteristic polynomial $(x-1)^4$ and minimal polynomial $(x-1)^2$? Which one of these is A?

(iii) Derive the rational canonical form of A by putting the matrix $xI-A$ into Smith normal form.

(iv) What is the Jordan normal form of A?

Proof. (i) We use a sequence of elementary operations to put $xI - A$ into Smith normal form:

$$xI - A = \begin{pmatrix} x-1 & -1 & 0 & 0 \\ 0 & x-1 & 0 & 0 \\ -2 & -3 & x+1 & -4 \\ -1 & -1 & 1 & x-3 \end{pmatrix} \sim \begin{pmatrix} -1 & x-1 & 0 & 0 \\ x-1 & 0 & 0 & 0 \\ -3 & -2 & x+1 & -4 \\ -1 & -1 & 1 & x-3 \end{pmatrix} \sim \begin{pmatrix} -1 & x-1 & 0 & 0 \\ 0 & (x-1)^2 & 0 & 0 \\ 0 & -3x+1 & x+1 & -4 \\ 0 & -x & 1 & x-3 \end{pmatrix}$$
$$\sim \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -x & 1 & x-3 \\ 0 & -3x+1 & x+1 & -4 \\ 0 & (x-1)^2 & 0 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -x & 1 & x-3 \\ 0 & 1 & x-2 & -3x+5 \\ 0 & (x-1)^2 & 0 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & x-2 & -3x+5 \\ 0 & -x & 1 & x-3 \\ 0 & (x-1)^2 & 0 & 0 \end{pmatrix}$$
$$\sim \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & x-2 & -3x+5 \\ 0 & 0 & x^2-2x+1 & -3x^2+6x-3 \\ 0 & 0 & -(x-2)(x-1)^2 & (3x-5)(x-1)^2 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & (x-1)^2 & 0 \\ 0 & 0 & -(x-2)(x-1)^2 & 3(x-1)^2 \end{pmatrix}$$
$$\sim \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & (x-1)^2 & 0 \\ 0 & 0 & 0 & (x-1)^2 \end{pmatrix}$$

We see that the invariant factors of A are $f_1(x) = (x-1)^2$ and $f_2(x) = (x-1)^2$. Hence the minimal polynomial is $m_A(x) = f_2(x) = (x-1)^2$ anf the characteristic polynomial is $\chi_A(x) = f_1(x)f_2(x) = (x-1)^4$.

(ii) Given the minimal polynomial and the characteristic polynomial, the possible Smith normal forms are:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & (x-1)^2 & 0 \\ 0 & 0 & 0 & (x-1)^2 \end{pmatrix} \qquad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & x-1 & 0 & 0 \\ 0 & 0 & x-1 & 0 \\ 0 & 0 & 0 & (x-1)^2 \end{pmatrix}$$

The first one is equivalent to A, as we have shown in part (i).

(iii) The companion matrix corresponding to $(x-1)^2 = x^2 - 2x + 1$ is given by

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

Hence A has rational canonical form:

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

(iv) The Jordan block corresponding to $(x-1)^2 = x^2 - 2x + 1$ is given by

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

Hence A has rational canonical form:

$$\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

□