Problem Set 6

Due Monday, March 2

Instructions: You are encouraged to work together on these problems, but each student should hand in their own final draft, written in a way that indicates their individual understanding of the solutions. Never submit something for grading that you do not completely understand. You cannot use any resources besides me, your classmates, and our course notes.

I will post the .tex code for these problems for you to use if you wish to type your homework. If you prefer not to type, please *write neatly.* As a matter of good proof writing style, please use complete sentences and correct grammar. You may use any result stated or proven in class or in a homework problem, provided you reference it appropriately by either stating the result or stating its name (e.g. the definition of ring or Lagrange's Theorem). Please do not refer to theorems by their number in the course notes, as that can change.

Problem 1. Consider the matrix

$$A = \begin{bmatrix} x & 1 & 0 \\ 1 & x & -3 \\ 0 & 0 & x-1 \end{bmatrix} \in \mathrm{Mat}_{3\times 3}(R),$$

where $R = \mathbb{Q}[x]$.

(a) Determine the Smith normal form for A.

Proof. First, we claim that $\mathrm{ann}_R(R/(d)) = (d)$. If $r \in (d)$ then $r(x+(d)) = rx + (d) = 0 + (d)$ so $(d) \subseteq \mathrm{ann}_R(R/(d))$. Conversely, if $r \in \mathrm{ann}_R(R/(d))$ then $r(1+(d)) = 0 + (d)$, thus $r \in (d)$. This shows that $\mathrm{ann}_R(R/(d)) = (d)$, as claimed.

We claim that if the free rank of M is r and the invariant factors of M are $d_1 \mid d_2 \mid \dots \mid d_k$ then

$$\mathrm{ann}_R(M) = \begin{cases} (0) & \text{if } r > 0 \\ (d_k) & \text{if } r = 0. \end{cases} \quad \square$$

Notice that $\mathrm{ann}_R(R) = (0)$, since the only element that kills 1 is 0. By Problem 6 we have

$$\mathrm{ann}_R\left(R^r \oplus R/(d_1) \oplus \cdots \oplus R/(d_k)\right) = \begin{cases} \mathrm{ann}_R(R) \cap \mathrm{ann}_R(R/(d_1)) \cap \ldots \cap \mathrm{ann}_R(R/(d_k)), r > 0 \\ \mathrm{ann}_R(R/(d_1)) \cap \ldots \cap \mathrm{ann}_R(R/(d_k)), r = 0 \end{cases}$$

$$= \begin{cases} (0) \cap (d_1) \cap \ldots \cap (d_k) & \text{if } r > 0 \\ (d_1) \cap \ldots \cap (d_k) & \text{if } r = 0 \end{cases} = \begin{cases} (0) & \text{if } r > 0 \\ (d_k) & \text{if } r = 0 \end{cases}$$

(b) Determine a generator for the principal ideal $\mathrm{ann}_R(M)$ in terms of the elementary divisors and the free rank of M.

Proof. We will show if the free rank of M is r and the elementary divisors are $p_1^{e_1}, \dots, p_s^{e_s}$ then

$$\mathrm{ann}_R(M) = \begin{cases} (0) & \text{if } r > 0 \\ (\mathrm{lcm}(\mathrm{p}_1^{\mathrm{e}_1}, \dots, \mathrm{p}_\mathrm{s}^{\mathrm{e}_\mathrm{s}})) & \text{if } r = 0. \end{cases} \quad \square$$

As in a), we have

$$\operatorname{ann}_R\left(R^r \oplus R/(p_1^{e_1}) \oplus \cdots \oplus R/(p_s^{e_s})\right) = \begin{cases} (0) \cap (p_1^{e_1}) \cap \ldots \cap (p_s^{e_s}) & \text{if } r > 0 \\ (p_1^{e_1}) \cap \ldots \cap (p_s^{e_s}) & \text{if } r = 0. \end{cases}$$

The claim follows if we show that $(p_1^{e_1}) \cap \ldots \cap (p_s^{e_s}) = (\mathrm{lcm(p_1^{e1}, \ldots, p_s^{e_s})})$. Indeed:

$(\subseteq)$ If $r \in (p_1^{e_1}) \cap \ldots \cap (p_s^{e_s})$, then $r \in (p_i^{e_i})$ for all i, and in particular $p_i^{e_i} | r$ for all i. Therefore, $\mathrm{lcm(p_1^{e1}, \ldots, p_s^{e_s})|r}$, and thus $r \in (\mathrm{lcm(p_1^{e1}, \ldots, p_s^{e_s})})$.

$(\supseteq)$ Suppose that $r \in (\mathrm{lcm(p_1^{e1}, \ldots, p_s^{e_s})})$. Thus $p_i^{e_i} | \mathrm{lcm(p_1^{e1}, \ldots, p_s^{e_s})|r}$, which by transitivity implies that $p_i^{e_i} | r$, and $r \in (p_i^{e_i})$ for all i.

Problem 2. Let R be a domain. An R-module M is **torsionfree** if for $r \in R$ and $m \in M$, we have $rm = 0$ implies $r = 0$ or $m = 0$.

(a) Show that if R is a PID and M is a finitely generated torsionfree module, then M is free.

Proof. By the Structure Theorem for finitely generated modules over PIDs, we can write

$$M \cong R^t \oplus R/(r_1) \oplus \cdots \oplus R/(r_s).$$

If $s \neq 0$, then M cannot be torsionfree, since the element m corresponding to $1 + (r_s) \in R/(r_s)$ is a nonzero element satisfying $r_s m = 0$. Thus, we must have $M \cong R^t$, so M is free. □

(b) Give an example of a torsionfree module M over a PID R such that M is not free.

Proof. Consider the $\mathbb{Z}$-module $\mathbb{Q}$. This is torsionfree, since if $nr = 0$ with $n \in \mathbb{Z}$ and $q \in \mathbb{Q}$, since $\mathbb{Q}$ is a domain, we must have $n = 0$ or $q = 0$. We showed in an earlier problem set that $\mathbb{Q}$ is not a free $\mathbb{Z}$-module. □

(c) Give an example of a finitely generated torsionfree module M over a domain R such that M is not free.

Proof. Let $R = \mathbb{Z}[x]$ and $M = (2, x) \subseteq R$. Note that R is a domain; thus, if $r \in R$ is nonzero and $m \in M$ is nonzero, we can consider $m \in R$, and then $rm \neq 0$. This shows that M is torsionfree.

However, M is not free. To see it, suppose that there is a basis B for M. We must have $B \neq \varnothing$, since $M \neq 0$. Note that any element of B must be nonzero, since $1 \cdot 0 = 0$ implies that 0 cannot be part of any linearly independent set. If $|B| \geq 2$, take $a, b \in B \subseteq M$, and note that $a \cdot b - b \cdot a = 0$ implies that a, b are linearly dependent (since $a, b \neq 0$), so we must have $|B| = 1$. This would imply that M is generated by one element, so the ideal $(2, x)$ is principal. We showed in a problem set last semester that $(2, x)$ is not principal though. Thus, no basis B exists, so M is not free. □

Problem 3. Let F be a field and consider a monic polynomial $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ in $F[x]$ with $n \geqslant 1$.

(a) Show that the principal ideal $(f(x))$ is a subspace of the F-vector space $F[x]$.

Proof. First, note that $(f(x))$ is nonempty, since it contains $f(x)$. To show that $(f(x))$ is a subspace we need to check that $(f(x))$ is closed under addition and multiplication by elements of F. This is certainly true as ideals are closed under addition and multiplication by any elements of $F[x]$, and thus in particular closed under multiplication by elements of F. □

(b) Show that the set $B = \{\overline{1}, \overline{x}, \ldots, \overline{x^{n-1}}\}$, where $\overline{x^i} = x^i + (f(x))$, is a basis for the quotient F-vector space $F[x]/(f(x))$.

Proof. Let $g(x) \in F[x]$. By the Division Algorithm in $F[x]$, we have $g(x) = f(x)q(x) + r(x)$ where $r(x) = 0$ or $\deg(r) < n$. Since $g(x) - r(x) \in (f(x))$, we deduce that $g(x) + (f(x)) = r(x) + (f(x))$. Since $\deg(r) < n$, it follows that $r(x) + (f(x))$ is in the F-span of B, hence B spans $F[x]/(f(x))$.

Suppose $a_0\overline{1} + a_1\overline{x} + \cdots + a_{n-1}\overline{x^{n-1}} = 0$ in $F[x]/(f(x))$. Then $a_0 + a_1x + \cdots + a_{n-1}x^{n-1} \in (f(x))$. But the only polynomial in $(f(x))$ of degree less than n is 0, so $a_0 = \cdots = a_{n-1} = 0$ and thus B is linearly independent. □

(c) Consider the linear transformation $\mu_x : F[x]/(f(x)) \to F[x]/(f(x))$ defined by $\mu_x(v) = \overline{x}v$ for any $v \in F[x]/(f(x))$. Find the matrix representing μ_x in the basis B from part (b).

Proof. Recall that the columns of $[\lambda_x]_B^B$ are obtained by collecting the coefficients of the expressions for $l_x(b)$ for each $b \in B$ as linear combinations of the elements of B.

$$\begin{aligned}
l_x(\overline{1}) = \overline{x} \quad &= 0 \cdot \overline{1} + 1 \cdot \overline{x} + 0 \cdot \overline{x^2} + \cdots + 0 \cdot \overline{x^{n-1}} \\
l_x(\overline{x}) = \overline{x^2} \quad &= 0 \cdot \overline{1} + 0 \cdot \overline{x} + 1 \cdot \overline{x^2} + \cdots + 0 \cdot \overline{x^{n-1}} \\
&\vdots \\
l_x(\overline{x^{n-2}}) = \overline{x^{n-2}} \quad &= 0 \cdot \overline{1} + 0 \cdot \overline{x} + 0 \cdot \overline{x^2} + \cdots + 1 \cdot \overline{x^{n-1}}
\end{aligned}$$

Finally,

$$l_x(\overline{x^{n-1}}) = -a_0 \cdot \overline{1} - a_1 \cdot \overline{x} - a_2 \cdot \overline{x^2} + \cdots - a_{n-1} \cdot \overline{x^{n-1}}.$$

Thus

$$[\lambda_x]_B^B = \begin{bmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \ddots & 0 & -a_2 \\ \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & \cdots & 0 & 1 & -a_{n-1} \end{bmatrix}. \quad □$$

Problem 4. Let K be a field, and G be a finite subgroup of $K^\times$. Show[1,2] that G is cyclic.

Proof. Since the multiplication in K is commutative, G is an abelian group, and by assumption, a finite abelian group. In Invariant Factor Form, we then have

$$G \cong \mathbb{Z}/n_1 \oplus \cdots \mathbb{Z}/n_t$$

for some $n_1 | \cdots | n_t$. Observe that the order of any element in G divides n_t, since n_t annihilates G as a $\mathbb{Z}$-module.

By way of contradiction, suppose that G is not cyclic, so $t > 1$ and, in particular, $|G| > n_t$. Since every element of G has order dividing n_t, we have $g^{n_t} = 1$ for all $g \in G$. In particular, every element of G is a root of the polynomial $x^{n_t} - 1 \in K[x]$. However, a polynomial $f(x) \in K[x]$ can have at most $\deg(f)$ many roots in K, so $x^{n_t} - 1$ has at most n_t roots. This is a contradiction. We conclude that G must be cyclic. □

[1] Hint: Consider the invariant factors of G, and let e be the largest one. Show that every element of G is a root of the polynomial $x^e - 1 \in K[x]$.

[2] Note that as a special case of this, $(\mathbb{Z}/p)^\times$ is cyclic.