Problem Set 3

Due Thursday, February 4

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. Let F be a field, and V be a finite-dimensional F-vector space. Let W be a subspace of V. Show that $W = V$ if and only if $\dim(W) = \dim(V)$.

Proof. If $W = V$, then $\dim(W) = \dim(V)$. Conversely, if $W \subseteq V$ and $\dim(W) = \dim(V)$, we have $\dim(V) = \dim(W) + \dim(V/W)$, so $\dim(V/W) = 0$. This implies that $V/W = 0$, so $W = V$. □

Problem 2. Let R be a commutative ring. Show that if every R-module is free then R is a field.

Proof. Suppose that R is a commutative ring that is not a field. Then, from a problem from 817, there exists a proper nonzero ideal I.

We claim that R/I is not a free module. By way of contradiction, suppose that there exists a basis B. Since $R/I \neq 0$, we must have $B \neq \varnothing$. Take $r + I \in B$. Then for $a \in I \neq 0$, we have $a(r + I) = 0$ in R/I. This gives a nontrivial dependence relation on B, so B is not a basis. This shows that R/I is not free. □

Problem 3. Prove that[1] if R is a commutative ring then $R^m \cong R^n$ as R-modules if and only if $m = n$.

Proof. We prepare with a Lemma:

Lemma: If I is an ideal of R, then $R^n/IR^n \cong (R/I)^n$.

Proof: Let $f : R^n \to (R/I)^n$ be the unique R-module homomorphism such that $f(e_i) = \overline{e_i}$, where e_i is the vector with a 1 in the ith position and 0 elsewhere, and $\overline{e}_i$ is the vector with $1 + I$ in the ith position and $0 + I$ elsewhere. Such a map exists by the UMP for free modules since $\{e_1, \ldots, e_n\}$ form a basis for R^n.

Since the $\overline{e}_i$ form a basis for $(R/I)^n$ and since $\mathrm{im}(f)$ is a subspace of $(R/I)^n$ that contains all the $\overline{e}_i$, it follows that $\mathrm{im}(f) = (R/I)^n$, and thus f is surjective. A vector $(a_1, \ldots, s_n)$ is in the kernel of f if and only if $(a_1 + I, \ldots, a_n + I) = (0 + I, \ldots, 0 + I)$, or equivalently $a_i \in I$ for all i. Therefore

$$\ker(f) = \{(a_1, \ldots, a_n) \mid a_i \in I\} = \left\{ \sum_{i=1}^{n} a_i e_i \mid a_i \in I \right\} = IR^n.$$

[1] Hint: Consider $R^n/\mathfrak{m}R^n$ for a maximal ideal $\mathfrak{m}$.

The last equality follows because the containment $\subseteq$ holds by definition of IR^n and the containment $\supseteq$ is justified by the calculations below:

$$IR^n = \left\{ \sum_{i=1}^{m} b_i r_i \mid b_i \in I, r_i \in R^n \right\} = \left\{ \sum_{i=1}^{m} b_i \sum_{j=1}^{n} c_{ij} e_j \mid b_i \in I, c_{ij} \in R \right\}$$

$$= \left\{ \sum_{j=1}^{n} \left(\sum_{i=1}^{m} b_i c_{ij} \right) e_j \mid b_i \in I, c_{ij} \in R \Rightarrow b_i c_{ij} \in I \right\}.$$

So, by the first isomorphism theorem, f induces an R-**module** isomorphism

$$\overline{f} : R^n/IR^n \xrightarrow{\cong} (R/I)^n.$$

Moreover, both the source and target of $\overline{f}$ are R/I-modules: the right-hand side for obvious reasons and the left-hand side by an earlier exercise. We actually want $\overline{f}$ to be an R/I-module isomorphism. We already know that $\overline{f}$ preserves sums, since it is an R-module homomorphism. All that remains is to check that $\overline{f}$ is R/I-linear. Since $\overline{f}$ is R-linear:

$$\overline{f}((r+I)(m+IR^n)) = \overline{f}((rm+IR^n)) = f(rm) = rf(m) = (r+I)\overline{f}(m+IR^n).$$

The last equality follows since R/I acts on $(R/I)^n$ by $(r+I)t = rt$ for any $t \in (R/I)^n$. □

Now assume that $\varphi : R^n \to R^m$ is an R-module isomorphism. Take any maximal ideal $\mathfrak{m}$ of R, which exists by a result from Math 817. Consider the quotient map $q\colon R^m \to R^m/\mathfrak{m}R^m$ and the composite map $\psi = q \circ \varphi$. This is an R-module homomorphism, which is surjective since both q and φ are surjective. Let's consider the kernel of ψ. We know that $\ker q = \mathfrak{m}R^m$, since q is the canonical projection. Since φ is injective, the kernel of ψ is just the preimage of $\mathfrak{m}R^n$ via φ:

$$\ker(\psi) = \psi^{-1}(0) = \varphi^{-1}(q^{-1}(0)) = \varphi^{-1}(\mathfrak{m}R^m).$$

But φ^{-1} is an R-module homomorphism as well, so

$$\ker(\psi) = \mathfrak{m}\varphi^{-1}(R^m) = \mathfrak{m}R^n.$$

The First Isomorphism Theorem now gives the existence of an R-module isomorphism

$$\overline{\psi} : R^n/\mathfrak{m}R^n \to R^m/\mathfrak{m}R^m \quad \overline{\psi}(m+\mathfrak{m}R^n) = \psi(m).$$

We claim that $\overline{\psi}$ is in fact an $R/\mathfrak{m}$-module homomorphism; we need to check that this is an $R/\mathfrak{m}$-linear map:

$$\overline{\psi}((r+\mathfrak{m})(m+\mathfrak{m}R^n)) = \overline{\psi}(rm+\mathfrak{m}R^n) = \psi(rm) = r\psi(m) = (r+I)\overline{\psi}(m+\mathfrak{m}R^n),$$

where the last equality uses again the formula for the $R/\mathfrak{m}$-action on $R^m/\mathfrak{m}R^m$.

Using part a), we have the further isomorphisms

$$(R/\mathfrak{m})^n \cong R^n/\mathfrak{m}R^n \cong R^m/\mathfrak{m}R^m \cong (R/\mathfrak{m})^m.$$

Now rewriting the above isomorphism in terms of the field $F = R/\mathfrak{m}$ gives $F^n \cong F^m$ as F-vector spaces, and we know from class that this is true if and only if $m = n$. □

Problem 4. Let F be a field, and V be a finite-dimensional F-vector space. Let $T : V \to V$ be a linear transformation.

(a) Show that if $T^2 = 0$, then $\operatorname{rank}(T) \leq \frac{1}{2}\dim(V)$.

Proof. By the Rank-Nullity Theorem, we have

$$\dim(\ker(T)) + \operatorname{rank}(T) = \dim(V).$$

Since $T \circ T = 0$, we have $\operatorname{im}(T) \subseteq \ker(T)$. Then any basis of $\operatorname{im}(T)$ can be extended to a bases of $\ker(T)$, and thus

$$\operatorname{rank}(T) \leqslant \dim(\ker(T)).$$

So

$$\dim(V) = \dim(\ker(T)) + \dim(\operatorname{im}(T)) \geqslant \dim(\operatorname{im}(T)) + \dim(\operatorname{im}(T)) = 2\operatorname{rank}(T),$$

which implies the result. □

(b) Show that $\dim(\ker(T^2)) \leq 2\dim(\ker(T))$.

Proof. Let $I = \operatorname{im}(T)$ and consider $T|_I \colon I \to T$. Note that $T^2(V) = T|_I(I)$. We also have $\dim(I) = \dim(V) - \dim(\ker(T))$ by the Rank-Nullity Theorem and $\operatorname{rank}(T|_I) = \dim(I) - \dim(\ker(T|_I))$. Since $\ker(T|_I) = \ker(T) \cap I$, we have $\dim(\ker(T|_I)) \leq \dim(\ker(T))$. All together, we have

$$\begin{aligned}\operatorname{rank}(T^2)) &= \operatorname{rank}(T|_I) = \dim(I) - \dim(\ker(T|_I)) \\ &= \dim(V) - \dim(\ker(T)) - \dim(\ker(T|_I)) \geq \dim(V) - 2\dim(\ker(T))\end{aligned}$$

and by one more application of Rank-Nullity, $\dim(\ker(T^2)) \leq 2\dim(\ker(T))$ □

Problem 5. Let F be a field, and V and W be F-vector spaces with $\dim(V) = n$ and $\dim(W) = m$.

(a) Let $T : V \to W$ be a linear transformation. Show that there exist bases B for V and C for W such that

$$[T]_B^C = \begin{bmatrix} \mathbb{1}_{k\times k} & 0_{k\times(n-k)} \\ 0_{(m-k)\times k} & 0_{(m-k)\times(n-k)} \end{bmatrix}$$

where $\mathbb{1}_{k\times k}$ is a $k \times k$ identity matrix and $0_{i\times j}$ is an $i \times j$ matrix of zeroes.

Proof. Take a basis for $\ker(T) \subseteq V$, and call it $b_{k+1}, \ldots, b_n$. We can extend this to a basis for V, and let $b_1, \ldots, b_n$ be this basis. Note that $T(b_1), \ldots, T(b_k)$ are linearly independent: if

$$f_1T(b_1) + \cdots f_kT(b_k) = 0,$$

then $T(f_1b_1 + \cdots + f_kb_k) = 0$, so $v = f_1b_1 + \cdots + f_kb_k \in \ker(T)$, and hence v is in the span of $b_{k+1}, \ldots, b_n$; this is only possible if $f_i = 0$ for all i. Set $c_1 = T(b_1), \ldots, c_k = T(b_k)$, and extend $c_1, \ldots, c_k$ to a basis for V. It follows from the definition that $[T]_B^C$ is as claimed. □

(b) Let $T : V \to V$ be a linear transformation. Show that there exists a basis B for V such that

$$[T]_B^B = \begin{bmatrix} \mathbb{1}_{k\times k} & 0_{k\times(n-k)} \\ 0_{(n-k)\times k} & 0_{(n-k)\times(n-k)} \end{bmatrix}$$

if and only if $T^2 = T$.

Proof. Suppose there is a basis for which the matrix is as claimed. Then $[T^2]_B^B = ([T]_B^B)^2 = [T]_B^B$, so $T^2 = T$.

Now suppose that $T^2 = T$. Then for any $v = T(w) \in \mathrm{im}(T)$, we have $T(v) = T^2(w) = T(w) = v$, and in particular, $\ker(T) \cap \mathrm{im}(T) = 0$. By the Rank-Nullity Theorem, the dimension of $\ker(T)$ and the dimension of $\mathrm{im}(T)$ add up to $\dim(V)$. Take a basis $b_1, \ldots, b_k$ for $\mathrm{im}(T)$ and a basis $b_{k+1}, \ldots, b_n$ for $\ker(T)$; we claim that the union is a basis for V. Indeed, if $f_1 b_1 + \cdots f_n b_n = 0$, then $f_1 b_1 + \cdots + f_k b_k = -f_{k+1} b_{k+1} - \cdots - f_n b_n \in \ker(T) \cap \mathrm{im}(T) = 0$, and hten each $f_i = 0$ by linear independence of each basis. Thus $b_1, \ldots, b_n$ is linearly independent, and the span of this set is a subspace of dimension n, so is equal to V by the first problem. □