Problem Set 4 solutions

Problem 1. Let W be a subspace of a vector space V. Show that $\dim(V) = \dim(W) + \dim(V/W)$.

Proof. We will show the following: $\dim(V) < \infty$ if and only $\dim(W) + \dim(V/W)$. This will show the formula holds when one of the dimensions is infinite; when all three are finite, we will show that $\dim(V) = \dim(W) + \dim(V/W)$.

Case 1: If $\dim(V) = \infty$, then we claim that at least one of $\dim(W)$ or $\dim(V/W)$ is infinite.

Indeed, by problem 3 on Problem Set 3 we have that if both $\dim(W) < \infty$ and $\dim(V/W) < \infty$ (i.e both W and V/W are finitely generated) then V is finitely generated, so $\dim(V) < \infty$. This shows the contrapositive of the claim above.

Case 2: If $\dim(V) < \infty$, then we will show that $\dim(W) < \infty$ and $\dim(V/W) < \infty$, and prove that the formula above holds.

Any basis for W is in particular a linearly independent set of V, and thus it can be extended to a basis of V. Since every basis of V is finite, then any basis of W must also be finite. Say $B = \{w_1, \ldots, w_s\} \subseteq W$ is a basis for W and let $C = \{w_1, \ldots, w_s, v_1, \ldots, v_t\}$ be a basis for V. In particular, note that $\dim(V) = s + t$. We claim that $D = \{v_1 + W, \ldots, v_t + W\}$ is a basis for V/W, which in particular will show that $\dim(V/W) = t$, and thus

$$\dim(V) = s + t = \dim(W) + \dim(V/W).$$

First, we show that D generates V/W. Let $v + W \in V/W$. Since C generates V, we can find field elements $c_1, \ldots, c_s$ and $d_1, \ldots, d_t$ such that

$$v = \sum_{i=1}^{s} c_i w_i + \sum_{j=1}^{t} d_j v_j.$$

Since $w_i + W = 0 + W$ for all i, we get

$$v + W = \left(\sum_{i=1}^{s} c_i w_i + \sum_{j=1}^{t} d_j v_j \right) + W = \sum_{j=1}^{t} d_j (v_j + W),$$

Now we will show that D is linearly independent. Suppose that d_i are such that

$$0 = \sum_{j=1}^{t} d_j (v_j + W) = \left(\sum_{j=1}^{t} d_j v_j \right) + W.$$

Then $d_1 v_1 + \cdots + d_t v_t \in W$, so we can find $c_1, \ldots, c_s$ such that

$$\sum_{j=1}^{t} d_j v_j = \sum_{i=1}^{s} c_i w_i \implies \sum_{i=1}^{s} (-c_i) w_i + \sum_{j=1}^{t} d_j v_j.$$

But C is a linearly independent set, so all the $c_i = 0$ and $d_j = 0$. □

Problem 2. Let F be a field, $f \colon V \to W$ be an F-linear transformation, and $\operatorname{coker}(f) := W/\operatorname{im}(f)$. Prove that

$$\dim(\operatorname{coker}(f)) + \dim(V) = \dim(W) + \dim(\ker(f)).$$

Proof. By the Rank-Nullity Theorem,

$$\dim(V) = \dim(\ker(f)) + \dim(\operatorname{im}(f)).$$

By Problem 1, $\dim(\operatorname{coker}(f)) + \dim(\operatorname{im}(f)) = \dim(W)$. Adding $\dim(\operatorname{coker}(f))$ on both sides and using the equality from Problem 1 gives

$$\dim(V) + \dim(\operatorname{coker}(f)) = \dim(W) + \dim(\ker(f)). \qquad \square$$

Problem 3. Let $\phi : V \to V$ be an F-linear transformation. Prove that if $\phi \circ \phi = 0$, then

$$\dim(\operatorname{im}(\phi))) \leqslant \frac{1}{2}\dim(V).$$

Proof. By the Rank-Nullity Theorem, we have

$$\dim(\ker(\phi)) + \dim(\operatorname{im}(\phi)) = \dim(V).$$

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

$$\dim(\operatorname{im}(\phi)) \leqslant \dim(\ker(\phi)).$$

So

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

which implies the result. $\square$

Problem 4. Let R be a commutative ring with $1 \neq 0$. Let $f\colon R^a \to R^b$ be a surjective R-module homomorphism. Show that $a \geqslant b$.

Solution. Let $\mathfrak{m}$ be a maximal ideal of R, which exists by Math 817. Since f is R-linear, for every $c \in \mathfrak{m}$ and $x \in R^n$ we have $f(cx) = cf(x)$, so $f(\mathfrak{m}R^a) \subseteq \mathfrak{m}R^b$. Let $q\colon R^b \to R^b/\mathfrak{m}R^b$ be the canonical projection. Since $f(\mathfrak{m}R^a) \subseteq \mathfrak{m}R^b$, we conclude that $\mathfrak{m}R^a$ is contained in the kernel of $q \circ f$. By a result from class, $q \circ f$ induces a well-defined R-module homomorphism $R^a/\mathfrak{m}R^a \to R^b/\mathfrak{m}R^b$. More precisely, the map

$$\begin{aligned} R^a/\mathfrak{m}R^a &\xrightarrow{\overline{f}} R^b/\mathfrak{m}R^b \\ x + \mathfrak{m}R^a &\longmapsto f(x) + \mathfrak{m}R^b \end{aligned}$$

is a well-defined R-module homomorphism. Moreover, $\overline{f}$ is surjective: for any $x + \mathfrak{m}R^b \in R^b/\mathfrak{m}R^b$, we can find $y \in R^a$ such that $f(y) = x$, and $\overline{f}(y + \mathfrak{m}R^a) = f(y) + \mathfrak{m}R^b = x + \mathfrak{m}R^b$. Note that the source and target of $\overline{f}$ are both also $R/\mathfrak{m}$-modules, by a result from Problem Set 3. Now we claim that in fact $\overline{f}$ is also $R/\mathfrak{m}$-linear: indeed,

$$\overline{f}((c+\mathfrak{m})(x+\mathfrak{m}R^a)) = \overline{f}(cx+\mathfrak{m}R^a) = f(cx)+\mathfrak{m}R^a = cf(x)+\mathfrak{m}R^a = c(f(x)+\mathfrak{m}R^a) = (c+\mathfrak{m})\overline{f}(x+\mathfrak{m}R^a).$$

So we conclude that $\overline{f}\colon R^a/\mathfrak{m}R^a \to R^b/\mathfrak{m}R^b$ is a surjective homomorphism of $R/\mathfrak{m}$-modules. Notice also that $R/\mathfrak{m}$ is a field, so $R^a/\mathfrak{m}R^a$ and $R^b/\mathfrak{m}R^b$ are vector spaces over that field. Composing with the isomorphisms $(R/\mathfrak{m}R)^a \cong R^a/\mathfrak{m}R^a$ and $R^b/\mathfrak{m}R^b \cong (R/\mathfrak{m}R)^b$ from Problem Set 3, we conclude that $\overline{f}$ is a surjective linear transformation of $R/\mathfrak{m}$-vector spaces. This reduces the problem to showing that if $F^a \to F^b$ is a surjective linear transformation, then $a \geqslant b$.

Let $\varphi\colon F^a \to F^b$ is a surjective linear transformation. Then $\operatorname{im}(\varphi) = F^b$. By the Rank-Nullity Theorem,

$$b + \dim(\ker(\varphi)) = \dim(F^b) + \dim(\ker(\varphi)) = \dim(\operatorname{im}(\varphi)) + \dim(\ker(\varphi)) = \dim(F^a) = a.$$

Since $\dim(\ker(\varphi)) \geqslant 0$, we conclude that $b \leqslant a$.

Problem 5. Let R be a ring, M and N left R-modules, and $p: M \to N$ a surjective R-module homomorphism. We say p is a **split surjection** if there exists an R-module homomorphism $j: N \to M$ such that $p \circ j = id_N$.

a) Prove that if N is free, then every surjective R-module homomorphism of the form $p : M \to N$ is a split surjection.

Proof. Let B be a basis of N. Since p is onto, for each $b \in B$ there exists at least one $m \in M$ such that $p(m) = b$. Choose one such m_b for each $b \in B$. This gives us a function $g : B \to M$, defined by $g(b) = m_b$, so that $p(g(b)) = b$ for all $b \in B$. By the UMP of bases, there is a (unique) R-module homomorphism $j : N \to M$ such that $j(b) = g(b)$ for all $b \in B$. The composition $p \circ j$ is an R-module homomorphism from N to N that sends b to b for all $b \in B$. Since B is a basis of N, it must be that $p \circ j = id_N$ (by the uniqueness part of the UMP for bases). Thus p is a split surjection. □

b) Give an explicit example of a ring R and a surjective R-module homomorphism that is not split.

Proof. Take $R = \mathbb{Z}$, $M = \mathbb{Z}$, $N = \mathbb{Z}/(2)$, and $p : M \to N$ the canonical surjection sending n to $n + (2)$. We claim p is not a split surjection. In fact, we claim that the only $\mathbb{Z}$-module homomorphisms from $\mathbb{Z}/(2)$ to $\mathbb{Z}$ is the zero map, which does not give a splitting.

Throughout, let $\overline{j}$ denote the element $j + (2)$ of $\mathbb{Z}/(2)$. Say $g : \mathbb{Z}/(2) \to \mathbb{Z}$ is any $\mathbb{Z}$-module homomorphism. Then $g(\overline{0}) = 0$. Also,

$$0 = g(\overline{0}) = g(\overline{1} + \overline{1}) = g(\overline{1}) + g(\overline{1}).$$

Since the only element x of $\mathbb{Z}$ satisfying $x + x = 0$ is $x = 0$, this proves $g(\overline{1}) = 0$ too, and hence g is the zero map. □