Problem Set 5
Abstract Algebra II

Bennett Rennier
barennier@gmail.com

January 15, 2018

Ex A We call an R-module P *projective* if it has the following property: For any R-modules M and N where we have a surjective homomorphism $\varphi : M \to N$ and homomorphism $\psi : P \to N$, there is a homomorphism $\psi' : P \to M$ which satisfies $\varphi \circ \psi' = \psi$. Prove that every free R-module is projective.

Proof.

$$\begin{tikzcd} M \arrow[r, two heads, "\varphi"] & N \\ F \arrow[u, dotted, "\psi'"] \arrow[ur, "\psi"] & \end{tikzcd}$$

Let F be a free R-module. Since F is free, it has a basis, which we will denote by $\{x_i\}_{i\in I}$ for some index set I. We see that ψ sends these elements to $\{\psi(x_i)\}_{i\in I}$. Since φ is surjective, that means there exist elements $\{y_i\}_{i\in I}$ such that $\varphi(y_i) = \psi(x_i)$. (Note that this requires the Axiom of Choice in the general case.) Let $\psi' : F \to M$ be defined by $\psi' : x_i \mapsto y_i$. We see then that $(\varphi \circ \psi')(x_i) = \varphi(\psi'(x_i)) = \varphi(y_i) = \psi(x_i)$. Since $\varphi \circ \psi'$ and ψ agree on the basis elements, then they must be the same, i.e. $\varphi \circ \psi' = \psi$. This proves the statement. $\square$

Ex B We can "reverse arrows" and define what it means for a module to be injective. We call an R-module *injective* if given any R-modules M and N and an injective homomorphism $\varphi : N \to M$ and homomorphism $\psi : N \to I$, then there is always a homomorphism $\psi' : M \to I$ so that the obvious triangle commutes. Let k be a fixed field and prove by verifying the definitions that every k-module is both projective and injective.

Proof.

$$\begin{tikzcd} N \arrow[r, hook, "\varphi"] \arrow[d, "\psi"] & M \arrow[dl, dotted, "\psi'"] \\ V & \end{tikzcd}$$

Since k is a field, then N, M, and I are really k-vector spaces. Since every vector space has a basis, that means that V and N are free modules. By Ex A, this means that V is projective. Since N is free, let $\{x_i\}_{i\in I}$ be the basis of N. Then $\{\varphi(x_i)\}_{i\in I}$ has the same cardinality as $\{x_i\}_{i\in I}$, as φ is injective. Let $\psi' : M \to V$ be defined by sending $\varphi(x_i)$ to $\psi(x_i)$, which is possible as $\{x_i\}_{i\in I}$ has the same cardinality as $\{\varphi(x_i)\}_{i\in I}$. Then we see that $(\psi' \circ \varphi)(x_i) = \psi'(\varphi(x_i)) = \psi(x_i)$. Since $\psi' \circ \varphi$ and ψ agree on the basis elements, then they must be equal, i.e. $\psi' \circ \varphi = \psi$. $\square$

Ex C Prove that if F is a free R-module and $F \simeq P \oplus Q$ for submodules P and Q, then P is a projective R-module. That is, prove that direct summands of free modules are projective.

Proof. Let N and M be R-modules and let there be homomorphisms $\varphi : M \to N$ and $\psi : P \to N$ where φ is surjective. This gives us the following diagram:

$$\begin{tikzcd}
M \arrow[r, two heads, "\varphi"] & N \\
P \arrow[ur, "\psi"] \arrow[r, hook, shift right, "\iota"'] & F \arrow[l, two heads, shift right, "\pi"'] \arrow[u, "\psi\circ\pi"']
\end{tikzcd}$$

This digram commutes as $(\psi \circ \pi) \circ \iota = \psi \circ (\pi \circ \iota) = \psi \circ \mathrm{id}_P = \psi$. The other way around the triangle commutes trivally as $(\psi \circ \pi) = \psi \circ \pi$. Since F is a free module, then this means there exists a $(\psi \circ \pi)' : F \to M$, which keeps the diagram commutative. Using this, we get our ψ' as $(\psi \circ \pi)' \circ \iota : P \to M$, which trivally keeps the diagram commutative. This proves that P is projective. For a better visualization, this all accumulates into the following diagram:

$$\begin{tikzcd}
M \arrow[r, two heads, "\varphi"] & N \\
P \arrow[u, dotted, "(\psi\circ\pi)'\circ\iota"] \arrow[ur, "\psi"'] \arrow[r, hook, shift right, "\iota"'] & F \arrow[l, two heads, shift right, "\pi"'] \arrow[u, "\psi\circ\pi"'] \arrow[ul, "(\psi\circ\pi)'"]
\end{tikzcd}$$

$\square$

Ex D Prove that if P is a projective R-module, then there is a free R-module F and there are homomorphisms $\alpha : F \to P$ and $\beta : P \to F$ such that $\alpha \circ \beta = \mathrm{Id}_P$.

Proof. Let P be a projective R-module. This means that P is the quotient of some free module, as F/Q. There is the canonical homomorphism $\pi : F \to F/Q \simeq P$ where $\pi : f \mapsto f + Q$. We also know that this homomorphism is surjective. Let α be another name for π. Since P is projective, this gives us β, such that the following diagram commutes:

$$\begin{tikzcd}
F \arrow[r, two heads, "\pi=\alpha"] & F/Q \\
P \arrow[u, dotted, "\beta"] \arrow[ur, leftrightarrow, "="']
\end{tikzcd}$$

Thus, since the diagram is commutative, we get that $\alpha \circ \beta = \mathrm{id}_P$. Note that α is surjective and that β is injective (as it has a left inverse). $\square$

Ex E Prove that $e = \beta \circ \alpha \in \mathrm{End}(F)$ is an idempotent under multiplication given by composition. Prove that if you set $P' = \mathrm{Im}(e)$ and $Q = \mathrm{Im}(1-e)$, then $P \simeq P'$ and $F \simeq P' \oplus Q$. That is, combining B, C, and D we see that an R-module is projective if and only if it is a direct summand of a free module.

Proof. We see that $e^2 = (\beta \circ \alpha)^2 = \beta \circ \alpha \circ \beta \circ \alpha = \beta \circ \mathrm{id}_P \circ \alpha = \beta \circ \alpha = e$, which proves that e is an idempotent. Using e, we can construct the short exact sequence:

$$0 \longrightarrow \ker(e) \overset{\iota}{\hookrightarrow} F \overset{e}{\twoheadrightarrow} \mathrm{Im}(e) \longrightarrow 0$$

Let $\mu : \mathrm{Im}(e) \to F$ be the inclusion map and let $x \in \mathrm{Im}(e)$. That means that $x = e(f)$ for some $f \in F$. We see then that $(e \circ \mu)(x) = (e \circ \mu)(e(f)) = e(\mu(e(f))) = e(e(f)) = e^2(f) = e(f) = x$. Thus, $e \circ \mu = \mathrm{id}_{\mathrm{Im}(e)}$. By Proposition 25, this means that our sequence splits, which proves that $F \simeq \mathrm{Im}(e) \oplus \ker(e)$.

We see that since α is surjective (see last exercise), $\mathrm{Im}(e) = (\beta \circ \alpha)(F) = \beta(P)$. Since β is injective, this means that $\mathrm{Im}(e) = P'$, where P' is an isomorphic copy of P in F. We also see that for all $f \in F$ that $e((1-e)(f)) = e(f - e(f)) = e(f) - e^2(f) = e(f) - e(f) = 0$. This proves that $\mathrm{Im}(1-e) \subseteq \ker(e)$. Conversely, suppose that $f \in \ker(e)$, so f is in $\mathrm{Im}(1-e)$. Then, $(1-e)(f) = f - e(f) = f$. This proves that $\mathrm{Im}(1-e) = \ker(e)$.

Putting it all together, we have that $F \simeq \mathrm{Im}(e) \oplus \ker(e) = \mathrm{Im}(e) \oplus \mathrm{Im}(1-e) = P' \oplus Q$ and that $P' \simeq P$. This proves the statement. □

Ex F Let $R = k[x]$ be the polynomial ring in one variable with k a fixed ground field. Prove that R is indecomposable as an R-module but not simple.

Proof. We see that the action of R on itself is completely defined by $x.p(x) = xp(x)$. So R is the vector space of all polynomials, let's denote this by $\mathcal{P}$, along with the linear transformation $T : \mathcal{P} \to \mathcal{P}$ where $T(p(x)) = xp(x)$. If we use sequences to denote the elements of $\mathcal{P}$, we see that T is simply the right shift operator. Note that in this view that all but finitely many entries must be zero; this will be assumed implicitly throughout the rest of the proof. We define the codegree of a nonzero polynomial $p(x) = a_0 + a_1 x + a_2 x^2 + \dots a_n x^n$ as the smallest i such that $a_i \neq 0$.

Firstly, we see that $U = \{(0, x_1, x_2, x_3, \dots) \mid x_i \in F\}$ is clearly an subspace that is invariant under the right shift operator, which shows that R is not simple. Now let U be any subspace of $\mathcal{P}$ that's invariant under the T. Suppose that $U \neq \{0\}$ and let $u(x) \in U$ be a nonzero polynomial with minimal codegree. Let $j = \mathrm{codeg}(u(x))$. This means that $u(x) = (0, 0, \dots, 0, a_1, a_2, \dots, a_n, 0, 0, \dots)$ where a_1 is in the $(j+1)$th position. Then since k is a field and U is a vector space that is invariant under the right shift operator, we define vectors v_i to be

$$v_i(z) = \frac{x}{a_1} F^i(u(x)) = (0, \dots, 0, z, za_2/a_1, za_3/a_1, \dots, za_n/a_1, 0, \dots) \in U$$

where z is in the $(\ell + j + 1)$th position. We see that $\mathrm{span}\{v_i\}_{i \in \mathbb{N}} = \{(x_1, x_2, \dots) \mid x_j \in k \text{ and } x_j = 0 \text{ for all } j \leq i\} \subseteq U$. Since $u(x)$ was of miminal codegree, there can't be any vectors in U that are not of this form, which means that we actually have equality.

Thus, every subspace invariant under T looks like $U_j = \{(x_1, x_2, x_3, \dots) \mid x_i \in k \text{ and } x_i = 0 \text{ for all } i \leq j\}$.

Suppose now then that R was decomposable. That would mean that $\mathcal{P} = U_n \oplus U_m$ for some n and m. We know that there must be some vectors $u(x) \in U_n$ and $w(x) \in U_m$ such that $u(x) + w(x) = 1$. This means that it must be that at least one of these two polynomials has a nonzero coeffecient on the constant term, suppose that its $u(x)$. This means that $u(x)$ has a codegree of 0, which proves that $U_n = U_0 = \{(x_1, x_2, \dots) \mid x_i \in k\} = \mathcal{P}$ all along. Thus, $\mathcal{P}$ is indecomposable, which proves that R is indecomposable. □

Ex G We call a module *Noetherian* if every increasing chain of submodules eventually terminates. We call a module *Artinian* if every decreasing chain of submodules eventually terminates. Prove that every finite-dimensional $k[x]$-module is both Noetherian and Artinian. On the other hand $k[x]$ is Noetherian but not Artinian as a $k[x]$-module.

Proof. Suppose we have a finite-dimensional $k[x]$-module. Then this module is simply a finite-dimensional k-vector space, call it V, along with a linear transformation $T : V \to V$. Submodules of V are subspaces of V which are invariant under T. If $W_1 \subsetneq W_2 \subsetneq \dots$ is a chain of such subspaces, then $\dim(W_1) < \dim(W_2) < \dots$. However $\dim(W_i) < \dim(V)$, since they are all subspaces. This means proves that the sequence must eventually terminate. Similarly, if we have a decreasing chain $W_1 \supsetneq W_2 \supsetneq \dots$, then $\dim(W_1) > \dim(W_2) > \dots$. Since $\dim(W_i) > 0$, this sequence must also terminate. This proves that every finite-dimensional $k[x]$-module is both Noetherian and Artinian.

We saw in the previous exercise that $k[x]$ over itself is equivalent to $\mathcal{P}$ (the space of all polynomials) under the right shift operator, and that the subspaces of $\mathcal{P}$ that are invariant under this operator are of the form $U_j = \{(x_1, x_2, x_3, \dots) \mid x_i \in k \text{ and } x_i = 0 \text{ for all } i \leq j\}$. Using this, we can easily see that $U_0 \supsetneq U_1 \supsetneq \dots$ is a decreasing chain of invariant subspaces (which correspond to submodules of $k[x]$) that never terminates. This proves that $k[x]$ is not Artinian as a $k[x]$-module.

Now suppose that $W_1 \subsetneq W_2 \subsetneq \dots$ is an nonterminating increasing chain of invariant subspaces. Then $W_1 = U_{n_1}$ for some $n_1 \in \mathbb{N}$ and each W_i corresponds to a U_{n_i} where n_i is a deceasing sequence of natural numbers. This means that n_i must eventually reach zero, suppose it does at n_j. Then for all $i \geq j$, we have that $W_i = U_0 = \mathcal{P}$. This contradictions that our chain is nonterminating, which proves every increasing chain of subspaces eventually terminates. This proves that $k[x]$ is Noetherian as a $k[x]$-module. □