36.12.5 Suppose that

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

is a short exact sequence of R-modules with C a free R-module. Show the sequence splits.

Solution Let $\mathfrak{C}$ be a basis for C.

Since the sequence is exact, g is an epimorphism, so for each $c_\alpha \in \mathfrak{C}$, there exists $b_\alpha \in B$ so that $g(b_\alpha) = c_\alpha$. Define

$$g' : \begin{cases} C \to B \\ \sum_\alpha r_\alpha c_\alpha \mapsto \sum_\alpha r_\alpha b_\alpha. \end{cases}$$

Since $\mathfrak{C}$ is a basis, this is well-defined. It is also a homomoprhism:

$$\begin{aligned} g'\left(t \sum_\alpha r_\alpha c_\alpha + \sum_\alpha s_\alpha c_\alpha\right) &= g'\left(\sum_\alpha (t r_\alpha + s_\alpha) c_\alpha\right) \\ &= \sum_\alpha (t r_\alpha + s_\alpha) b_\alpha \\ &= t \sum_\alpha r_\alpha b_\alpha + \sum_\alpha s_\alpha b_\alpha \\ &= t g'\left(\sum_\alpha r_\alpha c_\alpha\right) + g'\left(\sum_\alpha s_\alpha b_\alpha\right). \end{aligned}$$

Moreover,

$$(g \circ g')\left(\sum_\alpha r_\alpha c_\alpha\right) = g\left(\sum_\alpha r_\alpha b_\alpha\right) = \sum_\alpha r_\alpha g(b_\alpha) = \sum_\alpha r_\alpha c_\alpha,$$

so $gg' = 1_C$. Thus, the sequence splits.

36.12.10 Let P be an R-module. Then P is called R-*projective* if given any R-epimorphism $f\colon B \to C$ and R-homomorphism $g\colon P \to C$, there exists an R-homomoprhism $h\colon P \to B$ such that the diagram

$$\begin{tikzcd} & P \arrow[dl, "h"'] \arrow[d, "g"] \\ B \arrow[r, "f"'] & C \end{tikzcd}$$

commutes. Show that any free R-module is projective.

Solution Let P be a free-module, and let $\mathfrak{P}$ be a basis of P.

Let f, g be the homomorphisms described in the problem. For each $p_\alpha \in \mathfrak{P}$, consider $g(p_\alpha)$. Because f is an epimorphism, there exists b_α such that $f(b_\alpha) = g(p_\alpha)$, for each $p_\alpha \in \mathfrak{P}$. Set $h(p_\alpha) = b_\alpha$ for each p_α.

Then h is a homomorphism:

$$\begin{aligned} f\left(t \sum_\alpha r_\alpha p_\alpha + \sum_\alpha s_\alpha p_\alpha\right) &= f\left(\sum_\alpha (t r_\alpha + s_\alpha) p_\alpha\right) \\ &= \sum_\alpha (t r_\alpha + s_\alpha) b_\alpha \\ &= t \sum_\alpha r_\alpha b_\alpha + \sum_\alpha s_\alpha b_\alpha \\ &= t f\left(\sum_\alpha r_\alpha p_\alpha\right) + f\left(\sum_\alpha s_\alpha p_\alpha\right). \end{aligned}$$

h is also well-defined, since p_α is a basis.

Moreover, $(f \circ h)(p_\alpha) = f(b_\alpha) = g(p_\alpha)$, for every p_α, so the diagram commutes. Hence, P is projective.

36.12.11 Show that a direct summand of an R-free module is projective and a direct sum of R-modules is projective if and only if each direct summand of it is R-projective.

Solution Let P be an R-free module and let M be a direct summand of P, i.e., there exists N so that $M \oplus N = P$.

Now let B, C be R-modules, $f\colon B \to C$ be an R-epimorphism, and let $g\colon M \to C$ be an R-homomorphism. We wish to find $h\colon M \to B$ so that

$$\begin{tikzcd} & M \arrow[d, "g"] \arrow[dl, dashed, "h"'] \\ B \arrow[r, "f"'] & C \end{tikzcd}$$

commutes.

Notice that because M is a direct summand, there exists $\pi\colon P \to M$ so that $\pi \circ \mathrm{inc} = \mathrm{id}_M$, where inc is the inclusion mapping.

Now consider $\pi \circ g$, which is a homomorphism. Since P is projective, there exists $h'\colon P \to B$ so that $f \circ h' = g$. Set $h = h' \circ \mathrm{inc}$, and this gives our desired map, so M is projective.

"$\Longrightarrow$"

This follows by induction on the previous claim.

"$\Longleftarrow$"

Let $P = \bigoplus_{\alpha \in A} P_\alpha$, and suppose that each P_α is R-projective.

Let $g\colon P \to C$ be an R-homomorphism and let $f\colon B \to C$ be an R-epimorphism. Consider the inclusions $i_\alpha\colon P_\alpha \to P$. Then we have the following commutative diagram:

$$\begin{tikzcd} & P_\alpha \arrow[d, "g \circ i_\alpha"] \arrow[dl, dashed, "h_\alpha"'] \\ B \arrow[r, "f"'] & C \end{tikzcd}$$

Since P_α is projective, there exists h_α so that $f \circ h_\alpha = g \circ i_\alpha$. Set $h = \sum_\alpha h_\alpha \circ \pi_\alpha$, where π_α is the projection onto the α-th coordinate. This is a homomorphism, and this gives

$$(f \circ h)(0 + \cdots + 0 + p_\alpha + 0 + \cdots + 0) = (f \circ h_\alpha)(p_\alpha) = g(0 + \cdots + 0 + p_\alpha + 0 + \cdots + 0),$$

and by linearity, this extends to any element of p. Hence, P is projective.

36.12.12 Let P be an R-module. Show that P is a projective R-module if and only if, whenever

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0 \qquad (*)$$

is a short exact sequence of R-modules and R-homomorphisms, then

$$0 \longrightarrow \mathrm{Hom}_R(P, A) \xrightarrow{f_*} \mathrm{Hom}_R(P, B) \xrightarrow{g_*} \mathrm{Hom}_R(P, C) \longrightarrow 0$$

is exact. In particular, if C is R-projective, then $(*)$ is split exact.

Solution "$\Longrightarrow$"

Suppose P is projective.

From a previous homework assignment, we already know that the sequence is exact at the first two modules, so we just need to show that g_* is surjective.

Let $h \in \mathrm{Hom}_R(P, C)$. By problem (10), there exists a homomorphism $h' \in \mathrm{Hom}_R(P, B)$ so that $g \circ h' = h$, so g_* is surjective, so the sequence is exact.

"$\Longleftarrow$"

Let $g\colon B \to C$ be an R-epimorphism and $h\colon P \to C$ be an R-homomorphism. Now let $f\colon A \to B$ be a function so that $(*)$ is exact. Then g_* is onto, so there exists $h' \in \operatorname{Hom}_R(P, B)$ so that $g \circ h' = h$, so P is projective.

36.12.14 Let R be a commutative ring and M, N two R-modules. Let P be the free R-module on basis $\{(m, n) \mid m \in M,\ n \in N\}$ and X the submodule of P generated by the elements

(a) $(m_1 + m_2, n) - (m_1, n) - (m_2, n)$ for all $m_1, m_2 \in M$ and $n \in$.

(b) $(m, n_1 + n_2) - (m, n_1) - (m, n_2)$ for all $m \in M$ and $n_1, n_2 \in N$.

(c) $(rm, n) - r(m, n)$ for all $m \in M$, $n \in N$, and $r \in R$.

(d) $(m, rn) - r(m, n)$ for all $m \in M$, $n \in N$, and $r \in R$.

Let $f\colon M \times N \to P/X$ be the R-bilinear map induced by $(m, n) \mapsto (m, n) + X$, i.e., an R-homomorphism in each variable. Show that $f\colon M \times N \to P/X$ satisfies the following universal property: If $g\colon M \times N \to Q$ is an R-bilinear map, then there exists a unique R-homomorphism $h\colon P/X \to Q$ such that

$$\begin{tikzcd} M \times N \arrow[r, "f"] \arrow[dr, "g"'] & P/X \arrow[d, "h"] \\ & Q \end{tikzcd}$$

commutes. The R-module P/X is called the *tensor product* of M and N and denoted by $M \otimes_R N$ and the elements $(m, n) + X$ are denoted by $m \otimes n$.

Solution Uniqueness:

Let h be such a homomorphism. By definition, $h \circ f = g$. Let $(m, n) \in M \times N$, so that

$$h(f(m, n)) = g(m, n) \implies h((m, n) + X) = g(m, n).$$

Since f is an epimorphism, this gives us a formula for h for any element of P/X, so h is uniquely determined by this.

Existence:

Set $h((m, n) + X) = g(m, n)$ for every coset $(m, n) + X$. We just need to show that this is a well-defined homomorphism.

Let $(m, n) - (m', n') \in X$. Then

$$h((m, n) - (m', n') + X) = g(m - m', n - n')$$

$(m - m', n - n')$ must be a linear combination of the elements of (a), (b), (c), and (d). Since g is a bilinear map, it's easy to check that $g(m - m', n - n')$ must be zero so that h is well-defined.

Now we need to show that h is a homomorphism:

$$\begin{aligned} h(r(m, n) + (m', n') + X) &= h((rm + m', rn + n') + X) \\ &= g(rm + m', rn + n') \\ &= rg(m, n) + g(m', n') \\ &= rh((m, n) + X) + h((m', n') + X), \end{aligned}$$

so h is a homomorphism.

Lastly, by definition of h, $h \circ f = g$, so the diagram commutes.

36.12.21 Let R be a commutative ring and A, B, C be R-modules. Show that $\operatorname{Hom}_R(A, \operatorname{Hom}_R(B, C)) \simeq \operatorname{Hom}_R(A \otimes_R B, C)$.

Solution Let $M \times N = A \times B$, $Q = C$, f, X be as in problem 14.

Let $f\colon A \otimes_R B \to C$ be a homomorphism. Then set $(\bar{f}(a))(b) = f(a \otimes b)$. It's clear that this is a homomorphism since f is. Conversely, given $\bar{g}\colon A \to \operatorname{Hom}_R(B, C)$, set $g(a \otimes b) = (\bar{g}(a))(b)$. This is also a homomorphism because $\tilde{g}(a)$ is, and this is an inverse to $\bar{\cdot}$, so the two sets are isomorphic.

37.12.2 Let M be a Noetherian R-module. Show that any surjective R-endomorphism $f\colon M \to M$ is an isomorphism.

Solution Since M is Noetherian, it is finitely generated by $x_1, \ldots, x_n$ for some $n \geq 1$. We then endow M with an $R[x]$-module structure via $x \cdot m = f(m)$. Then $(x)M = M$, since f is an epimorphism.

Thus, for each x_i, we can find polynomials $p_{ij} \in (x)$ so that

$$x_i = \sum_{k=1}^{n} p_{ij} x_j.$$

We now apply Cayley-Hamilton to the $R[x]$-endomorphism on M given by $v(x) = x$. Let $P \coloneqq (p_{ij})_{ij}$. Then $v(x) = Px$, since each x_i is sent to a linear combination that is equal to itself. Note that if the coefficients of χ_P are μ_k, then $\mu_k \in (x)$, since when we expand, we get sums and products of elements in (x). Thus, there exists $\tilde{\mu}_k \in R[x]$ such that $\mu_k = x\tilde{\mu}_k$. By Cayley-Hamilton,

$$0 = \chi_P(v)(m) = \left(v^n + \sum_{k=1}^{n-1} \mu_k v^k\right)(m) = m + \sum_{k=1}^{n-1} x\tilde{\mu}_k m = m + \sum_{k=1}^{n-1} \tilde{\mu}_k f(m) \implies m = \left(-\sum_{k=1}^{n-1} \tilde{\mu}_k\right) f(m).$$

So multiplication by $-\sum \tilde{\mu}_k$ is an inverse homomorphism for f, so f is an isomorphism.

37.12.5 Let R be a Noetherian ring, $\mathfrak{A}$ an ideal in R, A a finitely generated R-module, and B a submodule of A. Suppose that C is a submodule of A that contains $\mathfrak{A}B$ and is maximal with respect to the property that $C \cap B = \mathfrak{A}B$. Let x be an element of $\mathfrak{A}$. Show all of the following:

a. The chain of submodules $\{a \in A \mid x^m a \in C \text{ for all } a \in A\}$, $m \in \mathbb{Z}^+$, stabilizes.

b. There exists an integer n such that $(x^n A + C) \cap B = \mathfrak{A}B$.

c. $\mathfrak{A}^n A \subseteq C$ for some n.

d. If $B = \bigcap_{i=0}^{\infty} \mathfrak{A}^n A$, then $\mathfrak{A}B = B$.

Solution a. Since C is a submodule, multiplication by x keeps elements inside C, so the sequence of submodules is indeed a chain. Moreover, each of these sets is an ideal. Multiplication by an element of R is clear since C is a submodule. On the other hand, if $a, b \in A$ with $x^n a, x^m b \in C$, then $x^{n+m}(a + b) \in C$, because C is a submodule.

Since R is Noetherian, it follows that the chain stabilizes.

b. Let $z \in \mathfrak{A}B \subseteq C$ so that we can write $z = ab$, for some $a \in \mathfrak{A}$ and $b \in B$. Because $0 \in A$, $z = x^n 0 + ab \in (x^n A + C) \cap B$ for any $n \geq 1$. So, we need to find $n \geq 1$ so that the other inclusion holds.

Set $A_n = (C\colon x^n)$. By (a), the chain $\{A_n\}$ stabilizes, so there exists $n \geq 1$ such that $A_n = A_{n+1} = A_{n+2} = \cdots$, i.e., if $a \in A_n$, then $x^{n+k} a \in C \implies x^n a \in C$ for all $k \geq 0$.

Now let $x^n a + c \in (x^n A + C) \cap B$. Then $x(x^n a) = x^{n+1} a \in \mathfrak{A}B \subseteq C$, so $x^{n+1} a \in C \implies x^n a \in C \implies x^n a + c \in C$, so $x^n A + C \subseteq C$. Hence, $(x^n A + C) \cap B \subseteq C \cap B = \mathfrak{A}B$, as required.

c. Suppose otherwise, and that for every $n \geq 1$, there exists $x \in \mathfrak{A}$ and $a \in A$ so that $x^n a \notin C$.

By (b), there exists $N \geq 1$ so that $(x^N A + C) \cap B = \mathfrak{A}B \subseteq C$. Then $x^N a + c = c_1$, for some $c, c_1 \in C$. But because C is a submodule, this implies that $x^N a \in C$.

If $N \geq n$, then by the argument used in (b), $x^n a \in C$, which can't happen. On the other hand, if $N < n$, because C is a submodule, $x^{n-N}(x^N a) \in C$, which is also impossible. Hence, no such n exists, and the claim holds.

d. It's clear that $\mathfrak{A}B \subseteq B$, since B is a submodule, so we need to show the other direction. By (c), we have $B \subseteq C$, so $B = B \cap B \subseteq C \cap B = \mathfrak{A}B$. Thus, $\mathfrak{A}B = B$.

37.12.6 Let R be a commutative ring, $\mathfrak{A}$ an ideal in R, M an R-module generated by n elements, and x an element of R satisfying $xM \subseteq \mathfrak{A}M$. Show that $(x^n + y)M = 0$ for some y in $\mathfrak{A}$. In particular, if $\mathfrak{A}M = M$, then $(1 + y)M = 0$ for some $y \in \mathfrak{A}$.

Solution Let $x_1, \dots, x_n$ generate M, and consider the endomorphism $u(m) = xm$, where x is as in the problem statement.

Notice that $u(x_i) = xx_i \in xM \subseteq \mathfrak{A}M$, so we can find $a_{i1}, \dots, a_{in} \in \mathfrak{A}$ so that $a_{i1}x_1 + \cdots + a_{in}x_n = xx_i$. Hence, we can represent u as the matrix $(a_{ij})_{ij}$. We can then represent the characteristic polynomial of u as

$$\chi_u(t) = t^n + \sum_{k=0}^{n-1} b_k t^k, \quad b_k \in \mathfrak{A}.$$

By Cayley-Hamilton,

$$0 = \chi_u(u)(m) = u^n(m) + \sum_{k=0}^{n-1} b_k u^k(m) = \left(x^n + \sum_{k=0}^{n-1} b_k x^k\right) m,$$

for any m. Hence, if we take $y = \sum b_k x^k$, we have $(x^n + y)M = 0$, as required.

If $\mathfrak{A}M = M = 1 \cdot M$, then we get the other claim right away.

37.12.7 Let R be a Noetherian ring. Using the previous two exercises, show the following:

a. Suppose that R is a domain and $\mathfrak{A} < R$ be an ideal. Let M be a finitely generated R-module satisfying $\operatorname{ann}_R(m) = 0$ for all $m \in M$. Then $\bigcap_{i=0}^{\infty} \mathfrak{A}^n M = 0$.

b. Let $\mathfrak{A} = \bigcap_{\operatorname{Max}(R)} \mathfrak{m}$. Then $\bigcap_{i=0}^{\infty} \mathfrak{A}^n M = 0$.

Solution a. By problem 5(c), if we set $B = \bigcap_{i=0}^{\infty} \mathfrak{A}^n M$, then $\mathfrak{A}B = B$. By problem (6), there exists $y \in \mathfrak{A}$ so that $(1 + y)B = 0$. $y \neq -1$, or else $\mathfrak{A} = R$, which is impossible. Thus, $1 + y$ is non-zero. Then for every $m \in B$, we can write $m = ab$, where $a \in \mathfrak{A}$ and $b \in B$. Then

$$0 = (1 + y)m = (1 + y)(ab) = [(1 + y)a]b = 0 \implies (1 + y)a = 0,$$

since the annihilator of any element in B is zero. Since R is a domain and $1 + y$ is non-zero, $a = 0 \implies m = ab = 0$, so $B = 0$.

Since R is a domain, this means that $m = 0$, i.e., $B = 0$, as required.

b. Again, set $B = \bigcap_{i=0}^{\infty} \mathfrak{A}^n M$ and use the same argument as (a) so that $\mathfrak{A}B = B$ and $(1 + y)B = 0$ for some $y \in \mathfrak{A}$.

Suppose B has a non-zero element x. Because y is in the Jacobson radical, $1 + y$ is a unit, so there exists $z \in R$ such that $z(1 + y) = 1$, so

$$x = z(1 + y)x = z \cdot 0 = 0.$$

Hence, $B = 0$.