# LINEAR ALGEBRA II: PROJECTIVE MODULES

Let $R$ be a ring. By 'module' we will mean $R$-module and by 'homomorphism' (respectively isomorphism) we will mean homomorphism (respectively isomorphism) of $R$-modules, unless explicitly stated otherwise.

## 1. Definition and motivation

**Definition 1.1.** *A module $P$ is projective if, given*

- *any surjective homomorphism $\varepsilon : B \twoheadrightarrow C$, and*
- *any homomorphism $\gamma : P \to C$,*

*there exists a homomorphism $\beta : P \to B$ such that $\varepsilon \circ \beta = \gamma$.*

**Proposition 1.2.** *Let $P$ be a projective module. Then any surjective homomorphism $\varepsilon : Q \twoheadrightarrow P$ induces an isomorphism of the form $Q \cong \ker(\varepsilon) \oplus P$.*

*Proof.* Since $P$ is projective, we may and will define a homomorphism $\beta : P \to Q$ which satisfies $(\varepsilon \circ \beta)(p) = p$ for all $p \in P$. We may hence define a map $\alpha : \ker(\varepsilon) \oplus P \to Q$ by the formula $\alpha((q,p)) := q + \beta(p)$ and proceed to prove that it is an isomorphism.

The fact that $\alpha$ is a homomorphism is a straightforward consequence of the fact that so is $\beta$.

In order to prove injectiveness, we assume that $\alpha((q,p)) = q + \beta(p) = 0$ and deduce that $\beta(p) = -q \in \ker(\varepsilon)$ and hence that $p = \varepsilon(\beta(p)) = 0$. It follows that $q = -\beta(0) = 0$ and hence that $(q,p) = 0$, as required.

In order to prove surjectiveness, we let $q$ be any element of $Q$. We then have that $\varepsilon(q - \beta(\varepsilon(q))) = \varepsilon(q) - \varepsilon(\beta(\varepsilon(q))) = \varepsilon(q) - \varepsilon(q) = 0$. So we have that $q - \beta(\varepsilon(q))$ belongs to $\ker(\varepsilon)$ and finally find that $\alpha((q - \beta(\varepsilon(q)), \varepsilon(q))) = q - \beta(\varepsilon(q)) + \beta(\varepsilon(q)) = q$. $\square$

**Remark 1.3.** *Proposition 1.2 shows than when studying the structure of a module, it can be useful to construct a surjective homomorphism to a projective module in order to shift attention to the two components in the direct sum decomposition given by the proposition, whose structure may then turn out to be easier to understand. We proved in Theorem 3.15 b) that free modules have the precise same property that Proposition 1.2 attributes to projective modules. In fact, it is easy to use Theorem 3.15 a) to show that every free module is projective. However, the converse is not true in general, which justifies giving a name to this important class of modules.*

**Theorem 1.4.** *Every free module is projective.*

*Proof.* Let $F = \bigoplus_{j \in J} Rf_j$ be a free module and suppose given any surjective homomorphism $\varepsilon : B \twoheadrightarrow C$ and any homomorphism $\gamma : F \to C$. For any $j \in J$, let $b_j$ be any element of $B$ such that $\varepsilon(b_j) = \gamma(f_j)$. By Theorem 3.15 a), there exists a homomorphism $\beta : F \to B$ such that $\beta(f_j) = b_j$ for every $j \in J$. But then $(\varepsilon \circ \beta)(f_j) = \gamma(f_j)$ for every $j \in J$, and since this equality holds for every generator $f_j$ of $F$, it is easy to deduce that $\varepsilon \circ \beta = \gamma$, as required. □

## 2. Exact sequences and commutative diagrams

**Definition 2.1.**

- *Let $\phi : A \to B$ and $\psi : B \to C$ be homomorphisms. The sequence of homomorphisms $A \xrightarrow{\phi} B \xrightarrow{\psi} C$ is said to be exact at $B$ if $\ker(\psi) = \mathrm{im}(\phi)$.*
- *A sequence of homomorphisms $M_0 \to M_1 \to \ldots \to M_n \to M_{n+1}$ is called exact if it is exact at $M_1, \ldots, M_n$.*
- *An exact sequence of the form $0 \to A \to B \to C \to 0$ is called a short exact sequence (or s.e.s. for short). Here 0 denotes the trivial module, and both the arrow going from 0 to the $A$ and the arrow going from $C$ to 0 denote the zero homomorphism (i.e., the homomorphism sending every element to zero).*

**Remark 2.2.** *To understand the significance of short exact sequences, consider the following situations:*

(1) *Let $0 \to A \xrightarrow{\phi} B \xrightarrow{\psi} C \to 0$ be a short exact sequence. Exactness at $A$ is equivalent to $\phi$ being injective, exactness at $C$ is equivalent to $\psi$ being surjective and exactness at $B$ is equivalent to having $\ker(\psi) = \mathrm{im}(\phi)$. The first isomorphism theorem implies that $\phi$ induces an isomorphism of the form $A/\ker(\phi) \xrightarrow{\sim} \mathrm{im}(\phi)$ and that $\psi$ induces an isomorphism of the form $B/\ker(\psi) \xrightarrow{\sim} \mathrm{im}(\psi)$. So the assumption that the sequence is exact means that $\phi$ gives an isomorphism from $A$ to the submodule $\mathrm{im}(\phi) = \phi(A)$ of $B$ and that $\psi$ induces an isomorphism of the form*
$$B/\phi(A) = B/\mathrm{im}(\phi) = B/\ker(\psi) \xrightarrow{\sim} \mathrm{im}(\psi) = C.$$

(2) *Conversely, let $A$ be a submodule of a module $B$. Then we obtain a short exact sequence of the form*
$$0 \to A \xrightarrow{\iota} B \xrightarrow{\pi} B/A \to 0$$
*where $\iota$ is just the tautological inclusion (i.e., $\iota(a) = a$ for all $a \in A$) and $\pi$ is just the natural projection given by $\pi(b) := b + A$ for any $b \in B$. Indeed, $\iota$ is clearly injective, $\pi$ is clearly surjective and $\ker(\pi) = A = \mathrm{im}(\iota)$, so the sequence is exact.*

**Definition 2.3.** *We say that a diagram of homomorphisms of the form*
$$\begin{array}{ccc} A & \xrightarrow{\alpha} & B \\ {\scriptstyle\gamma}\big\downarrow & & \big\downarrow{\scriptstyle\beta} \\ C & \xrightarrow{\delta} & D \end{array}$$

*is commutative if* $\beta \circ \alpha = \delta \circ \gamma$. *This notion generalizes in an obvious way to more complicated diagrams of homomorphisms.*

**Lemma 2.4.** *Let*

$$\begin{array}{ccccccccc} & & A_1 & \xrightarrow{\mu} & A_2 & \xrightarrow{\varepsilon} & A_3 & \longrightarrow & 0 \\ & & {\scriptstyle\alpha_1}\downarrow & & {\scriptstyle\alpha_2}\downarrow & & {\scriptstyle\alpha_3}\downarrow & & \\ 0 & \longrightarrow & B_1 & \xrightarrow{\mu'} & B_2 & \xrightarrow{\varepsilon'} & B_3 & & \end{array}$$

*be a commutative diagram with exact rows and assume that both* $\alpha_1$ *and* $\alpha_3$ *are isomorphisms. Then* $\alpha_2$ *is an isomorphism.*

*Proof.* We first show that $\alpha_2$ is injective: suppose that $a \in A_2$ is such that $\alpha_2(a) = 0$. Then $(\alpha_3 \circ \varepsilon)(a) = (\varepsilon' \circ \alpha_2)(a) = 0$. Since $\alpha_3$ is injective, this implies that $\varepsilon(a) = 0$. Since $\ker(\varepsilon) = \mathrm{im}(\mu)$, there exists $a' \in A_1$ such that $\mu(a') = a$. Then $(\mu' \circ \alpha_1)(a') = (\alpha_2 \circ \mu)(a') = \alpha_2(a) = 0$. But, since both $\mu'$ and $\alpha_1$ are injective, this implies that $a' = 0$, so that $a = \mu(a') = \mu(0) = 0$, as required.

We now show that $\alpha_2$ is surjective: let $b \in B_2$. Since $\alpha_3$ is surjective, there exists $a \in A_3$ such that $\alpha_3(a) = \varepsilon'(b)$, and since $\varepsilon$ is surjective, there exists $a' \in A_2$ such that $\varepsilon(a') = a$. But then

$$\varepsilon'(b - \alpha_2(a')) = \varepsilon'(b) - (\varepsilon' \circ \alpha_2)(a') = \varepsilon'(b) - (\alpha_3 \circ \varepsilon)(a') = \varepsilon'(b) - \varepsilon'(b) = 0.$$

Since $\ker(\varepsilon') = \mathrm{im}(\mu')$, there exists $b' \in B_1$ such that $\mu'(b') = b - \alpha_2(a')$. Since $\alpha_1$ is surjective, there exists $a'' \in A_1$ such that $\alpha_1(a'') = b'$. But then

$$\alpha_2(\mu(a'') + a') = (\mu' \circ \alpha_1)(a'') + \alpha_2(a') = \mu'(b') + \alpha_2(a') = b,$$

and we have proved that $\alpha_2$ is surjective. □

**Definition 2.5.** *A short exact sequence* $0 \to A \xrightarrow{\mu} B \xrightarrow{\varepsilon} C \to 0$ *splits if there exists a homomorphism* $\sigma : C \to B$ *with the property that* $\varepsilon \circ \sigma = \mathrm{id}_C$. *The homomorphism* $\sigma$ *is then called a splitting.*

**Remark 2.6.** *For any modules* $A$ *and* $C$, *the short exact sequence* $0 \to A \xrightarrow{\iota_A} A \oplus C \xrightarrow{\pi_C} C \to 0$, *where* $\iota_A(a) = (a, 0)$ *and* $\pi_C((a, c)) = c$, *splits. Conversely, the following also holds:*

**Lemma 2.7.** *If the short exact sequence* $0 \to A \xrightarrow{\mu} B \xrightarrow{\varepsilon} C \to 0$ *splits, then* $B \cong A \oplus B$.

*Proof.* We fix a splitting $\sigma : C \to B$ and define a homomorphism $\psi : A \oplus C \to B$ by setting $\psi((a, c)) := \mu(a) + \sigma(c)$. We then have that $\psi(\iota_A(a)) = \psi((a, 0)) = \mu(a)$ and that $\varepsilon(\psi((a, c))) = \varepsilon(\mu(a)) + \varepsilon(\sigma(c)) = 0 + \mathrm{id}_C(c) = c = \pi_C((a, c))$, where we have used the fact that $\ker(\varepsilon) = \mathrm{im}(\mu)$ so $\varepsilon \circ \mu = 0$. We deduce the existence of a commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{\iota_A} & A \oplus C & \xrightarrow{\pi_C} & C & \longrightarrow & 0 \\ & & {\scriptstyle \mathrm{id}_A}\big\downarrow & & {\scriptstyle \psi}\big\downarrow & & {\scriptstyle \mathrm{id}_C}\big\downarrow & & \\ 0 & \longrightarrow & A & \xrightarrow{\mu} & B & \xrightarrow{\varepsilon} & C & \longrightarrow & 0. \end{array}$$

Since $\mathrm{id}_A$ and $\mathrm{id}_C$ are clearly bijective, Lemma 2.4 implies that $\psi$ is an isomorphism. □

## 3. The group of homomorphisms

For any modules $A$ and $B$, we write $\mathrm{Hom}_R(A, B)$ for the set of homomorphisms from $A$ to $B$. We define a binary operation on $\mathrm{Hom}_R(A, B)$ as follows: given $\phi, \psi \in \mathrm{Hom}_R(A, B)$, we define an element $\phi + \psi$ of $\mathrm{Hom}_R(A, B)$ by the formula

$$(\phi + \psi)(a) := \phi(a) + \psi(a), a \in A.$$

**Lemma 3.1.** *The map $\phi + \psi : A \to B$ is indeed an element of $\mathrm{Hom}_R(A, B)$. Furthermore, this binary operation makes $\mathrm{Hom}_R(A, B)$ into an abelian group (or, equivalently, a $\mathbb{Z}$-module).*

*Proof.* The first assertion of the lemma is straightforward to prove, as is associativity of the binary operation. The identity element of $\mathrm{Hom}_R(A, B)$ with respect to this binary operation is the zero homomorphism given by sending any element of $A$ to the identity element 0 of $B$, and for any $\phi \in \mathrm{Hom}_R(A, B)$, we obtain an inverse by setting $(-\phi)(a) := -\phi(a)$ for every $a \in A$. □

Let $\beta : B_1 \to B_2$ be a homomorphism (of $R$-modules). We define a map

$$\beta_* = \mathrm{Hom}_R(A, \beta) : \mathrm{Hom}_R(A, B_1) \to \mathrm{Hom}_R(A, B_2)$$

by setting $\beta_*(\phi) := \beta \circ \phi$.

**Lemma 3.2.** (1) *$\beta_*$ is a $\mathbb{Z}$-module homomorphism.*
(2) *Given $\beta' : B_2 \to B_3$, we have that $(\beta' \circ \beta)_* = \beta'_* \circ \beta_*$.*
(3) *$(\mathrm{id}_B)_* = \mathrm{id}_{\mathrm{Hom}_R(A,B)}$ where, for any set $S$, $\mathrm{id}_S$ denotes the identity function $S \to S$ (i.e., $\mathrm{id}_S(s) = s$ for all $s \in S$).*

*Proof.* We prove claim (1) by obtaining identities

$$\begin{aligned} \beta_*(\phi + \psi)(a) = \beta((\phi + \psi)(a)) &= \beta(\phi(a) + \psi(a)) = \beta(\phi(a)) + \beta(\psi(a)) \\ &= \beta_*(\phi)(a) + \beta_*(\psi)(a) = (\beta_*(\phi) + \beta_*(\psi))(a). \end{aligned}$$

Claim (2) is clear since

$$(\beta' \circ \beta)_*(\phi) = (\beta' \circ \beta) \circ \phi = \beta' \circ (\beta \circ \phi) = \beta'_*(\beta_*(\phi)) = (\beta'_* \circ \beta_*)(\phi).$$

Claim (3) is clear since $(\mathrm{id}_B)_*(\phi) = \mathrm{id}_B \circ \phi = \phi$, so that $(\mathrm{id}_B)_*$ is the identity map on $\mathrm{Hom}_R(A, B)$, as required. □

**Theorem 3.3.** *Let* $0 \to B_1 \xrightarrow{\mu} B_2 \xrightarrow{\varepsilon} B_3$ *be an exact sequence (of $R$-modules). Then the sequence of $\mathbb{Z}$-modules*

$$0 \to \mathrm{Hom}_R(A, B_1) \xrightarrow{\mu_*} \mathrm{Hom}_R(A, B_2) \xrightarrow{\varepsilon_*} \mathrm{Hom}_R(A, B_3)$$

*is exact for any ($R$-)module $A$.*

*Proof.* We first prove that $\mu_*$ is injective: suppose that $\mu \circ \phi = \mu_*(\phi) = 0 \in \mathrm{Hom}_R(A, B_2)$ for some $\phi \in \mathrm{Hom}_R(A, B_1)$. Then, since $\mu(\phi(a)) = 0$ for every $a \in A$ and $\mu$ is injective, we have that $\phi(a) = 0$ for every $a \in A$, i.e., $\phi = 0$ in $\mathrm{Hom}_R(A, B_1)$, as required.

We now prove that $\mathrm{im}(\mu_*) \subseteq \ker(\varepsilon_*)$, i.e., that $\varepsilon_*(\mu_*(\phi)) = \varepsilon \circ \mu \circ \phi = 0$ for any $\phi \in \mathrm{Hom}_R(A, B_1)$: since $\ker(\varepsilon) = \mathrm{im}(\mu)$, it follows that $\varepsilon(\mu(b)) = 0$ for any $b \in B_1$, and so $(\varepsilon \circ \mu \circ \phi)(a) = \varepsilon(\mu(\phi(a))) = 0$ for any $a \in A$ and any $\phi \in \mathrm{Hom}_R(A, B_1)$.

We next prove that $\ker(\varepsilon_*) \subseteq \mathrm{im}(\mu_*)$: let $\psi \in \mathrm{Hom}_R(A, B_2)$ be such that $\varepsilon_*(\psi) = \varepsilon \circ \psi = 0$. Then for any $a \in A$ we have that $\varepsilon(\psi(a)) = 0$ and since $\ker(\varepsilon) = \mathrm{im}(\mu)$, it follows that for any $a \in A$ there exists $b_a \in B_1$ such that $\mu(b_a) = \psi(a)$ and, furthermore, $b_a$ is the unique element of $B_1$ with this property (because $\mu$ is injective). We may hence define $\phi : A \to B_1$ by setting $\phi(a) := b_a$. We first claim that $\phi$ is actually an element of $\mathrm{Hom}_R(A, B_1)$: indeed, given $a, a' \in A$ and $r \in R$, one has that

$$\begin{aligned}\mu(\phi(a + a')) = \mu(b_{a+a'}) = \psi(a + a') = \psi(a) + \psi(a') &= \mu(b_a) + \mu(b_{a'}) \\ &= \mu(b_a + b_{a'}) = \mu(\phi(a) + \phi(a'))\end{aligned}$$

and that

$$\mu(\phi(ra)) = \mu(b_{ra}) = \psi(ra) = r\psi(a) = r\mu(b_a) = \mu(rb_a) = \mu(r\phi(a))$$

and so, since $\mu$ is injective, that $\phi(a + a') = \phi(a) + \phi(a')$ and that $\phi(ra) = r\phi(a)$. We now simply note that $\mu_*(\phi) = \mu \circ \phi = \psi$, so we have proved that $\ker(\varepsilon_*) \subseteq \mathrm{im}(\mu_*)$.

We may now conclude that the sequence is exact both at $\mathrm{Hom}_R(A, B_1)$ and at $\mathrm{Hom}_R(A, B_2)$, as required. □

**Example 3.4.** *It is not true in general that, if the sequence* $0 \to B_1 \xrightarrow{\mu} B_2 \xrightarrow{\varepsilon} B_3 \to 0$ *is exact (i.e., is a short exact sequence), the induced sequence should also be short exact for any $A$; that is, even if $\varepsilon$ happens to be surjective, $\varepsilon_*$ might not be so. To illustrate this counter-intuitive phenomenon, consider the sequence of $\mathbb{Z}$-modules (so we are taking $R$ to be $\mathbb{Z}$)*

$$0 \to \mathbb{Z} \xrightarrow{\mu} \mathbb{Z} \xrightarrow{\varepsilon} \mathbb{Z}/n\mathbb{Z} \to 0,$$

*where $\mu$ denotes multiplication by an integer $n \neq -1, 0, 1$ and $\varepsilon$ denotes the natural projection. It is easy to see that this sequence is exact. However, the map*

$$\varepsilon_* = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \varepsilon) : \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}) \to \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$$

*(so we are taking $A$ to be $\mathbb{Z}/n\mathbb{Z}$) is not surjective. To see this, one need only note that $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z})$ is a trivial $\mathbb{Z}$-module (indeed, the image under any $\mathbb{Z}$-homomorphism of $\mathbb{Z}/n\mathbb{Z}$ can have at most $n$ elements, but all the $\mathbb{Z}$-submodules of $\mathbb{Z}$ other than the trivial one are infinite, so the zero homomorphism is the only element of $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z})$), while $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$ is a non-trivial $\mathbb{Z}$-module (we have for instance the non-trivial element $\mathrm{id}_{\mathbb{Z}/n\mathbb{Z}} \in \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$). Since a set consisting of just one element cannot surject onto a set containing more than one element, the map $\varepsilon_*$ cannot be surjective.*

## 4. Characterization of projective modules

**Lemma 4.1.** *Let $\alpha : A_1 \oplus A_2 \to B$ be a homomorphism. Then the maps $\alpha_i : A_i \to B$ defined for $i \in \{1, 2\}$ by the formulas $\alpha_1(a_1) := \alpha((a_1, 0))$ for any $a_1 \in A_1$ and $\alpha_2(a_2) := \alpha((0, a_2))$ for any $a_2 \in A_2$ are also homomorphisms.*

**Proposition 4.2.** *A direct sum of modules $P_1 \oplus P_2$ is projective if and only if both $P_1$ and $P_2$ are projective.*

*Proof.* We first assume that both $P_1$ and $P_2$ are projective and proceed to prove that so is $P_1 \oplus P_2$. Suppose given a surjective homomorphism $\varepsilon : B \twoheadrightarrow C$ and a homomorphism $\gamma : P_1 \oplus P_2 \to C$. We define homomorphisms $\gamma_i : P_i \to C$ for $i \in \{1, 2\}$ as in Lemma 4.1. Then, for each such $i$, there exists a homomorphism $\beta_i : P_i \to B$ with the property that $\varepsilon \circ \beta_i = \gamma_i$. We now define a map $\beta : P_1 \oplus P_2 \to B$ by the formula $\beta((p_1, p_2)) := \beta_1(p_1) + \beta_2(p_2)$ is easily shown to be a homomorphism. But

$$\begin{aligned}(\varepsilon \circ \beta)((p_1, p_2)) = \varepsilon(\beta_1(p_1) + \beta_2(p_2)) = \gamma_1(p_1) + \gamma_2(p_2) &= \gamma((p_1, 0)) + \gamma((0, p_2)) \\ &= \gamma((p_1, 0) + (0, p_2)) = \gamma((p_1, p_2))\end{aligned}$$

and so we have proved that $P_1 \oplus P_2$ is projective.

Conversely, we now assume that $P_1 \oplus P_2$ and proceed to prove that $P_1$ is projective, noting that the prove for $P_2$ is completely analogous. Suppose given a surjective homomorphism $\varepsilon : B \twoheadrightarrow C$ and a homomorphism $\gamma : P_1 \to C$. We now define a map $\gamma' : P_1 \oplus P_2 \to C$ by setting $\gamma'((p_1, p_2)) := \gamma(p_1)$ and note that it is clearly a homomorphism. Using the hypothesis, we find that there exists a homomorphism $\beta : P_1 \oplus P_2 \to B$ with the property that $\varepsilon \circ \beta = \gamma'$. But is we now define a homomorphism $\beta_1 : P_1 \to B$ as in Lemma 4.1, we finally have that

$$(\varepsilon \circ \beta_1)(p) = \varepsilon(\beta((p, 0))) = \gamma'((p, 0)) = \gamma(p)$$

and so we have proved that $P_1$ is projective. □

**Remark 4.3.** *The proposition extends to direct sums indexed by arbitrary sets.*

**Theorem 4.4.** *For a module $P$, the following statements are equivalent:*

(1) *$P$ is projective.*

(2) *for every short exact sequence (of R-modules)* $0 \to A \xrightarrow{\mu} B \xrightarrow{\varepsilon} C \to 0$, *the induced sequence of* $\mathbb{Z}$*-modules*

$$0 \to \mathrm{Hom}_R(P, A) \xrightarrow{\mu_*} \mathrm{Hom}_R(P, B) \xrightarrow{\varepsilon_*} \mathrm{Hom}_R(P, C) \to 0$$

*is exact.*

(3) *for any surjective homomorphism* $\varepsilon : B \twoheadrightarrow P$ *there exists a homomorphism* $\beta : P \to B$ *such that* $\varepsilon \circ \beta = \mathrm{id}_P$.

(4) $P$ *is a direct summand in every module of which it is a quotient.*

(5) $P$ *is a direct summand in a free module.*

*Proof.* We first prove that (1) implies (2): by the definition of projective modules, we have that for any $\gamma \in \mathrm{Hom}_R(P, C)$ there exists $\beta \in \mathrm{Hom}_R(P, B)$ such that $\gamma = \varepsilon \circ \beta = \varepsilon_*(\beta)$. We have proved that $\varepsilon_*$ is surjective, or equivalently that the induced sequence is exact at $\mathrm{Hom}_R(P, C)$. Now we may simply note that the sequence is exact by Theorem 3.3.

To prove that (2) implies (3), we simply apply (2) to the short exact sequence $0 \to \ker(\varepsilon) \to B \xrightarrow{\varepsilon} P \to 0$. we deduce that the map $\varepsilon_* : \mathrm{Hom}_R(P, B) \to \mathrm{Hom}_R(P, P)$ is surjective, and hence that there exists a homomorphism $\beta : P \to B$ such that $\varepsilon \circ \beta = \varepsilon_*(\beta) = \mathrm{id}_P$.

To prove that (3) implies (4), we recall that if $B$ is isomorphic to a quotient $B/A$, then we have a short exact sequence $0 \to A \to B \xrightarrow{\varepsilon} P \to 0$ which, by (3), splits. Lemma 2.7 now implies that $P$ is a direct summand in $B$, as required.

To prove that (4) implies (5), we simply have to prove that every module $P$ is a quotient of a free module. Let $S$ be a set of generators of $P$ and define a free module $F := \bigoplus_{s \in S} Rs$. Then the (unique) homomorphism $f : F \to P$ sending each element $(\ldots, 0, \ldots, 0, s, 0, \ldots, 0, \ldots)$ to $s$ is clearly surjective, and $P$ is thus isomorphic to $F/\ker(f)$.

To prove that (5) implies (1), we simply fix a free module $F$ which contains $P$ as a direct summand. Then $F$ is projective by Theorem 1.4 and hence $P$ is projective by Proposition 4.2. $\square$

**Examples 4.5.** (1) *Some of these properties for modules might seem familiar from the theory of vector spaces. This is simply because if R is a field, then every (R-)module is free, hence projective.*

(2) *By combining Example 3.4 and Theorem 4.4, we know that* $\mathbb{Z}/n\mathbb{Z}$ *is not projective as a* $\mathbb{Z}$*-module for any integer* $n \neq -1, 0, 1$. *By the structure theorem for finitely generated abelian groups and Proposition 4.2, we find that a finitely generated* $\mathbb{Z}$*-module is projective if and only if it is free. As we will soon see, this result generalizes to finitely generated modules over any principal ideal domain by simply applying the analogous structure theorem and combining it with Proposition 4.2 and the equivalence of conditions (1) and (4) in Theorem 4.4.*

(3) *Let $p$ and $q$ be distinct primes; it is easy to prove that $\mathbb{Z}/pq\mathbb{Z}$ is isomorphic to $\mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/q\mathbb{Z}$ as a $\mathbb{Z}/pq\mathbb{Z}$-module, so by Proposition 4.2 we find that both $\mathbb{Z}/p\mathbb{Z}$ and $\mathbb{Z}/q\mathbb{Z}$ are projective $\mathbb{Z}/pq\mathbb{Z}$-modules. They are however clearly not free, so the converse of Theorem 1.4 does not hold in general.*

(4) *Submodules of projective modules need not be projective; to construct a counterexample, one may just let $p$ be a prime and prove that the sequence of $\mathbb{Z}/p^2\mathbb{Z}$-modules*

$$0 \to \mathbb{Z}/p\mathbb{Z} \xrightarrow{\mu} \mathbb{Z}/p^2\mathbb{Z} \xrightarrow{\varepsilon} \mathbb{Z}/p\mathbb{Z} \to 0$$

*is exact but does not split. Here $\mu$ sends an element $a + p\mathbb{Z}$ to $a + p^2\mathbb{Z}$ and $\varepsilon$ sends an element $b+p^2\mathbb{Z}$ to $b+p\mathbb{Z}$. So $\mathbb{Z}/p\mathbb{Z}$ identifies via $\mu$ with a submodule of the free, hence projective, $\mathbb{Z}/p^2\mathbb{Z}$-module $\mathbb{Z}/p^2\mathbb{Z}$, but is not exact because if it were the short exact sequence would split by property (3) of Theorem 4.4.*

After working through examples (3) and (4), and noting the contrast with the situation in examples (1) and (2), it is natural to ask over which class of rings are all projective modules free, and over which class of rings are all submodules of projective modules also projective. As one could expect, things work nicely over any principal ideal domain.

**Theorem 4.6.** *If $R$ is a principal ideal domain, then every submodule of a free $R$-module is free.*

*Proof.* The proof of the general case can be found at [1, I,Thm. 5.1] and we do not give it here. However, we note that the result is immediate for submodules of finitely generated free $R$-modules by the structure theorem of finitely generated modules over principal ideal domains. $\square$

**Corollary 4.7.** *Over a principal ideal domain, every projective module is free.*

*Proof.* By Theorem 4.4, every projective module is a direct summand in a free module, and hence must be free itself. $\square$

**Corollary 4.8.** *Over a principal ideal domain, every submodule of a projective module is projective.*

*Proof.* We simply combine Corollary 4.7, Theorem 4.6 and Theorem 1.4. $\square$

## References

[1] P. J. Hilton, U. Stammbach, *A course in homological algebra*, Springer-Verlag, 1971.