§2. Projective and injective modules

Let K be a field and $0 \to U \xrightarrow{f} V \xrightarrow{g} W \to 0$ an exact sequence of K-vectorspaces. This sequence splits: By 1.2 and 1.3 we have to find a linear map $h: W \to V$ such that $g \circ h = id_W$ or a linear map $j: V \to U$ such $j \circ f = id_U$. We construct both maps: $W = 0$ or $U = 0$: clear.
W has a basis $\{w_i \mid i \in I\}$. For each i choose a preimage v_i of w_i under g. Define h by sending the basis element w_i to v_i and linearly extending.
Then $g \circ h(w_i) = g(v_i) = w_i \Rightarrow g \circ h = id_W$.
Now j: f is injective. U has a basis $\{u_\lambda \mid \lambda \in \Lambda\}$ and $\{f(u_\lambda) \mid \lambda \in \Lambda\}$ is a linearly independent set of vectors. Extend it to a basis $\{f(u_\lambda) \mid \lambda \in \Lambda\} \cup \{b_\mu \mid \mu \in M\}$ of V. Define j by sending $f(u_\lambda)$ to u_λ, b_μ to 0, and linearly extending. Then $j \circ f(u_\lambda) = u_\lambda \Rightarrow j \circ f = id_U$.
The constructions of h and j are not the same. We will see in general that the conditions for a sequence to split are different for the starting term and for the end term. The property used for constructing h is easy to generalize:

2.1 Definition: An A-module M is called a **free module** $\Leftrightarrow M \cong \bigoplus_{i \in I} {}_A A$, a direct sum of copies of the regular module ${}_A A$, for some index set I.

In ${}_A A$, the element $1 = 1_A$ is a generator: $A = \{a \cdot 1 \mid a \in A\}$ and it is linearly independent: $\lambda \cdot 1 = 0$ for some $\lambda \in A \Rightarrow \lambda = 0$. So we may call $\{1\}$ a basis of A.
Similarly, $\{1_i \mid i \in I\}$ may be called a basis of $\bigoplus_{i \in I} A$, where 1_i is 1_A in the i-th copy and 0 elsewhere.
Formally (motivated by a characterization of bases of vectorspaces):

2.2 Definition: Let M be an A-module and $S \subset M$ a subset. S is called an A-basis (or just a basis) of $M \Leftrightarrow \forall$ A-modules X $\forall$ set maps $S \xrightarrow{\alpha} X$ $\exists!$ A-module homomorphism $\hat{\alpha}: M \to X$ such that $\alpha = \hat{\alpha}|_S$ (restriction).
M is then called a **free A-module** (on the basis S).

$S=\emptyset$ is allowed. Check that $M=0$ is free on $S=\emptyset$.
If M is free on S and N is free on T and there is a bijection $S \xrightarrow{\varphi} T$, then ${}_A M \cong_A N$. How to find the isomorphism?
Verify that for $A=K$, a field, this definition of basis coincides with the definition used for vector spaces.
$\{1_i\}_{i\in I}$ is a basis of $\bigoplus_{i\in I} A$. Proof?

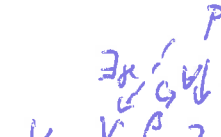
${}_A X$ free and ${}_A Y$ ~~free~~ $\cong_A X \Rightarrow {}_A Y$ free as well. Why?

Consequence: An A-module ${}_A M$ is free $\Leftrightarrow \exists I: {}_A M \cong \bigoplus_{i\in I} A$

Let F be a free module. Then every short exact sequence
$0 \to X \xrightarrow{f} Y \xrightarrow{g} F \to 0$ splits.
h can be constructed in the same way as for vectorspaces, by choosing a basis $\{b_i\}_{i\in I}$ of F and mapping b_i to a preimage under g.

Looks easy, just as in linear algebra. There is, however, a problem: Modules are not usually free. For instance, for $A=K[x]$: $M=K[x]$ is free, $M=K[x]/\langle f(x)\rangle$ is free $\Leftrightarrow f(x)=0$. Why?
So there may be modules without basis such that each ses ending there still splits. And there are!
We define these modules by a stronger property, a "lifting property" and then we prove these are the modules we are looking for. And we will precisely describe them.

2.3 Definition: An A-module P is projective $:\Leftrightarrow$ $\forall$ surjective A-module homomorphisms $\beta: Y \to Z$ and all homomorphisms $\alpha: P \to Z$ $\exists \rho: P \to Y$, a homomorphism satisfying $\alpha = \beta \circ \rho$.



(ρ is a "lift" or a lifting of α along β)

y need not be unique (choose $z=0$ to find a counterexample)

Notation: A-Free are the free A-modules

A-free are the finitely generated free A-modules

A-Proj are the projective A-modules

A-proj are the finitely generated projective A-modules

(M finitely generated means: $\exists m_1,\dots,m_n \in M\ \forall m\in M\ \exists a_1,\dots,a_n\in A$: $m=\sum_{i=1}^{n} a_i m_i$)

This notation can be adjusted to right modules: Free-A, proj-A, etc.

More notation: $\mathrm{Add}({}_A A)(M) = \{{}_A X : {}_A X \text{ is a direct summand of } \bigoplus_{i\in I} M, \text{ for some } I\}$

$\mathrm{add}({}_A M) = \{{}_A Y : {}_A Y \text{ is a direct summand of } M^n, \text{ for some } n\in\mathbb{N}\}$

2.4 Theorem: A-Proj $= \mathrm{Add}({}_A A)$ and A-proj $= \mathrm{add}\, A$.

In other words: the projective A-modules are exactly the direct summands of the free A-modules.

Proof: It is enough to prove A-Proj $= \mathrm{Add}({}_A A)$

Let P be projective. Like every module, P is a quotient of a free module,

$\exists$ surjection $\varphi: \bigoplus_{i\in I} A \to P \to 0$ for some I

(choose for instance $I=P$

and send the basis vector b_{p_0} (entry 1 at index p_0, 0 elsewhere to $p_0\in P$)

Now consider the diagram

$$\begin{array}{ccccc} & & & & P \\ & & \exists\Psi: & \swarrow & \downarrow \mathrm{id}_P \\ \bigoplus_{i\in I} A & \xrightarrow{\varphi} & P & \to & 0 \end{array}$$

Ψ exists as P is projective and $\varphi\circ\Psi = \mathrm{id}_P$

This implies that P is a direct summand of $\bigoplus_{i\in I} A$ (use that $\Psi\circ\varphi$ is an idempotent in $\mathrm{End}_A(\bigoplus_{i\in I} A)$, compare for instance there cap on Unique decompositions)

Conversely, any direct sum $\bigoplus_{i\in I} A$ (any I) is free, hence projective, since we can define homomorphisms on the basis. We have to check that any direct summand P of $\bigoplus_{i\in I} A$ (notation: $P \mid \bigoplus_{i\in I} A$) is projective.

Write $\bigoplus_{i\in I} A = P \oplus Q$ (the existence of the complement Q can be shown by using idempotents in $\mathrm{End}_A(\bigoplus_{i\in I} A) =: P = e(\bigoplus_{i\in I} A)$, then set $Q := (1-e)(\bigoplus_{i\in I} A)$)

We have to find γ in $\exists ?\gamma$:

$$\begin{array}{ccccc} & & P & & \\ & \swarrow^{\gamma} & \downarrow \alpha & & \\ Y & \xrightarrow{\beta} & Z & \to 0 & \end{array} \qquad (*)$$

First look instead at

$$\begin{array}{ccccc} P\oplus Q = \bigoplus_{i\in I} A \text{ (free)} & & & & \\ \exists (\gamma_1,\gamma_2) \swarrow & \hookrightarrow & \downarrow (\alpha, 0) & & \\ Y & \xrightarrow{\beta} & Z & \to 0 & \end{array}$$

Here $\exists (\gamma_1,\gamma_2): P\oplus Q \to Y$ such that $\beta \circ (\gamma_1,\gamma_2) = (\alpha, 0)$. Then $\beta\circ\gamma_1 = \alpha$.

$\Rightarrow$ Set $\gamma := \gamma_1$ and $(*)$ works. □

Now we know R A-Proj and A-proj. But we still have to show these are the modules we were looking for in the beginning.

2.5 Theorem: A module P is projective $\Leftrightarrow$ every short exact sequence ending at P, $0 \to X \xrightarrow{f} Y \xrightarrow{g} P \to 0$, splits.

In other words, P projective $\Leftrightarrow$ $\mathrm{Ext}_A(P, -) = 0$.

this means: $\mathrm{Ext}_A(P, X) = 0 \ \forall X$

Proof: Let P be projective and $0 \to X \xrightarrow{f} Y \xrightarrow{g} P \to 0$ exact, and form the diagram

$$\begin{array}{ccc} & & P \\ & \overset{\exists \gamma}{\nearrow} & \uparrow \mathrm{id}_P =: \alpha \\ Y & \xrightarrow{g} & P \end{array}$$

Then $h := \gamma$ shows the sequence splits.

Conversely, suppose every ses ending in P splits. Write P as quotient of a free module and thus form the ses $0 \to \ker(u) \to \bigoplus_{i\in I} A \xrightarrow{q} P \to 0$

This splits and therefore P is a direct summand of $\bigoplus_{i\in I} A \Rightarrow P$ is projective. □

For a field k every module is projective. Are there other k-algebras with this property?

2.6 Corollary: For a k-algebra A, finite dimensional over k, the following are equivalent:

(a) Every finite dimensional A-module is projective.

(b) Every finite dimensional A-module is semisimple, ie a finite direct sum of simple A-modules.

(c) ${}_A A$ is semisimple.

(d) A is a semisimple algebra.

(e) Every short exact sequence in A-mod splits, i.e $Ext^1_A(-,-) = 0$ on A-mod.

Proof: For (c) $\Leftrightarrow$ (d) see the recap material on semisimple algebras.

By the existence of composition series (see the recap material on the theorem of Jordan-Hölder), (e) implies (c).

By Schur's lemma, ses of semisimple modules split, thus (c) $\Rightarrow$ (e).

(b) $\Rightarrow$ (c) is clear, the converse follows by going through (e).

(e) implies (a) by 2.5.

(a) implies (e) also by 2.5 $\square$

Try to work out the details of this proof, thus testing your knowledge on basic representation theory. If necessary, we will discuss the details.

List some examples of algebras
that are known to be semisimple

and some examples of algebras
that are not semisimple.

There is still something left to be done: We need to find examples that are projective modules, but not free modules (otherwise we should try to prove that projective = free).

Let $1_A = e_1 + \dots + e_n$ be a decomposition of 1_A into a sum of pairwise orthogonal idempotents, i.e. $e_i^2 = e_i$ for $i = 1, \dots, n$ and $e_i e_j = 0$ for $i \neq j$.
(In other words $e_i e_j = \delta_{ij} e_i$, δ_{ij} = Kronecker delta).
Then ${}_A A = {}_A Ae_1 \oplus \dots \oplus {}_A Ae_n$. ($Ae_i = \{ae_i : a \in A\}$)

Compare with the case of idempotents in the (recap on) the Krull-Remak-Schmidt Theorem.

Prove this statement:

- each Ae_i is a left module
- $Ae_i \cap Ae_j = 0$ for $i \neq j$
- $A = Ae_1 + \dots + Ae_n$

When $n \geq 2$ and all $e_i \neq 0$, the Ae_i are proper submodules of Ae_i, hence have smaller K-dimension than A. $\Rightarrow$ Ae_i are projective, but not free.

Give explicit examples of non-trivial decompositions of ${}_A A$:

- $A = Mat(n \times n, K)$

- $A = KQ$, Q a quiver

- A = upper triangular $n \times n$-matrices, or another algebra of matrices

Now we have solved half of the problem stated at the beginning: We know the modules P such that $\mathrm{Ext}^1_A(P,-)=0$, whatever we plug in as $-$ in the second place. Now we face the second half of the question: For which modules I is $\mathrm{Ext}^1_A(-,I)=0$, whatever we plug in as $-$ in the first place? We don't know any I (apart from $I=0$).

But there should be some symmetry in the situation. Recall for instance Lemma 1.3, which states two equivalent conditions on a sequence to split: one on the existence of h on the right hand side, and the other one on the existence of j on the left hand side.

How can we (tutor) change left and right hand side of ses?

Recall a useful tool from linear algebra! Let K be a field and V a vector space. Then $DV = \mathrm{Hom}_K(V,K)$ (= V^*) is a vector space, too, the dual space. When $\dim V < \infty$, $V^{**} = D(DV)$ is isomorphic to V by the evaluation map:

$$V \xrightarrow{ev} V^{**} = \mathrm{Hom}_K(V^*, K)$$
$$v \longmapsto ev(v): f \in V^* \longmapsto f(v)$$

do you remember the proof?

For a linear map $\varphi: V \to W$ there is a dual map $\varphi^*: W^* \to V^*$ (after choosing bases, this can be represented by the transposed matrix of the matrix representing φ).

$$\begin{array}{ccc} W^* & \to & V^* \\ \Psi & & \Psi \\ f & \mapsto & f\circ\varphi \end{array}$$

When φ is injective, then $\varphi^* = D\varphi$ is surjective, and vice versa. This is exactly what we want! Let $0 \to U \xrightarrow{f} V \xrightarrow{g} W \to 0$ be a ses of (findim) vector spaces. Then $0 \to DW \xrightarrow{Dg} DV \xrightarrow{Df} DU \to 0$ is a ses too. Check

Can we do the same with A-modules, at least finite dimensional ones, where A is an algebra over a field K? Let ${}_AM$ be a left A-module. Then M is a K-vector space, too, and $D(M) = \mathrm{Hom}_K(M, K)$ (= M^*, dual) also is a K-vector space. Does $D(M)$ have an A-module structure?

Let $f \in D(M)$, ie $f: M \to K$ is K-linear. We have to define a times f for $a \in A$ and check this is an A-module action. There is only one reasonable way: Send $m \in M$ to $f(am) \in K$, since m is the only element here we can multiply by a – while $f(m) \in K$, which has no A-structure.

For $a, b \in A$: $f(ab\cdot m)$ means: first multiply m by b and then multiply the result by a, and then apply f.
This suggests a right module structure. More precisely:
For $a \in A$, $f \in D(M)$ set $fa : m \longmapsto f(am)$. This is k-linear, hence $fa \in D(M)$.
For $b \in A$, then $(fa)b : m \longmapsto (fa)(bm) = f(abm)$,
and $f(ab) : m \longmapsto f((ab)m)$ $=$

Result: k-duality D sends a left A-module M to a right A-module $D(M)$, and, of course, a right A-module N to a left A-module $D(N)$. When these modules are finite dimensional, then $D(D(M)) \simeq M$ and $D(D(N)) \simeq N$.
When $\varphi : M_1 \to M_2$ is a left module homomorphism, the dual map $D\varphi : DM_2 \to DM_1$ is a right module homomorphism:

$f : M_2 \to k$ $\quad$ $(D\varphi)(f) : m_1 \longmapsto f(\varphi(m_1))$, by definition

$\Rightarrow (D\varphi)(fa) : m_1 \longmapsto fa(\varphi(m_1)) = f(a\varphi(m_1))$

and $(D\varphi)(f) : am_1 \longmapsto f(\varphi(am_1)) = \varphi$ homom of left A-modules

$\Rightarrow ((D\varphi)(f))a : m_1 \longmapsto (D(\varphi)(f))(am_1) = (D\varphi)(fa)(m_1)$,

and similarly for right modules.

To summarise: k-duality $\overset{D=}{\mathrm{Hom}_k(-,k)}$ sends left A-modules to right A-modules and vice versa, and left A-module homomorphisms to right A-module homomorphisms, and vice versa. Applying D twice returns the module we started with, up to isomorphism, and the same homomorphism.

Since an A-module homomorphism $\varphi : M_1 \to M_2$ is k-linear, we get for free:
φ injective $\Leftrightarrow D\varphi$ surjective and φ surjective $\Leftrightarrow D\varphi$ injective.
More generally: $D(\ker\varphi) = \mathrm{coker}(D\varphi)$ and $D(\mathrm{coker}\,\varphi) \simeq \ker(D\varphi)$.
$\Rightarrow$ If $0 \to M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \to 0$ is a ses of left A-modules, then
$0 \to DM_3 \xrightarrow{Dg} DM_2 \xrightarrow{Df} DM_1 \to 0$ is a ses of right A-modules, and vice versa. And one sequence splits iff the other one splits. Check some of these assertions directly, if you don't feel comfortable with dualities.

This tells us: $Ext^1({}_AX, {}_AY) \overset{\text{vector space}}{\cong} Ext^1((DX)_A, (DY)_A)$

$\Rightarrow Ext^1({}_AP, -) = 0 \Leftrightarrow Ext^1(D(-)_A, D(P)_A) = 0$

$\Uparrow$ $\Downarrow$

P projective $\Rightarrow$ P projective

2.7 Corollary: $Ext^1_A(-, {}_AI) = 0 \Leftrightarrow D(I)$ is a projective right A-module.

Examples of such I: $D(A_A)$, $D(eA_A)$ for $e = e^2 \in A$.

Such modules I are called injective. The general definition is as follows:

2.8 Definition: An A-module I is injective $:\Leftrightarrow \forall$ injective A-module homomorphisms $\beta: X \to Y$ and all homomorphisms $\alpha: X \to I$ $\exists$ homomorphism $\gamma: Y \to I$ such that $\alpha = \gamma \circ \beta$

$$\begin{array}{ccccc} 0 & \to & X & \xrightarrow{\beta} & Y \\ & & \downarrow{\scriptstyle \alpha} & \swarrow{\scriptstyle \exists \gamma} & \\ & & I & & \end{array}$$

(This is "dual" to 2.3)

2.9 Corollary: For a finite dimensional $\mathbb{K}$-algebra A and finite dimensional A-modules, the following statements are equivalent:

(a) ${}_AP$ is projective

(b) $D({}_AP) = I_A$ is injective

(c) Every short exact sequence ending in P splits.

(d) Every short exact sequence starting in I splits.

We don't need to know more, but generally speaking this is not yet a satisfactory answer, since it restricts to finite dimensional modules over finite dimensional algebras. Projective modules exist over any ring, since free modules exist. What about injective modules? They also exist in general.

Idea of an approach: Every ring is a $\mathbb{Z}$-algebra. Thus we should first find injective $\mathbb{Z}$-modules.

A useful example of an injective abelian group is $\mathbb{Q}/\mathbb{Z}$.

More generally, a module I over a principal ideal domain is injective iff it is divisible. Divisible means: $r \cdot I = I \ \forall r \in R, r \neq 0$.
The $\mathbb{K}$-duality $D = \mathrm{Hom}_{\mathbb{K}}(-, \mathbb{K})$ in general gets replaced by $\mathrm{Hom}_{\mathbb{Z}}(-, \mathbb{Q}/\mathbb{Z})$ and applying it to projective modules yields injective modules.

An important fact is: There are enough projective modules and enough injective modules in the following sense:
Let M be any module. Then there exist ~~P proj~~ P projective (for instance free) and $\alpha: P \to M$ surjective. And there exists I injective and $\beta: M \to I$ injective (as a map).
So, every module is a quotient of a projective module and a submodule of an injective module.