Lecture Notes for the course

Representation Theory

Part I

Francesca Mantese
Master Degree in Mathematics
Università di Verona, 2014/2015

These notes are based on the following books:
F. W. Anderson, K. R. Fuller , *Rings and categories of modules*, second ed., Springer, New York, 1992;
B. Stenström , *Rings of quotients*, Springer-Verlag (1975)
M. Auslander, I. Reiten, S. O. Smalø, *Representation theory of artin algebras*, Cambridge University Press (1994).

1. Rings and Modules

Recall that a *ring* is a system $(R, +, \cdot, 0, 1)$ consisting of a set R, two binary operations, addition $(+)$ and multiplication $(\cdot)$, and two elements $0 \neq 1$ of R, such that $(R, +, 0)$ is an abelian group, $(R, \cdot, 1)$ is a monoid (i.e., a semigroup with identity 1) and multiplication is left and right distributive over addition. A ring whose multiplicative structure is abelian is called a *commutative ring*.

Example 1.1. (1) $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are commutative rings.
(2) Let K be a field; the ring $K[x_1, \dots, x_n]$ of polynomials in the indeterminates $x_1, \dots, x_n$ is a commutative ring.
(3) Let K be a field; consider the ring $R = M_n(K)$ of $n \times n$-matrices with coefficients in K with the usual "rows times columns" product. Then R is a non-commutative ring

Definition 1.2. *A left R-module is an abelian group M togheter with a map $R \times M \to M$, $(r, m) \mapsto rm$, such that for any $r, s \in R$ and any $x, y \in M$*

M1 $r(x + y) = rx + ry$
M2 $(r + s) = rx + sx$
M3 $(rs)x = r(sx)$
M4 $1x = x$

We write ${}_RM$ to indicate that M is a left R-module.

Example 1.3. (1) Any abelian group G is a left $\mathbb{Z}$-module by defining, for any $x \in G$ and $n > 0$, $nx = \underbrace{x + \cdots + x}_{n\ times}$.
(2) Given a field K, any vector space V over K is a left K-module.
(3) Let R be the matrix ring $M_n(K)$ and consider the vector space $V = K^n$. Given a matrix A and a vector $v \in V$, let Av the usual "rows times columns" product. Then V is a left R-module.
(4) Any ring R is a left R-module, by using the left multiplication of R on itself. It is called the *regular* module.
(5) Consider the zero element of the ring R. Then the abelian group $\{0\}$ is trivially a left R-module.

Remark 1.4. Consider M an abelian group and $\mathrm{End}^l(M)$ the ring of the endomorphism of M acting on the left (i.e. $fg(x) = f(g(x))$. A *representation* of R in $\mathrm{End}^l(M)$ is a homomorphism of ring

$$\lambda : R \to \mathrm{End}^l(M), \qquad r \mapsto \lambda(r)$$

From the properties of ring homomorphisms it follows that for any $r, s \in R$ and $x, y \in M$

(1) $\lambda(r)(x + y) = \lambda(r)x + \lambda(r)y$
(2) $\lambda(r + s)x = \lambda(r)x + \lambda(s)x$
(3) $\lambda(rs)x = \lambda(r)(\lambda(s)x)$
(4) $\lambda(1)x = x$

In other words, we can consider $\lambda(r)$ acting on the elements of M as a left multiplication by the element $r \in R$: then we can define $rx := \lambda(r)x$, and this gives a structure of left R-module on M. Conversely, to any left R-module M, we can associate a representation of R in $\mathrm{End}^l(M)$, by defining $\lambda(r) := rx$.

Similarly, we define right R-modules:

Definition 1.5. *A right R-module is an abelian group M togheter with a map $M \times R \to M$, $(m, r) \mapsto mr$, such that for any $r, s \in R$ and any $x, y \in M$*

M1 $(x + y)r = xr + yr$
M2 $x(r + s) = xr + xs$
M3 $x(rs) = (xr)s$
M4 $x1 = x$

We write M_R to indicate that M is a right R-module.

For the connection between right modules and representations see Exercise 3.8.

If R is a commutative ring, then left R-modules and right R-modules coincide. Indeed, given a left R-module M with the map $R \times M \to M$ $(r,m) \mapsto rm$, we can define a map $M \times R \to M$ $(m,r) \mapsto mr := rm$. This map satisfies the axioms of Definition 1.5 (Verify!) and so M is also a right R-module. The crucial point is that, in the third axiom, since R is commutative we have $x(rs) = (rs)x = (sr)x = s(rx) = (rx)s = (xr)s$.

Example 1.6. Consider the ring $R = M_n(K)$ and V the vector space of the columns $M_{n\times 1}(K)$. This is in a obvious way a left R-module but not a right R-module. Similarly, the vector space of the rows $M_{1\times n}(K)$ is a right R-module but not a left R-module.

Exercise 1.7. Show that given ${}_RM$, for any $x \in M$ and $r \in R$, we have

(1) $r0 = 0$
(2) $0x = 0$
(3) $r(-x) = (-r)x = -(rx)$

Definition 1.8. *Let ${}_RM$ be a left R-module. A subset L of M is a* submodule *of M if L is a subgroup of M and $rx \in L$ for any $r \in R$ and $x \in L$ (i.e. L is a left R-module under operations inherit from M). We write $L \leq M$.*

Example 1.9.

(1) Let G be a $\mathbb{Z}$-module. The submodules of G are exactly the subgroups of G.
(2) Let K a field and V a K-module. The submodules of V are exactly the vector subspace of K.
(3) Let R a ring. The submodules of the left R-module ${}_RR$ are the left ideals of R. The submodules of the right R-module R_R are the right ideals of R.

Definition 1.10. *Let ${}_RM$ be a left R-module and $L \leq M$. The* quotient module *M/L is the quotient abelian group together with the map $R \times M/L \to M/L$ given by $(r, \overline{x}) \mapsto \overline{rx}$.*

Remark 1.11. The map $R \times M/L \to M/L$ given by $(r, \overline{x}) \mapsto \overline{rx}$ is well-defined, since if $\overline{x} = \overline{y}$ then $x - y \in L$ and hence $r(x-y) = rx - ry \in L$, that is $\overline{rx} = \overline{ry}$.

In this part of the course we mainly deal with left modules. So, in the following, unless otherwise is stated, with *module* we always mean *left module*.

2. Homomorphisms of modules

Definition 2.1. *Let ${}_RM$ and ${}_RN$ be R-modules. A map $f : M \to N$ is a* homomorphism *if $f(rx + sy) = rf(x) + sf(y)$ for any $x, y \in M$ and $r, s \in R$.*

Remark 2.2.

(1) From the definition it follows that $f(0) = 0$.
(2) Clearly if f and g are homomorphisms from M to N, also $f + g$ is a homomorphism. Since the zero map is obviously a homomorphism, the set $\mathrm{Hom}_R(M,N) = \{f | f : M \to N \text{ is a homomorphism}\}$ is an abelian group.
(3) If $f : M \to N$ and $g : N \to L$ are homomorphisms, then $gf : M \to L$ is a homomorphism. Thus the abelian group $\mathrm{End}_R(M) = \{f | f : M \to M \text{ is a homomorphism}\}$ has a natural structure of ring, called the *ring of endomorphisms of M*. The identity homomorphism $\mathrm{id}_M : M \to M$, $m \mapsto m$, is the unity of the ring.

Definition 2.3. *Given a homomorphism $f \in \mathrm{Hom}_R(M,N)$, the* kernel *of f is the set $\mathrm{Ker}\, f = \{x \in M | f(x) = 0\}$. The* image *of f is the set $\mathrm{Im}\, f = \{y \in N | y = f(x) \text{ for } x \in M\}$.*

It is easy to verify that $\mathrm{Ker}\, f \leq M$ and $\mathrm{Im}\, f \leq N$. Thus we can define the *cokernel* of f as the quotient module $\mathrm{Coker}\, f = N/\,\mathrm{Im}\, f$.

A homomorphism $f \in \mathrm{Hom}_R(M,N)$ is called a *monomorphism* if $\mathrm{Ker}\, f = 0$. f is called an *epimorphism* if $\mathrm{Im}\, f = N$. f is called *isomorphism* if it is both a monomorphism and an epimorphism. If f is an isomorphism we write $M \cong N$.

Remark 2.4.

(1) For any submodule $L \leq M$ there is a canonical monomorphism $i : L \to M$, which is the usual inclusion, and a canonical epimorphism $p : M \to M/N$ which is the usual quotient map.
(2) For any M the trivial map $0 \to M$, $0 \mapsto 0$, is a mono. The trivial map $M \to 0$, $m \mapsto 0$, is an epi.

(3) The monomorphisms, the epimorphisms and the isomorphisms are exactly the injective, surjective and bijective homomorphisms.

Exercise 2.5. Show that $f \in \operatorname{Hom}_R(M, N)$ is an isomorphism if and only if there exist $g \in \operatorname{Hom}_R(N, M)$ such that $gf = \mathrm{id}_M$ and $fg = \mathrm{id}_N$. In such a case g is unique. (We usually denote g as f^{-1}).

Proposition 2.6. *Any $f \in \operatorname{Hom}_R(M, N)$ induces an isomorphism $M/\operatorname{Ker} f \cong \operatorname{Im} f$.*

Proof. The induced map $M/\operatorname{Ker} f \to \operatorname{Im} f$, $\overline{m} \mapsto f(m)$ is a homomorphism. Moreover it is clearly a mono and an epi. □

The usual homomorphism theorems which hold for groups hold also for homomorphisms of modules.

Proposition 2.7. (1) *If $L \leq N \leq M$, then $(M/L)/(N/L) \cong M/L$.*
(2) *If $L, N \leq M$, denote by $L + N = \{m \in M | m = l + n \text{ for } l \in L \text{ and } n \in N\}$. Then $L + N$ is a submodule of M and $(L + N)/N \cong N/(N \cap L)$.*

Exercise 2.8. Prove the previous Proposition.

3. Exact Sequences

Definition 3.1. *A sequence of homomorphisms of R-modules*

$$\cdots \to M_{i-1} \xrightarrow{f_{i-1}} M_i \xrightarrow{f_i} M_{i+1} \xrightarrow{f_{i+1}} \cdots$$

is called exact *if $\operatorname{Ker} f_i = \operatorname{Im} f_{i-1}$ for any i.*
An exact sequence of the form $0 \to M_1 \to M_2 \to M_3 \to 0$ is called a short exact sequence

Observe that if $L \leq M$, then the sequence $0 \to L \xrightarrow{i} M \xrightarrow{p} M/L \to 0$, where i and p are the canonical inclusion and quotient homomorphisms, is short exact (Verify!) Conversely, if $0 \to M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \to 0$ is a short exact sequence, then f is a mono, g is an epi, and $M_3 \cong \operatorname{Coker} f$ (Verify!).

The following result is very useful:

Proposition 3.2. *Consider the commutative diagram with exact rows*

$$\begin{tikzcd}
0 \arrow[r] & L \arrow[r, "f"] \arrow[d, "\alpha"] & M \arrow[r, "g"] \arrow[d, "\beta"] & N \arrow[r] \arrow[d, "\gamma"] & 0 \\
0 \arrow[r] & L' \arrow[r, "f'"] & M' \arrow[r, "g'"] & N' \arrow[r] & 0
\end{tikzcd}$$

If α and γ are monomorphisms (epimorphims, or isomorphisms, respectively), then so is β

Proof. (1) Suppose α and γ are monomorphisms and let m such that $\beta(m) = 0$. Then $\gamma(g(m)) = 0$ and so $m \in \operatorname{Ker} g = \operatorname{Im} f$. Hence $m = f(l)$, $l \in L$ and $\beta(m) = \beta(f(l)) = f'(\alpha(l)) = 0$. Since f' and α are mono, we conclude $l = 0$ and so $m = 0$.

(2) Suppose α and γ are epimorphisms and let $m' \in M'$. Then $g'(m') = \gamma(g(m))$, so $g'(m') = g(\beta(m))$; hence $m' - \beta(m) \in \operatorname{Ker} g' = \operatorname{Im} f'$ and so $m' - \beta(m) = f'(l')$, $l' \in L'$. Let $l \in L$ such that $l' = \alpha(l)$: then $m' - \beta(m) = f'(\alpha(l)) = \beta(f(l))$ and so we conclude $m' = \beta(m - f(l))$.

□

Exercises

Exercise 3.3. Let ${}_RM$ be a R-module and ${}_RR$ the regular module. Consider the abelian group $\operatorname{Hom}_R(R, M)$ and the map $\varphi : \operatorname{Hom}_R(R, M) \to M$, $f \mapsto f(1)$. Verify that φ is an isomorphism of $\mathbb{Z}$-modules.

Exercise 3.4. Let $\varphi : S \to R$ a ring homomorphism. Show that any left R-module M is also a left S-modules, by the map $S \times M \to M$, $(s, m) \mapsto \varphi(s)m$.

Exercise 3.5. Let ${}_RM$ and define $\operatorname{Ann}_R(M) = \{r \in R | rm = 0 \text{ for any } m \in M\}$. M is called *faithful* if $\operatorname{Ann}_R(M) = 0$. Verify that $\operatorname{Ann}_R(M)$ is a two-sided ideal of R. Verify that M has a natural structure of $R/\operatorname{Ann}_R(M)$-module, given by the map $R/\operatorname{Ann}_R(M) \times M \to M$, $(\overline{r}, m) \mapsto rm$. Verify that M over $R/\operatorname{Ann}_R(M)$ is a faithful module.

Exercise 3.6. Let f be a homomorphism of R-modules.
Show that f is a mono if and only if $fg = 0$ implies $g = 0$.
Show f is an epi if and only if $gf = 0$ implies $g = 0$

Exercise 3.7. Consider the ring $R = \begin{pmatrix} K & K \\ 0 & K \end{pmatrix}$. Show that $P_1 = \{\begin{pmatrix} k & 0 \\ 0 & 0 \end{pmatrix} | \ k \in K\}$ and $P_2 = \{\begin{pmatrix} 0 & k_1 \\ 0 & k_2 \end{pmatrix} | \ k_1, k_2 \in K\}$ are left submodules of ${}_RR$. Show that $Q_1 = \{\begin{pmatrix} k_1 & k_2 \\ 0 & 0 \end{pmatrix} | \ k_1, k_2 \in K\}$ and $Q_2 = \{\begin{pmatrix} 0 & 0 \\ 0 & k \end{pmatrix} | \ k \in K\}$ are right submodules of R_R

Exercise 3.8. Consider M an abelian group and $\operatorname{End}^r(M)$ the ring of the endomorphism of M acting on the right (i.e. $(x)fg = ((x)f)g$. Show that any representation of R in $\operatorname{End}^r(M)$ corresponds to a right R-module M_R.

4. Sums and products of modules

Let I be a set and $\{M_i\}_{i\in I}$ a family of R-modules. The cartesian product $\prod_I M_i = \{(x_i)|x_i \in M_i\}$ has a natural structure of left R-module, by defining the operations component-wise:

$$(x_i)_{i\in I} + (y_i)_{i\in I} = (x_i + y_i)_{i\in I}, \quad r(x_i)_{i\in I} = (rx_i)_{i\in I}.$$

This module is called the *direct product* of the modules M_i. It contains a submodule

$$\bigoplus_I M_i = \{(x_i)|x_i \in M_i \text{ and } x_i = 0 \text{ for almost all } i \in I\}$$

Recall that "almost all" means "except for a finite number". The module $\oplus_I M_i$ is called the *direct sum* of the modules M_i. Clearly if I is a finite set then $\prod_I M_i = \{(x_i)|x_i \in M_i\} = \oplus_I M_i$. For any component $j \in I$ there are canonical homomorphisms

$$\prod_I M_i \to M_j \ , \ (x_i)_{i\in I} \mapsto x_j \quad \text{ and } \quad M_j \to \prod_I M_i \ , \ x_j \mapsto (0, 0, \dots, x_j, 0, \dots, 0)$$

called the *projection* on the j^{th}-component and the *injection* of the j^{th}-component. They are epimorphisms and monomorphism, respectively, for any $j \in I$. The same is true for $\oplus_I M_i$.

When $M_i = M$ for any $i \in I$, we use the following notations

$$\prod_I M_i = M^I, \qquad \bigoplus_I M_i = M^{(I)}, \qquad \text{and if } \ I = \{1, \dots, n\}, \ \oplus_I M_i = M^n$$

Let $_RM$ be a module and $\{M_i\}_{i\in I}$ a family of submodules of M. We define the *sum* of the M_i as the module

$$\sum_I M_i = \{\sum_{i\in I} x_i | x_i \in M_i \text{ and } x_i = 0 \text{ for almost all } i \in I\}.$$

Clearly $\sum_I M_i \leq M$ and it is the smallest submodule of M containing all the M_i. (Notice that in the definition of $\sum_I M_i$ we need almost all the components to be zero in order to define properly the sum of elements of M).

Remark 4.1. Let $_RM$ be a module and $\{M_i\}_{i\in I}$ a family of submodules of M. Following the previous definitions we can construct both the module $\oplus_I M_i$ and module $\sum_I M_i$ (which is a submodule of M). We can define a homomorphism

$$\alpha : \oplus_I M_i \to M, \quad (x_i)_{i\in I} \mapsto \sum_{i\in I} x_i.$$

Then $\operatorname{Im}\alpha = \sum_I M_i$. If α is a monomorphism, then $\oplus_I M_i \cong \sum_I M_i$ and we say that the module $\sum_I M_i$ is the *(internal) direct sums* of its submodules M_i. Often we omit the word "internal" and if $M = \sum_I M_i$ and α is an isomorphism, we say that M is the direct sums of the submodules M_i and we write $M = \oplus_I M_i$.

5. Split exact sequences

If L and N are R-modules, there is a short exact sequence, called *split*,

$$0 \to L \xrightarrow{i_L} L \oplus N \xrightarrow{\pi_N} N \to 0, \text{ with } i_L(l) = (l, 0) \ \ \pi_N(l, n) = n, \quad \text{for any } l \in L, n \in N.$$

More generally:

Definition 5.1. *A short exact sequence* $0 \to L \xrightarrow{f} M \xrightarrow{g} N \to 0$ *is said to be* split *if there is an isomorphism* $M \cong L \oplus N$ *such that the diagram*

$$\begin{tikzcd}
0 \arrow[r] & L \arrow[r, "f"] \arrow[d, equal] & M \arrow[r, "g"] \arrow[d, "\alpha", "\cong"'] & N \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & L \arrow[r, "i_L"] & L \oplus N \arrow[r, "\pi_N"] & N \arrow[r] & 0
\end{tikzcd}$$

commutes.

Proposition 5.2. *The following properties of an exact sequence* $0 \to L \xrightarrow{f} M \xrightarrow{g} N \to 0$ *are equivalent:*

(1) *the sequence is split*
(2) *there exists a homomorhism* $\varphi : M \to L$ *such that* $\varphi f = \mathrm{id}_L$
(3) *there exists a homomorhism* $\psi : N \to M$ *such that* $g\psi = \mathrm{id}_N$

Proof. $1 \Rightarrow 2$. Since the sequence splits, then there exists α as in Definition 5.1. Let $\varphi = \pi_L \circ \alpha$. So for any $l \in L$ $\varphi f(l) = \pi_L \alpha f(l) = \pi_L(l, 0) = l$.
$1 \Rightarrow 3$ Similar (Verify!)
$2 \Rightarrow 1$. Define $\alpha : M \to L \oplus N$, $m \mapsto (\varphi(m), g(m))$. Since $\alpha f(l) = (\varphi(f(l)), g(f(l))) = (l, 0)$ and $\pi_N \alpha(m) = g(m)$ we get that the diagram

$$\begin{tikzcd}
0 \arrow[r] & L \arrow[r, "f"] \arrow[d, equal] & M \arrow[r, "g"] \arrow[d, "\alpha"] & N \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & L \arrow[r, "i_L"] & L \oplus N \arrow[r, "\pi_N"] & N \arrow[r] & 0
\end{tikzcd}$$

commutes. Finally, by Proposition 3.2, we conclude that α is an isomorphism.
$2 \Rightarrow 3$ Similar (Verify!) □

Definition 5.3. *Given* ${}_R L \leq_R M$*,* L *is a* direct summand *of* M *if there exists a submodule* ${}_R N \leq_R M$ *such that* M *is the direct sum of* L *and* N*.* N *is called a* complement *of* L*. If* M *does not admit direct summands it is said to be* indecomposable.

By the results in the previous section, if L is a direct summand of M and N a complement of L, it means that any m in M can be written in a unique way as $m = l + n$, $l \in L$ and $n \in N$. We write $M = L \oplus N$ and $L \overset{\oplus}{\leq} M$.

Example 5.4. (1) consider the $\mathbb{Z}$-module $\mathbb{Z}/6\mathbb{Z}$. Then $\mathbb{Z}/6\mathbb{Z} = 3\mathbb{Z}/6\mathbb{Z} \oplus 2\mathbb{Z}/6\mathbb{Z}$. The regular module ${}_{\mathbb{Z}}\mathbb{Z}$ is indecomposable
(2) let K be a field and V a K-module. Then, by a well-know result of linear algebra, any $L \leq V$ is a direct summand of V.
(3) Let $R = \begin{pmatrix} K & K \\ 0 & K \end{pmatrix}$. Then $R = P_1 \oplus P_2$, where $P_1 = \{\begin{pmatrix} k & 0 \\ 0 & 0 \end{pmatrix} \mid k \in K\}$ and $P_2 = \{\begin{pmatrix} 0 & k_1 \\ 0 & k_2 \end{pmatrix} \mid k_1, k_2 \in K\}$.

Exercises

Exercise 5.5. Let ${}_R L \leq_R M$. Show that L is a direct summand of M if and only if there exists ${}_R N \leq_R M$ such that $L + N = M$ and $L \cap N = 0$.

Exercise 5.6. Let $M_1, M_2 \leq M$ such that $M = M_1 \oplus M_2$. Then for any $f_1 : M_1 \to N$ and $f_2 : M_2 \to N$ there exists a morphism $f : M \to N$ such that $f = f_1\pi_1 + f_2\pi_2$. Conversely, show that for any $f : M \to N$ there exist unique $f_1 : M_1 \to N$ and $f_2 : M_2 \to N$ such that $f = f_1\pi_1 + f_2\pi_2$

Exercise 5.7. Let ${}_R M$ be a module and $\{M_i\}_{i \in I}$ a family of submodules of M and let the morphism α as in the Remark 4.1. The following are equivalent:
(1) α is an isomorphism
(2) if $m \in M$, then m can be written in a unique way as sum of elements of the M_i
(3) $M = \sum_I M_i$ and, for any $i \in I$, $M_i \cap (\sum_{I \setminus \{i\}} M_j) = 0$

Exercise 5.8. Let $0 \to L \xrightarrow{f} M \xrightarrow{g} N \to 0$ be a split exact sequence and α the isomorphism as in Definition 5.1. Show that $M = \alpha^{-1}(L) \oplus \alpha^{-1}(N)$, $\alpha^{-1}(L) \cong L$, and $\alpha^{-1}(N) \cong N$.

6. Free modules and finitely generated modules

Definition 6.1. *A module* ${}_R M$ *is said to be* generated *by a family* $\{x_i\}_{i \in I}$ *of elements of* M *if each* $x \in M$ *can be written as* $x = \sum_I r_i x_i$*, with* $r_i \in R$ *for any* $i \in I$*, and* $r_i = 0$ *for almost every* $i \in I$*.*
The $\{x_i\}_{i \in I}$ *are called a set of* generator *of* M *and we write* $M =< x_i, i \in I >$*.*
If the coefficients r_i *are uniquely determined by* x*, the* $(x_i)_{i \in I}$ *are called a* basis *of* M*.*
The module M *is said to be* free *if it admits a basis.*

Proposition 6.2. *A module $_RM$ is free if and only $M \cong R^{(I)}$ for some set I.*

Proof. The module $R^{(I)}$ is free with basis $(e_i)_{i\in I}$, where e_i is the canonical vector with all zero components except for the i-th equal to 1.
Conversely if M is free with basis $(x_i)_{i\in I}$, then we can define a homomorphism $\alpha : R^{(I)} \to M$, $(r_i)_{i\in I} \mapsto \sum_I r_i x_i$. It is easy to show that α is an isomorphism, as a consequence of the definition of a basis: indeed, it is clearly an epi and if $\alpha(r_i) = \sum r_i x_i = 0$, since the r_i are uniquely determined by 0, we conclude that $r_i = 0$ for all i, i.e. α is a mono. □

Given a free module M with basis $(x_i)_I$, then every homomorphism $f : M \to N$ is uniquely determined by its value on the x_i and the elements $f(x_i)$ can be chosen arbitrarily in N. Indeed, chosen the $f(x_i)$, given $x = \sum r_i x_i \in M$, we construct $f(x) = \sum r_i f(x_i)$. Since $(x_i)_{i\in I}$ is a basis this is a good definition. (Notice: analogy with vector spaces!).

Proposition 6.3. *Any module is quotient of a free module*

Proof. Let M be an R-module. Since we can always choose $I = M$, the module M admits a set of generators. Let $(x_i)_{i\in I}$ a set of generators for M and define a homomorphism $\alpha : R^{(I)} \to M$, $(r_i)_{i\in I} \mapsto \sum_i r_i x_i$. Clearly α is an epi and so $M \cong R^{(I)}/\operatorname{Ker}\alpha$ □

Definition 6.4. *A module $_RM$ is* finitely generated *it there exists a finite set of generators for M. A module is* cyclic *if it can be generated by a single element.*

By Proposition 6.3 $_RM$ is finitely generated if and only if there exists an epimorphism $R^n \to M$ for some $n \in \mathbb{N}$. Similarly, $_RM$ is cyclic if and only if $M \cong R/J$, for a left ideal $J \leq R$.

Example 6.5. The regular module $_RR$ is cyclic, generated by the unity element $_RR =< 1 >$

Proposition 6.6. *Let $_RL \leq {}_RM$.*
1. *If M is finitely generated, then M/L is finitely generated.*
2. *If L and M/L are finitely generated, so is M*

Proof.
1. If $\{x_1, \dots, x_n\}$ is a set of generator of M, then $\{\overline{x}_1, \dots, \overline{x}_n\}$ is a set of generator for M/L.
2. Let $< x_1, \dots, x_n >= L$ and $< \overline{y}_1, \dots, \overline{y}_m >= M/L$, where $x_1, \dots, x_n, y_1, \dots, y_m \in M$. Let $x \in M$ and consider $\overline{x} = \sum_{i=1,\dots m} r_i \overline{y_i}$ in M/L. Then $x - \sum_{i=1,\dots m} r_i y_i \in L$ and so $x - \sum_{i=1,\dots m} r_i y_i = \sum_{j=1,\dots,n} r_j x_j$. Hence $x = \sum_{i=1,\dots m} r_i y_i + \sum_{j=1,\dots,n} r_j x_j$, i.e. $\{x_1, \dots, x_n, y_1 \dots, y_m\}$ is a finite set of generators of M.

□

Notice that M finitely generated doesn't imply L finitely generated. For example, let R be the ring $R = K[x_i, i \in \mathbb{N}]$. Consider the regular module $_RR$ and its submodule $L =< x_i, i \in \mathbb{N} >$.

Exercises

Exercise 6.7. Show that any submodule of $_\mathbb{Z}\mathbb{Z}$ is finitely generated.

Exercise 6.8. Show that the $\mathbb{Z}$-module $\mathbb{Q}$ is not finitely generated.

Exercise 6.9. A module M is *simple* if $L \leq M$ implies $L = 0$ or $L = M$ (i.e. M doesn't have non trivial submodules).
1. show that any simple module is cyclic
2. Exhibit a cyclic module which is not simple.

Exercise 6.10. Let R be a ring. An element $e \in R$ is *idempotent* if $e^2 = e$. Show that
1. if e is idempotent, then $(1 - e)$ is idempotent and $R = Re \oplus R(1 - e)$ (where Re and $R(1 - e)$ denote the cyclic modules generated by e and $(1 - e)$, respectively)
2. if $R = I \oplus J$, with I and J left ideals of R, then there exist idempotents e and f such that $1 = e + f$, $I = Re$ and $J = Rf$.

Exercise 6.11. Show that a left R-module M is finitely generated if and only if it is quotient of a finitely generated free module(i.e of a module R^n for a suitable n).

7. Categories and functors

This is very short introduction to the basic concepts of category theory. For more details and for the set-theoretical foundation (in particular the distinction between sets and classes) we refer to S. MacLane, Category for the working mathematician, Graduate Texts in Math., Vol 5, Springer 1971.

Definition 7.1. *A category $\mathcal{C}$ consists in:*

1. *A class $Obj(\mathcal{C})$, called the* objects *of $\mathcal{C}$;*
2. *for each ordered pair (C, C') of objects of $\mathcal{C}$, a set* $\mathrm{Hom}_{\mathcal{C}}(C, C')$ *whose elements are called* morphisms *from C to C';*
3. *for each ordered triple (C, C', C'') of objects of $\mathcal{C}$, a map*
$$\mathrm{Hom}_{\mathcal{C}}(C, C') \times \mathrm{Hom}_{\mathcal{C}}(C', C'') \to \mathrm{Hom}_{\mathcal{C}}(C, C'')$$
called composition *of morphisms*

such that the following axioms C1, C2, C3 hold:
(before stating the axioms, we introduce the notations $\alpha : C \to C'$ for any $\alpha \in \mathrm{Hom}_{\mathcal{C}}(C, C')$, and $\beta\alpha$ for the compostion of $\alpha \in \mathrm{Hom}_{\mathcal{C}}(C, C')$ and $\beta \in \mathrm{Hom}_{\mathcal{C}}(C', C''))$

C1: if $(C, C') \neq (D, D')$, then $\mathrm{Hom}_{\mathcal{C}}(C, C') \cap \mathrm{Hom}_{\mathcal{C}}(D, D') = \emptyset$
C2: if $\alpha : C \to C'$, $\beta : C' \to C''$, $\gamma : C'' \to C'''$ are morphisms, then $\gamma(\beta\alpha) = (\gamma\beta)\alpha$
C3: for each object C there exists $1_C \in \mathrm{Hom}_{\mathcal{C}}(C, C)$, called *identity morphism*, such that $1_C\alpha = \alpha$ and $\beta 1_C = \beta$ for any $\alpha : C' \to C$ and $\beta : C \to C'$.

Notice that, for any $C \in Obj(\mathcal{C})$, the identity morphism 1_C is unique. Indeed, if also $1'_C$ satisfies [C3], then $1_C = 1_C 1'_C = 1'_C$.

A morphism $\alpha : C \to C'$ is an *isomorphism* if there exists $\beta : C' \to C$ such that $\beta\alpha = 1_C$ and $\alpha\beta = 1_{C'}$. If α is an isomorphism, C and C' are called *isomorphic* and we write $C \cong C'$.

Example 7.2.
1. The category **Sets**: the class of objects is the class of all sets; the morphisms are the maps between sets with the usual compositions.
2. The category **Ab**: the objects are the abelian groups; the morphisms are the group homomorphisms with the usual compositions.
3. The category R-**Mod** for a ring R: the objects are the left R-modules and the morphisms are the module homomorphisms with the usual compositions.
4. The category **Mod-**R for a ring R: the objects are the right R-modules and the morphisms are the module homomorphisms with the usual compositions.

Notice that, given a category $\mathcal{C}$, we can construct the *dual* category $\mathcal{C}^{op}$, with $Obj(\mathcal{C}^{op}) = Obj(\mathcal{C})$, $\mathrm{Hom}_{\mathcal{C}^{op}}(C, C') = \mathrm{Hom}_{\mathcal{C}}(C', C)$, and $\alpha * \beta = \beta \cdot \alpha$, where $*$ denotes the composition in $\mathcal{C}^{op}$ and $\cdot$ the composition in $\mathcal{C}$ ($\mathcal{C}^{op}$ is obtained from $\mathcal{C}$ by "reversing the arrows"). Any statement regarding a category $\mathcal{C}$ dualizes to a corresponding statement for $\mathcal{C}^{op}$.

Definition 7.3. *Let $\mathcal{B}$ and $\mathcal{C}$ be two categories. A* functor $F : \mathcal{B} \to \mathcal{C}$ *assigns to each object $B \in \mathcal{B}$ an object $F(B) \in \mathcal{C}$, and assigns to any morphism $\beta : B \to B'$ in $\mathcal{B}$ a morphism $F(\beta) : F(B) \to F(B')$ in $\mathcal{C}$, in such a way:*

F1: *$F(\beta\alpha) = F(\beta)F(\alpha)$ for any $\alpha : B \to B'$, $\beta : B' \to B''$ in $\mathcal{B}$*
F2: *$F(1_B) = 1_{F(B)}$ for any B in $\mathcal{B}$.*

By construction, a functor $F : \mathcal{B} \to \mathcal{C}$ defines a map for any B, B' in $\mathcal{B}$
$$\eta_{B,B'} : \mathrm{Hom}_{\mathcal{B}}(B, B') \to \mathrm{Hom}_{\mathcal{C}}(F(B), F(B')), \quad \beta \mapsto F(\beta)$$
The functor F is called *faithful* if all these maps are injective and is called *full* it they are surjective. If F is full and faithful, then all the maps $\eta_{B,B'}$ are bijective and so the morphisms in the two categories are the same.

A functor $F : \mathcal{B}^{op} \to \mathcal{C}$ is called a *contravariant* functor from $\mathcal{B}$ to $\mathcal{C}$. In particular a contravariant functor F assigns to any morphism $\beta : B \to B'$ in $\mathcal{B}$ a morphism $F(\beta) : F(B') \to F(B)$ in $\mathcal{C}$.

Example 7.4.
1. Let $\mathcal{B}$ and $\mathcal{C}$ two categories. $\mathcal{B}$ is a *subcategory* of $\mathcal{C}$ if $Obj(\mathcal{B}) \subseteq Obj(\mathcal{C})$, $\mathrm{Hom}_{\mathcal{B}}(B, B') \subseteq \mathrm{Hom}_{\mathcal{C}}(B, B')$ for any B, B' objects of $\mathcal{B}$, and the compositions in $\mathcal{B}$ and $\mathcal{C}$ are the same. In this case there is a canonical functor $\mathcal{B} \to \mathcal{C}$ which is clearly faithful. If this functor is also full, $\mathcal{B}$ is said a *full subcategory* of $\mathcal{C}$.

(2) Let $M \in R$-Mod. As we have already observed $\mathrm{Hom}_R(M,N)$ is an abelian group for any $N \in R$-Mod. So we can define a functor (Verify the axioms!)
$$\mathrm{Hom}_R(M,-) : R\text{-Mod} \to \mathbf{Ab}, \quad N \mapsto \mathrm{Hom}_R(M,N)$$
such that for any $\alpha : N \to N'$,
$$\mathrm{Hom}_R(M,\alpha) : \mathrm{Hom}_R(M,N) \to \mathrm{Hom}_R(M,N'), \ \varphi \mapsto \alpha\varphi$$

(3) Let $M \in R$-Mod and consider the abelian group $\mathrm{Hom}_R(N,M)$ for any $N \in R$-Mod. So we can define a contravariant functor (Verify the axioms!)
$$\mathrm{Hom}_R(-,M) : (R\text{-Mod})^{op} \to \mathbf{Ab}, \quad N \mapsto \mathrm{Hom}_R(N,M)$$
such that for any $\alpha : N \to N'$,
$$\mathrm{Hom}_R(\alpha,M) : \mathrm{Hom}_R(N',M) \to \mathrm{Hom}_R(N',M), \ \psi \mapsto \psi\alpha$$

In these lectures we will deal mainly with categories having some kind of additive structure. For instance in the category R-Mod, any set of morphisms $\mathrm{Hom}_R(M,N)$ is an abelian group and the composition preserves the sums.

Definition 7.5. *A category $\mathcal{C}$ is called* preadditive *if each set $\mathrm{Hom}_{\mathcal{C}}(C,C')$ is an abelian group and the compositions maps $\mathrm{Hom}_{\mathcal{C}}(C,C') \times \mathrm{Hom}_{\mathcal{C}}(C',C'') \to \mathrm{Hom}_{\mathcal{C}}(C,C'')$ are bilinear.*

If $\mathcal{B}$ and $\mathcal{C}$ are preadditive categories, a functor $F : \mathcal{B} \to \mathcal{C}$ is additive *if $F(\alpha+\alpha') = F(\alpha)+F(\alpha')$ for $\alpha,\alpha' : C \to C'$.*

Example 7.6. The category R-Mod is a preadditive category. If $M \in R$-Mod, then $\mathrm{Hom}_R(M,-)$ and $\mathrm{Hom}_R(-,M)$ are additive functors.

Definition 7.7. *Let R and S two rings and let $F : R\text{-Mod} \to S\text{-Mod}$ be an additive functor. F is called* left exact *if, for any exact sequence $0 \to L \to M \to N \to 0$ in R-Mod, the sequence $0 \to F(L) \to F(M) \to F(N)$ in S-Mod is exact. F is called* right exact *if, for any exact sequence $0 \to L \to M \to N \to 0$ in R-Mod, the sequence $F(L) \to F(M) \to F(N) \to 0$ in S-Mod is exact. The functor F is* exact *if it is both left and right exact.*

In particular, if F is exact then for any exact sequence in R-Mod $0 \to L \to M \to N \to 0$, the corresponding sequence $0 \to F(L) \to F(M) \to F(N) \to 0$ in S-Mod is exact.

Proposition 7.8. *Let $X \in R$-Mod. The functor $\mathrm{Hom}_R(X,-)$ is left exact*

Proof. Let $0 \to L \xrightarrow{f} M \xrightarrow{g} N \to 0$ be an exact sequence in R-Mod. Denoted by $f^* = \mathrm{Hom}_R(X,f)$ and $g^* = \mathrm{Hom}_R(X,g)$, we have to show that the sequence of abelian groups $0 \to \mathrm{Hom}_R(X,L) \xrightarrow{f^*} \mathrm{Hom}_R(X,M) \xrightarrow{g^*} \mathrm{Hom}_R(X,N)$ is exact. In particular, we have to show that f^* is a mono and that $\mathrm{Im}\, f^* = \mathrm{Ker}\, g^*$.

Let us start considering $\alpha : X \to L$ such that $f^*(\alpha) = 0$. So for any $x \in X$ $f^*(\alpha)(x) = f\alpha(x) = 0$. Since f is a mono we conclude $\alpha(x) = 0$ for any $x \in X$, that is $\alpha = 0$.

Consider now $\beta \in \mathrm{Im}\, f^*$; then there exists $\alpha \in \mathrm{Hom}_R(X,L)$ such that $\beta = f^*(\alpha) = f\alpha$. Hence $g^*(\beta) = g\beta = gf\alpha = 0$, since $gf = 0$. So we get $\mathrm{Im}\, f^* \leq \mathrm{Ker}\, g^*$.

Finally, let $\beta \in \mathrm{Ker}\, g^*$, so that $g\beta = 0$ This means $\mathrm{Im}\,\beta \leq \mathrm{Ker}\, g = \mathrm{Im}\, f$. For any $x \in X$ define α as $\alpha(x) = f^{\leftarrow}(\beta(x))$: α is well-defined since f is a mono and clearly $\beta = f\alpha = f^*(\alpha)$. So we get $\mathrm{Ker}\, g^* \leq \mathrm{Im}\, f^*$ □

In a similar way one prove that the functor $\mathrm{Hom}_R(-,X)$ is left exact. Notice that, since $\mathrm{Hom}_R(-,X)$ is a contravariant functor, left exact means that for any exact sequence in R-Mod $0 \to L \to M \to N \to 0$, the corresponding sequence of abelian groups $0 \to \mathrm{Hom}_R(N,X) \to \mathrm{Hom}_R(M,X) \to \mathrm{Hom}_R(L,X)$ is exact.

Remark 7.9. Notice that if F is an additive functor and $0 \to L \xrightarrow{f} M \xrightarrow{g} N \to 0$ is a split exact sequence in R-Mod, then $0 \to F(L) \xrightarrow{F(f)} F(M) \xrightarrow{F(g)} F(N) \to 0$ is split exact. Indeed, since there exists φ such that $\varphi f = id_L$ (see Proposition 5.2), $F(\varphi)F(f) = id_{F(L)}$, so $F(f)$ is a split mono. Similarly one show that $F(g)$ is a split epi.

In particular, for a given module $X \in R$-Mod the functors $\mathrm{Hom}_R(X,-)$ and $\mathrm{Hom}_R(-,X)$ could be not exact. Nevertheless, if $0 \to L \to M \to N \to 0$ is a split exact sequence in R-Mod, then the sequence $0 \to \mathrm{Hom}_R(X,L) \to \mathrm{Hom}_R(X,M) \to \mathrm{Hom}_R(X,N) \to 0$ and the sequence $0 \to$

$\mathrm{Hom}_R(N,X)\to\mathrm{Hom}_R(M,X)\to\mathrm{Hom}_R(L,X)\to 0$ are split exact. In particular $\mathrm{Hom}_R(X,L\oplus N)\cong\mathrm{Hom}_R(X,L)\oplus\mathrm{Hom}_(X,N)$ and $\mathrm{Hom}_R(L\oplus N,X)\cong\mathrm{Hom}_R(L,X)\oplus\mathrm{Hom}_R(N,X)$

One often wishes to compare two functors with each other. So we introduce the notion of *natural transformation*:

Definition 7.10. *Let F and G two functors $\mathcal{B}\to\mathcal{C}$. A natural transformation $\eta: F\to G$ is a family of morphisms $\eta_B: F(B)\to G(B)$, for any $B\in\mathcal{B}$, such that for any morphism $\alpha: B\to B'$ in $\mathcal{B}$ the following diagram in $\mathcal{C}$ is commutative*

$$\begin{tikzcd} F(B) \arrow[r, "\eta_B"] \arrow[d, "F(\alpha)"'] & G(B) \arrow[d, "G(\alpha)"] \\ F(B') \arrow[r, "\eta_{B'}"] & G(B') \end{tikzcd}$$

If η_B is an isomorphism in $\mathcal{C}$ for any $B\in\mathcal{B}$, then η is called a natural equivalence.

Two categories $\mathcal{B}$ and $\mathcal{C}$ are *isomorphic* if there exist functors $F:\mathcal{B}\to\mathcal{C}$ and $G:\mathcal{C}\to\mathcal{B}$ such that $GF=1_{\mathcal{B}}$ and $FG=1_{\mathcal{C}}$. This is a very strong notion, in fact there are several and relevant examples of categories $\mathcal{B}$ and $\mathcal{C}$ which have essentially the same structure, but where there is a bijective correspondence between the isomorphism classes of objects rather than between the individual objects. Therefore we define the following concept:

Definition 7.11. *A functor $F:\mathcal{B}\to\mathcal{C}$ is an* equivalence *if there exists a functor $G:\mathcal{C}\to\mathcal{B}$ and natural equivalences $GF\to 1_{\mathcal{B}}$ and $FG\to 1_{\mathcal{C}}$*

If the functor F is contravariant and gives an equivalence between $\mathcal{B}^{op}$ and $\mathcal{C}$, we say that F is a *duality.*

Proposition 7.12. *A functor $F:\mathcal{B}\to\mathcal{C}$ is an equivalence if and only if it is full and faithful, and every object of $\mathcal{C}$ is isomorphic to an object of the form $F(B)$, with $B\in\mathcal{B}$.*

Thanks to the previous proposition and its analogous for any duality, one can prove the following properties (we state everything in case of a duality, since we will deeply deal with this setting in the final section):

Proposition 7.13. *Let $F:\mathcal{B}\to\mathcal{C}$ be a duality. Then:*

1. $0\to M\xrightarrow{f}N$ *is a mono in $\mathcal{B}$ if and only if* $F(N)\xrightarrow{F(f)}F(M)\to 0$ *is an epi in $\mathcal{C}$.*
2. $M\xrightarrow{f}N\to 0$ *is an epi in $\mathcal{B}$ if and only if* $0\to F(N)\xrightarrow{F(f)}F(M)$ *is an epi in $\mathcal{C}$.*
3. $M\xrightarrow{f}N$ *is an iso in $\mathcal{B}$ if and only if* $F(N)\xrightarrow{F(f)}F(M)$ *is an iso in $\mathcal{C}$.*
4. *The sequence* $0\to L\xrightarrow{f}M\xrightarrow{g}N\to 0$ *is exact in $\mathcal{B}$ if and only if the sequence* $0\to F(N)\xrightarrow{F(g)}F(M)\xrightarrow{F(f)}F(L)\to 0$ *is exact in $\mathcal{C}$*
5. *an object $B\in\mathcal{B}$ is projective if and only if $F(B)\in\mathcal{C}$ is injective.*
6. *An object $B\in\mathcal{B}$ is injective if and only if $F(B)\in\mathcal{C}$ is projective.*
7. *An object $B\in\mathcal{B}$ is indecomposable if and only if $F(B)\in\mathcal{C}$ is indecomposable.*
8. *An object $B\in\mathcal{B}$ is simple if and only if $F(B)\in\mathcal{C}$ is simple.*

Exercise

Exercise 7.14. Let $M,N,L\in R$-Mod. Give an explicit construction of the isomorphisms $\mathrm{Hom}_R(X,L\oplus N)\cong\mathrm{Hom}_R(X,L)\oplus\mathrm{Hom}_(X,N)$ and $\mathrm{Hom}_R(L\oplus N,X)\cong\mathrm{Hom}_R(L,X)\oplus\mathrm{Hom}_(N,X)$ of Remark 7.9.

Exercise 7.15. Let $(P,\leq)$ be a partially ordered set. Let us define a category $\mathcal{C}$ in this way: the objects of $\mathcal{C}$ are the elements of P, and with a unique morphism $p\to q$ whenever $p\leq q$, while $\mathrm{Hom}_{\mathcal{C}}(p,q)=0$ if $p\not\leq q$. Verify that the axioms [C1], [C2], [C3] are satisfied. This is an example of a *small* category, i.e. a category where the class of objects is a set.

Exercise 7.16. Let $\varphi: R\to S$ be a homomorphism of rings. Each left S-module M has also a structure of left R-module, defining $rx:=\varphi(r)x$ for any $x\in M$ and any $r\in R$. Let φ^* : S-Mod $\to R$-Mod, $M\mapsto M$, $\alpha\mapsto\alpha$ for any $M\in S$-Mod and for any $\alpha\in\mathrm{Hom}_S(M,N)$. Verify that φ^* is an additive and faithful functor (called *restriction of scalars*)

Exercise 7.17. A functor F is exact if and only if $F(L) \to F(M) \to F(N)$ is exact whenever $L \to M \to N$ is exact.

8. Projective modules

In general, for a given R-module M, the functor $\mathrm{Hom}_R(M, -)$ is left exact but not right exact. In this section we study the R-modules P for which $\mathrm{Hom}_R(P, -)$ is also right exact.

Definition 8.1. *A module $P \in R$-Mod is* projective *if $\mathrm{Hom}_R(P, -)$ is an exact functor.*

The right exactness is equivalent to require that for any $M \xrightarrow{g} N \to 0$ in R-Mod the homomorphism $\mathrm{Hom}_R(P, M) \xrightarrow{\mathrm{Hom}_R(P,g)} \mathrm{Hom}_R(P, N)$ is an epi, that is for any $\varphi \in \mathrm{Hom}_R(P, N)$ there exists $\psi \in \mathrm{Hom}_R(P, M)$ such that $g\psi = \phi$.

$$\begin{tikzcd} M \arrow[r, "g"] & N \arrow[r] & 0 \\ & P \arrow[u, "\varphi"'] \arrow[ul, dashed, "\psi"] & \end{tikzcd}$$

Example 8.2. Any free module is projective. Indeed, let $R^{(I)}$ a free R-module with $(x_i)_{i\in I}$ a basis. Given $M \xrightarrow{g} N \to 0$ and $\varphi : R^{(I)} \to N$ in R-Mod, let $m_i \in M$ such that $g(m_i) = \varphi(x_i)$ for any $i \in I$. Define $\psi(x_i) = m_i$ and, for $x = \sum r_i x_i$, $\psi(x) = \sum r_i m_i$. We get that $g\psi = \varphi$. Notice that from the construction is clear that the homomorphism ψ could be not unique.

Proposition 8.3. *Let $P \in R$-Mod. The following are equivalent:*
1. *P is projective*
2. *P is a direct summand of a free module*
3. *every exact sequence $0 \to L \xrightarrow{f} M \xrightarrow{g} P \to 0$ splits.*

Proof. $1 \Rightarrow 3$ Let $0 \to L \xrightarrow{f} M \xrightarrow{g} P \to 0$ be an exact sequence in R-Mod and consider the homorphism $1_P : P \to P$. Since P is projective there exists $\psi : P \to M$ such that $g\psi = 1_P$. By Proposition 5.2 we conclude that the sequence splits.
$3 \Rightarrow 2$ The module P is a quotient of a free module, so there exist an exact sequence $0 \to K \xrightarrow{f} R^{(I)} \xrightarrow{g} P \to 0$, which is split.
$2 \Rightarrow 1$ If $R^{(I)} = P \oplus L$, then $\mathrm{Hom}_R(R^{(I)}, N) \cong \mathrm{Hom}_R(P, N) \oplus \mathrm{Hom}_R(L, N)$ for any $N \in R$-Mod. So let us consider the homorphisms

$$\begin{tikzcd} M \arrow[r, "g"] & N \arrow[r] & 0 \\ & P \arrow[u, "\varphi"'] & \end{tikzcd} \quad \text{and} \quad \begin{tikzcd} M \arrow[r, "g"] & N \arrow[r] & 0 \\ & R^{(I)} \arrow[u, "{(\varphi,0)}"'] \arrow[ul, dashed, "\alpha"] & \end{tikzcd}$$

where $(\varphi, 0)(p + l) = \varphi(p) + 0(l) = \varphi(p)$ for any $p \in P$ and $l \in L$ and α exists since $R^{(I)}$ is projective. Then $\alpha = (\psi, \beta)$, with $\psi \in \mathrm{Hom}_R(P, N)$ and $\beta \in \mathrm{Hom}_R(L, N)$, where $\alpha(p + l) = \psi(p) + \beta(l)$ for any $p \in P$ and $l \in L$. Hence $g(\psi(p)) = g(\alpha(p)) = \varphi(p)$ for any $p \in P$. So we conclude that P is projective. $\square$

Example 8.4.
1. Let R be a principal ideal domain (for instance, $R = \mathbb{Z}$). Then any projective module is free. In particular, free abelian groups and projective abelian group coincide.
2. Let $R = \mathbb{Z}/6\mathbb{Z}$. Then $\mathbb{Z}/6\mathbb{Z} = 3\mathbb{Z}/6\mathbb{Z} \oplus 2\mathbb{Z}/6\mathbb{Z}$. The ideals $3\mathbb{Z}/6\mathbb{Z}$ and $2\mathbb{Z}/6\mathbb{Z}$ are projective R-modules, but not free R-modules (why?)

Proposition 8.5. *Let $P \in R$-Mod. P is projective if and only if there exists a family $(\varphi_i, x_i)_{i\in I}$ with $\varphi_i \in \mathrm{Hom}_R(P, R)$ and $x_i \in P$ such that for any $x \in P$ one has $x = \sum_i \varphi_i(x)x_i$ where $\varphi_i(x) = 0$ for almost every $i \in I$.*

Proof. Let P be projective and let $R^{(I)} \xrightarrow{\beta} P \to 0$ be a spli epi. Consider $(e_i)_{i\in I}$ a basis of $R^{(I)}$ and define $x_i = \beta(e_i)$. Observe that $\beta(\sum_i r_i e_i) = \sum_i r_i \beta(e_i) = \sum_i r_i x_i$. By Proposition 5.2, there exists $\varphi : P \to R^{(I)}$ such that $\beta\varphi = id_P$, which induces homomorphisms $\varphi_i = \pi_i\varphi$ where π_i is the projection on the i-th component, so $\varphi_i(x) \in R$ for any $i \in I$ and $\varphi(x) = \sum \varphi_i(x)$. Hence for any $x \in P$ one has $x = \beta\varphi(x) = \beta(\sum_i \varphi_i(x)) = \sum_i \varphi_i(x)x_i$, so $(\varphi_i, x_i)_{i\in I}$ satisfies the stated properties.

Conversely, let $(\varphi_i, x_i)_{i\in I}$ satisfy the statement and let $\beta : R^{(I)} \to P$, $e_i \mapsto x_i$. The homomorphism β is an epi, since the family $(x_i)_{i\in I}$ generates P, and $\beta(\sum r_i) = \sum r_i x_i$. Define $\varphi : P \to R^{(I)}$, $x \mapsto \sum \varphi_i(x)$. Then for any $x \in P$ one gets $\beta\varphi(x) = \beta(\sum \varphi_i(x)) = \sum \varphi_i(x)x_i = x$. By Proposition 5.2 we conclude that β is a split epi and so P is projective. □

Note that, from the results in the previous sections, the projective module ${}_R R$ plays a crucial role in the category R-Mod, since for any $M \in R$-Mod there exists an epi $R^{(I)} \to M \to 0$, for some set I. A module with such property is called a *generator* and so R is a *projective generator* for R-Mod.

In particular, for any $M \in R$-Mod there exists a short exact sequence $0 \to K \to P_0 \to M \to 0$, with P_0 projective. The same holds for the module K, and so, iterating the argument, we can construct an exact sequence

$$\cdots \to P_i \to \cdots \to P_1 \to P_0 \to M \to 0$$

where all the P_i are projectiveSuch a sequence is called a *projective resolution* of P. It is clearly not unique.

It is natural to ask if, for a given $M \in R$-Mod, there exists a projective module P and a "minimal" epi $P \to M \to 0$, in the sense that $f_{|L} : L \to M$ is epi for no proper projective submodule of P. More precisely, we define:

Definition 8.6. *A homomorphism $f : M \to N$ is* right minimal *if for any $g \in \mathrm{End}_R(M)$ such that $fg = f$, one gets g is an isomomorphism.*
If P_M is a projective module and $P_M \to M$ is epimorphism right minimal, then P_M is a projective cover *of M.*

Remark 8.7. Consider the diagram

$$\begin{tikzcd} & 0 & \\ P_M \arrow[r, "f"] \arrow[dr, dashed, shift left, "\varphi"] & M \arrow[u] \arrow[r] & 0 \\ & P \arrow[u, "g"'] \arrow[ul, dashed, shift left, "\psi"] & \end{tikzcd}$$

where P_M is a projective cover of M and P is a projective module. Since P_M and P are projective, there exist φ and ψ such that the diagram commutes. Hence $f\psi = g$ and $g\varphi = f$, so $f\psi\varphi = f$ and, since f is right minimal, we conclude $\psi\varphi$ is an iso. In particular φ is a mono. Define $\theta : P \to P_M$ as $\theta = (\psi\varphi)^{-1}\psi$: then $\theta\varphi = id_P$ and so φ is a split mono (see Proposition 5.2). We conclude that P_M is a direct summand of P. This explains the minimality property of the projective cover announced above.

If also P is a projective cover of M, using the same argument we get that $\varphi\psi$ is an iso, that is $\varphi = \psi^{-1}$ and P_M is isomorphic to P. We have shown that the projective cover is unique (modulo isomorphisms).

We state the following characterization of projective covers:

Theorem 8.8. *Let P a projective module. Then $P \xrightarrow{f} M \to 0$ is a projective cover of M if and only if* $\mathrm{Ker}\, f$ *is a superfluous submodule of P (i.e. for any submodule $L \leq P$, $L + \mathrm{Ker}\, f = P$ implies $L = P$.)*

Observe that, given $M \in R$-Mod, a projective cover for M could not exist. A ring in which any module admits a projective cover is called *semiperfect*

Let now $M \in R$-Mod and suppose there exist a projective resolution of M

$$\dots P_2 \xrightarrow{f_2} P_1 \xrightarrow{f_1} P_0 \xrightarrow{f_0} M \to 0$$

such that P_0 is a projective cover of M and P_i is a projective cover of $\mathrm{Ker}\, f_{i-1}$ for any $i \in \mathbb{N}$. Such a resolution is called a *minimal projective resolution* of M.

Exercise

Exercise 8.9. Let $P_1, P_2, \dots, P_n \in R$-Mod. Then $\oplus_{i=1,\dots,n} P_i$ is projective if and only if P_i is projective for any $i = 1, \dots, n$.

Exercise 8.10. Let $0 \to L \to M \to N \to 0$ a short exact sequence in R-Mod. If L and N are projective, then M is projective

Exercise 8.11. Let $P \in R$-Mod be a projective module. Show that, if P is finitely generated, then P is a direct summand of R^n, for a suitable $n \in \mathbb{N}$.

Exercise 8.12. Show that any abelian group $n\mathbb{Z}$, $n \in \mathbb{N}$, is a projective $\mathbb{Z}$-module.

Exercise 8.13. An epimorphism $f : M \to N \to 0$ is called *superfluous* if $\operatorname{Ker} f$ is a superfluous submodule of M. Show that, if f is superfluous and fg is an epimorphism, then g is an epimorphism.

9. Bimodules

Definition 9.1. *Let R and S rings. An abelian group M is a* left R- right S-bimodule *if M is a left R-module and a right S-module such that the two scalar multiplications satisfy $r(xs) = (rx)s$ for any $r \in R$, $s \in S$, $x \in M$. We write ${}_R M_S$.*

Example 9.2. Let $M \in R$-Mod and consider $S = \operatorname{End}^r_R(M)$, the ring of homomorphism R-linear of M, where homorphisms act on the right (i.e. $mf = f(m)$ and $m(fg) = g(f(m))$). So M is a right S-module (Verify!) and ${}_R M_S$ is a bimodule. Indeed $(rm)f = f(rm) = rf(m) = r(mf)$ for any $r \in R$, $m \in M$ and $f \in S$.

Given a bimodule ${}_R M_S$ and a left R-module N, the abelian group $\operatorname{Hom}_R(M, N)$ is naturally endowed with a structure of left S-module, by defining $(sf)(x) := f(xs)$ for any $f \in \operatorname{Hom}_R(M, N)$ and any $x \in M$. (Verify! crucial point: $(s_1(s_2 f))(x) = (s_2 f(xs_1)) = f(xs_1 s_2) = ((s_1 s_2) f)(x)$).

Similary, if ${}_R N_T$ is a left R- right T-bimodule and $M \in R$-Mod, then $\operatorname{Hom}_R(M, N)$ is naturally endowed with a structure of right T-module, by defining $(ft)(x) := f(x)t$ (Verify! crucial point: $(f(t_1 t_2))(x) = f(x)(t_1 t_2) = (f(x))t_1)t_2 = ((ft_1)(x))t_2 = ((ft_1)t_2)(x))$.

Moreover, one can show that if ${}_R M_S$ and ${}_R N_T$ are bimodules, then $\operatorname{Hom}_R({}_R M_S, {}_R N_T)$ is a left S- right T-bimodule (Verify!).

Arguing in a similar way for right R-modules, if ${}_S M_R$ and ${}_T N_R$ are bimodules, then the abelian group $\operatorname{Hom}_R({}_S M_R, {}_T N_R)$ is a left T- right S-bimodule, by $(tf)(x) = t(f(x))$ and $(fs)(x) = f(sx)$.

10. Injective modules

In this section we study the R-modules E for which $\mathrm{Hom}_R(-,E)$ is an exact functor. Observe that many results we are going to show are dual of those proved for projective modules.

Definition 10.1. *A module $E \in R$-Mod is* injective *if* $\mathrm{Hom}_R(-,E)$ *is an exact functor.*

The exactness is equivalent to require that for any $0 \to L \xrightarrow{f} M$ in R-Mod the homomorphism $\mathrm{Hom}_R(M,E) \xrightarrow{\mathrm{Hom}_R(f,E)} \mathrm{Hom}_R(L,E)$ is an epi, that is for any $\varphi \in \mathrm{Hom}_R(L,E)$ there exists $\psi \in \mathrm{Hom}_R(M,E)$ such that $\psi f = \varphi$.

$$\begin{tikzcd} 0 \arrow[r] & L \arrow[r, "f"] \arrow[d, "\varphi"'] & M \arrow[dl, dashed, "\psi"] \\ & E & \end{tikzcd}$$

Any module is quotient of a projective module. Does the dual property hold? that is, given any module $M \in R$-Mod, is it true that M embeds in a injective R-module? In the sequel we will answer to this crucial question.

An abelian group G is *divisible* if, for any $n \in \mathbb{Z}$ and for any $g \in G$, there exists $t \in G$ such that $g = nt$. We are going to show that an abelian group is injective if and only if it is divisible. We need the the following useful criterion to check whether a module is injective, known as Baer's Lemma.

Lemma 10.2. *Let $E \in R$-Mod. The module E is injective if and only if for any left ideal J of R and for any $\varphi \in \mathrm{Hom}_R(J,E)$ there exists $\psi \in \mathrm{Hom}_R(R,E)$ such that $\psi i = \varphi$, where i is the canonical inclusion $0 \to J \xrightarrow{i} R$.*

The lemma states that it is sufficient to check the injectivity property only for left ideals of the ring. In particular, the Baer's Lemma says that E is injective if and only if for any ${}_RJ \leq {}_RR$ and for any $\varphi \in \mathrm{Hom}_R(J,E)$ there exists $y \in E$ such that $\varphi(x) = xy$ for any $x \in J$.

Proposition 10.3. *A module $G \in \mathbb{Z}$-Mod is injective if and only if it is divisible.*

Proof. Let us assume G injective, consider $n \in \mathbb{Z}$ and $g \in G$ and the commutative diagram

$$\begin{tikzcd} 0 \arrow[r] & \mathbb{Z}n \arrow[r, "i"] \arrow[d, "\varphi"] & \mathbb{Z} \arrow[dl, dashed, "\psi"] \\ & G & \end{tikzcd}$$

where $\varphi(sn) = sg$ for any $s \in \mathbb{Z}$ and ψ exists since G is injective. Let $t = \psi(1)$, $t \in G$. Then $\varphi(n) = \psi(i(n))$ implies $g = nt$ and we conclude that G is divisible.

Conversely, suppose G divisible and apply Baer's Lemma. The ideal of $\mathbb{Z}$ are of the form $\mathbb{Z}n$ for $n \in \mathbb{Z}$, so we have to verify that for any $\varphi \in \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}n, G)$ there exists ψ such that

$$\begin{tikzcd} 0 \arrow[r] & \mathbb{Z}n \arrow[r, "i"] \arrow[d, "\varphi"] & \mathbb{Z} \arrow[dl, dashed, "\psi"] \\ & G & \end{tikzcd}$$

commutes. Let $g \in G$ such that $\varphi(n) = g$. Since $\mathbb{Z}$ is a free $\mathbb{Z}$-module, define $\psi(1) = t$ where $g = nt$ and so $\psi(r) = rt$ for any $r \in \mathbb{Z}$. Hence $\varphi(sn) = sg = snt = \psi(i(sn))$. □

The result stated in the previous proposition holds for any Principal Ideal Domain R (see Exercise 10.14).

Example 10.4. The $\mathbb{Z}$-module $\mathbb{Q}$ is injective.

Remark 10.5. Any abelian group G embeds in a injective abelian group. Indeed, consider a short exact sequence $0 \to K \to \mathbb{Z}^{(I)} \to G \to 0$ and the canonical inclusion in $\mathbb{Z}$-Mod $0 \to \mathbb{Z} \to \mathbb{Q}$. One easily check that $\mathbb{Q}^{(I)}/K$ is divisible (Verify!) and so injective. Then we get the induced monomorphism $0 \to G \cong \mathbb{Z}^{(I)}/K \to \mathbb{Q}^{(I)}/K$.

Proposition 10.6. *Let R be a ring. If $D \in \mathbb{Z}$-*Mod *is injective, then* $\mathrm{Hom}_{\mathbb{Z}}(R, D)$ *is an injective left R-module*

Proof. First notice that, since ${}_{\mathbb{Z}}R_R$ is a bimodule, $\mathrm{Hom}_{\mathbb{Z}}(R, D)$ is naturally endowed with a structure of left R-module. In order to verify that it is injective, we apply Baer's Lemma. So let ${}_RI \leq {}_RR$ and $h : I \to \mathrm{Hom}_{\mathbb{Z}}(R, D)$ an R-homomorphism. Then $\gamma : I \to D$, $a \mapsto h(a)(1)$ defines a $\mathbb{Z}$-homomorphism and, since D is an injective abelian group, there exists $\overline{\gamma} : R \to D$ which extends γ. Now we have, for any $a \in I$ and $r \in R$,

$$(a\overline{\gamma})(r) = \overline{\gamma}(ra) = \gamma(ra) = [h(ra)](1) = [rh(a)](1) = [h(a)](r)$$

so $h(a) = a\overline{\gamma}$ for any $a \in I$. Hence we conclude $\mathrm{Hom}_{\mathbb{Z}}(R, D)$ is injective by Baer's Lemma. $\square$

Corollary 10.7. *Let $M \in R$-*Mod. *Then there exists an injective module $E \in R$-*Mod *and a monomorphism $0 \to M \to E$.*

Proof. Consider the isomorphism of $\mathbb{Z}$-modules $\varphi : \mathrm{Hom}_R(R, M) \to M$, $f \mapsto f(1)$. Observe that since ${}_RR_R$ is a left R- right R-bimodule, then $\mathrm{Hom}_R(R, M)$ is naturally endowed with a structure of left R-module. One easily check that φ is also R-linear, hence ${}_RM \cong \mathrm{Hom}_R(R_R, M) \leq \mathrm{Hom}_{\mathbb{Z}}(R_R, M)$. By Remark 10.5, there is a mono of $\mathbb{Z}$-modules $0 \to M \to G$ from which we obtain a mono of R-modules $0 \to \mathrm{Hom}_{\mathbb{Z}}(R_R, M) \to \mathrm{Hom}_{\mathbb{Z}}(R_R, G)$, where $\mathrm{Hom}_{\mathbb{Z}}(R_R, G)$ is an injective left R-module by Proposition 10.6. $\square$

Since any module M embeds in a injective one, it is natural to ask whether there exists a "minimal" injective module containing M.

Definition 10.8. *A homomorphism $f : M \to N$ is* left minimal *if for any $g \in \mathrm{End}_R(N)$ such that $gf = f$, one gets g is an isomomorphism.*
If E_M is an injective module and $M \to E_M$ is a monomorphism left minimal, then E_M is an injective envelope *of M.*

Remark 10.9. Consider the diagram

$$\begin{tikzcd}
& 0 \arrow[d] & \\
0 \arrow[r] & M \arrow[r, "f"] \arrow[d, "g"'] & E_M \arrow[dl, dashed, shift left, "\varphi"] \\
& E \arrow[ur, dashed, shift left, "\psi"] &
\end{tikzcd}$$

where E_M is an injective envelope of M and E is an injective module. Since E_M and E are injective, there exist φ and ψ such that the diagram commutes. Hence $\psi g = f$ and $\varphi f = g$, so $\psi\varphi f = f$ and, since f is left minimal, we conclude that $\psi\varphi$ is an iso. In particular φ is a mono and so it is a split mono. We conclude that E_M is a direct summand of E. This explains the minimality property of the injective envelope announced above.

If also E is an injective envelope of M, using the same argument we get that $\varphi\psi$ is an iso, that is φ is an iso and E_M is isomorphic to E. We have shown that the injective envelope is unique (modulo isomorphisms).

We state the following characterization of injective envelope.

Theorem 10.10. *Let E be an injective module. Then $0 \to M \xrightarrow{f} E$ is an injective envelope if and only if* $\mathrm{Im}\, f$ *is an essential submodule of M (i.e. for any submodule $L \leq E$, $L \cap \mathrm{Im}\, f \neq \{0\}$)*

Proof. Suppose $0 \to M \xrightarrow{f} E$ is an injective envelope and let $L \leq E$ such that $L \cap \mathrm{Im}\, f = \{0\}$. Then $\mathrm{Im}\, f \oplus L \leq E$ and we can consider the commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & M \arrow[r, "f"] \arrow[d, "f"'] & \mathrm{Im}\, f \oplus L \arrow[r, "i"] \arrow[dl, "{(\mathrm{id},0)}"'] & E \arrow[dll, dashed, "\varphi"] \\
& E & &
\end{tikzcd}$$

where i is the canonical inclusion of $\mathrm{Im}\, f \oplus L$ in E and φ exists since E is injective. Then $\varphi f = f$ but φ is clearly not an iso.

Conversely, let $\operatorname{Im} f$ be essential in M and let $g \in \operatorname{End}_R(E)$ such that $gf = f$. Since f is an essential mono we conclude that g is a mono (see Exercise 10.17), so it is a split mono. In particular, $\operatorname{Im} f \leq \operatorname{Im} g \overset{\oplus}{\leq} E$, contradicting the essentiality of $\operatorname{Im} f$. □

Not every module has a projective cover. Thus the next result is especially remarkable

Theorem 10.11. *Every module has an injective envelope.*

Proof. Let $M \in R$-Mod; by Corollary 10.7 there exists an injective module Q such that $0 \to M \to Q$. Consider the set $\{E' |\ M \leq E' \leq Q \text{ and} M \text{ essential in } E'\}$. One easily check that it is an inductive set so, by Zorn's Lemma, it contains a maximal elemnt E. Let us show that E is a direct summand of Q and so E is injective (see Exercise 10.16). To this aim, consider the set $\{F' | F' \leq Q \text{ and } F' \cap E = 0\}$. It is inductive so, again by Zorn's Lemma, it contains a maximal element F. Then there exists an obvious iso $g : E \oplus F/F \to E$ and $E \oplus F/F \leq Q/F$: from the maximality of F it follows that $E \oplus F/F \leq Q/F$ is an essential inclusion (Verify!) so consider the diagram

$$\begin{tikzcd} 0 \arrow[r] & E \oplus F/F \arrow[r, "j"] \arrow[d, "g"] & Q/F \arrow[dl, "\varphi"] \\ & Q & \end{tikzcd}$$

where j is the canonical inclusion and φ exists since Q is injective. Moroever φ is a mono since $\varphi j = g$ is a mono and j is an essential mono (see Exercise 10.17). It follows that M is essential in $E = \operatorname{Im} g$ and $E = \operatorname{Im} g = \varphi(E \oplus F/F)$ is essential in $\operatorname{Im} \varphi$. Thus M is essential in $\operatorname{Im} \varphi$ so, from the maximality of E we conclude that $E = \operatorname{Im} \varphi$ and hence $\varphi(E \oplus F/F) = \varphi(Q/F)$. Since φ is a mono we conclude $E \oplus F = Q$. □

Proposition 10.12. *Let $E \in R$-Mod. The following are equivalent:*

(1) *E is injective*

(2) *every exact sequence $0 \to E \xrightarrow{f} M \xrightarrow{g} N \to 0$ splits.*

Proof. $1 \Rightarrow 2$ Consider the commutative diagram

$$\begin{tikzcd} 0 \arrow[r] & E \arrow[r, "f"] \arrow[d, "\mathrm{id}_E"'] & M \arrow[dl, dashed, "\varphi"] \\ & E & \end{tikzcd}$$

where φ exists since E is injective. Since $\varphi f = \mathrm{id}_E$, by Proposition 5.2 we conclude that f is a split mono.

$2 \Rightarrow 1$ By Corollary 10.7 there exists an exact sequence $0 \to E \to F \to N \to 0$, where F is an injective module. Since the sequence splits, we get that E is a direct summand of a injective module, and so E is injective (see Exercise 10.16). □

Comparing the previous proposition with the analogous one for projective modules (see Proposition 8.3), there is an evident difference. Speaking about projective modules, we saw that a special role is played by the projective generator R. Does a module with the dual property exist? An injective module $E \in R$-Mod such that any $M \in R$-Mod embeds in E^{I_M}, for a set I_M, is called an *injective cogenerator* of R-Mod. We will see in the sequel that such a module always exists.

Remark 10.13. Dualizing what we showed in the projective case, for any module $M \in R$-Mod there exists a long exact sequence $0 \to M \xrightarrow{f_0} E_0 \xrightarrow{f_1} E_1 \xrightarrow{f_2} E_2 \to \dots$, where the E_i are injective. This is called an *injective coresolution* of M. If E_0 is an injective envelope of M and E_i in an injective envelope of $\operatorname{Ker} f_i$ for any $i \geq 1$, then the sequence is called a *minimal injective coresolution* of M.

Exercises

Exercise 10.14. Let R be a Principal Ideal Domain. Prove that an R-module is injective if and only if it is divisible.

Exercise 10.15. Let G be a divisible abelian group. Then $G^{(I)}$ and G/N are divisible, for any set I and for any subgroup N of G.

Exercise 10.16. Let E_i for $i = 1, \dots, n$ in R-Mod. Then $\bigoplus_{i \in I} E_i$ is injective if and only if E_i is injective for any $i = 1 \dots n$.

Exercise 10.17. A monomorphism $0 \to L \to M$ is R-Mod is called *essential monomorphism* if $\operatorname{Im} L$ is essential in M. Prove that if f is an essential morphism and gf is a mono, then g is a mono.

Exercise 10.18. Let $0 \to M \xrightarrow{f} L$ and $0 \to L \xrightarrow{g} N$ two essential monomorphism. Show that gf is an essential monomorphism.

11. On the lattice of submodules of M

Let $M \in R$-Mod and consider the partially ordered set $\mathcal{L}_M = \{L | L \leq M\}$. Then $\mathcal{L}_M$ is a complete lattice, where for any $N, L \in \mathcal{L}$, $\sup\{N, L\} = L + N$ and $\inf\{N, L\} = L \cap N$. The greatest element of $\mathcal{L}_M$ is M and the smallest if $\{0\}$.

Given an arbitrary module $M \in R$-Mod, it is natural to ask whether minimal or maximal elements of $\mathcal{L}$ exist. They are exactly the maximal submodules of M and the simple submodules of M, respectively. More precisely we introduce the following definitions:

Definition 11.1. *A module $S \in R$-Mod is* simple *if $L \leq S$ implies $L = \{0\}$ or $L = S$.*
A submodule $N < M$ is a maximal submodule *of M if $N \leq L \leq M$ implies $L = N$ or $L = M$.*

Example 11.2.
(1) Let K be a field. Then K is the unique (modulo isomorphisms) simple module in K-Mod.
(2) In $\mathbb{Z}$-Mod any abelian group $\mathbb{Z}/\mathbb{Z}p$ with p prime is a simple abelian group. So in $\mathbb{Z}$-Mod there are infinite simple modules.
(3) The regular module $\mathbb{Z}$ does not contain any simple submodule, since any ideal of $\mathbb{Z}$ is of the form $\mathbb{Z}n$ and $\mathbb{Z}m \leq \mathbb{Z}n$ whenever n divides m.

In general, it is not true that any module contains a simple or a maximal submodule. Nevertheless we have the following result (see also Exercise 11.17)

Proposition 11.3. *Let R be a ring and ${}_RI < {}_RR$. There exists a maximal left ideal M of R such that $I \leq M < R$. In particular R adimits maximal left ideals.*

Proof. Let $\mathcal{F} = \{L | I \leq L < R\}$. The set $\mathcal{F}$ is inductive since, given a sequence $L_0 \leq L_1 \leq \dots$, the left ideal $\bigcup L_i$ contains all the L_i and it is a proper ideal of R. Indeed, if $\bigcup L_i = R$, there would exist an index $j \in \mathbb{N}$ such that $1 \in L_j$ and so $L_j = R$. So by Zorn's Lemma, $\mathcal{F}$ has a maximal element, which is clearly a maximal left ideal of R. □

Example 11.4. Consider the regular module $\mathbb{Z}$. Then $\mathbb{Z}p$ is a maximal submodule of $\mathbb{Z}$ for any prime number p. Moreover the ideal $\mathbb{Z}n$ is contained in $\mathbb{Z}p$ for any p such that $p|n$.

Remark 11.5. Let $\mathcal{M} \leq R$ a maximal left ideal of R. Clearly $R/\mathcal{M}$ is a simple R-module, and this shows that simple modules always exists in R-Mod, for any ring R.

Conversely, let $S \in R$-Mod be a simple module. So $S = Rx$ for an element $x \in S$ and let $\operatorname{Ann}_R(x) = \{r \in R | rx = 0\}$. $\operatorname{Ann}_R(x)$ is a maximal left ideal of R, since it is the kernel of the epimorphism $\varphi : R \to S$, $1 \mapsto x$, and hence $S \cong R/\operatorname{Ann}_R(x)$.

Finally, for any simple module S consider the module $\operatorname{Ann}_R(S) = \cap_{x \in S} \operatorname{Ann}_R(x)$. It is easy to show that $\operatorname{Ann}_R(S)$ is a two-sided ideal of R, called the *annihilator of the simple module S* (see Exercises 11.18 and 3.5).

The simple modules play an crucial role in the study of the category R-Mod, for instance:

Proposition 11.6. *Let $E \in R$-Mod be an injective module. The module E is a cogenerator of R-Mod if and only if for any simple module $S \in R$-Mod there exists a mono $0 \to S \to E$.*

Proof. Assume E is a cogenerator, so for any simple module $S \in R$-Mod there exists a mono $0 \to S \overset{f_S}{\to} E^{I_S}$, for a set I_S. Then there exist $j \in I_S$ such that $\pi_j \circ f : S \to E$ is not the zero map. So, since $\mathrm{Ker}(\pi_j \circ f) \leq S$, we get that for any simple module S there exists a mono $\pi_j \circ f : S \to E$. Conversely, assume the existence a mono $0 \to S \to E$ for any simple module S. Let $M \in R$-Mod, and let $x \in M$, $x \neq 0$. So $Rx \leq M$ and $Rx \cong R/\mathrm{Ann}_R(x)$. By Proposition 11.3 there exists a maximal submodule $\mathcal{M} \leq R$ such that $\mathrm{Ann}_R(x) \leq \mathcal{M}$. Consider the diagram

$$\begin{tikzcd}
0 \arrow[r] & Rx \cong R/\mathrm{Ann}_R(x) \arrow[r] \arrow[d] & M \arrow[ddl, dashed, "\varphi_x"] \\
& R/\mathcal{M} \cong S \arrow[d, "f"'] & \\
& E &
\end{tikzcd}$$

where f is a mono that exists by assumption and $\varphi_x : M \to E$ exists since E is injective. In particular $\varphi_x(x) \neq 0$. Hence we can construct a mono $\varphi : M \to E^M$, $x \mapsto (0, 0, \dots, 0, \varphi_x(x), 0, \dots, 0)$, where $\varphi_x(x)$ is the x^{th} position. $\square$

Corollary 11.7. *Let $\{S_\lambda\}_{\lambda \in \Lambda}$ be a set of representative of the simple modules (modulo isomorphisms) in R-*Mod*. Then the injective envelope $E(\oplus S_\lambda)$ is a minimal injective cogenerator of R-*Mod

Proof. The injective module $E(\oplus S_\lambda)$ cogenerates all the simple modules, so by the previous Proposition it is an injective cogenerator. If W is a injective cogenerator of R-Mod, since $S_\lambda \leq W$ for any $\lambda \in \Lambda$ (see the argument in the previous proof) one gets $\oplus S_\lambda \leq W$. Since $E(\oplus S_\lambda)$ is the injective envelope of $\oplus S_\lambda$, we conclude $E(\oplus S_\lambda) \overset{\oplus}{\leq} W$. $\square$

Remark 11.8. If there is a finite number of simple modules in R-Mod (modulo isomorphisms), $S_1, S_2, \dots, S_n$, then $E(\oplus S_i) = \oplus E(S_i)$ is a minimal injective cogenerator of R-Mod

Definition 11.9. *Let $M \in R$-*Mod*. The* socle *of M is the submodule* $\mathrm{Soc}(M) = \sum\{S | S$ *is a simple submodule of* $M\}$. *The* radical *of M is the submodule* $\mathrm{Rad}(M) = \cap\{N | N$ *is a maximal submodule of* $M\}$.

Remark 11.10. If M does not contain any simpe module, we set $\mathrm{Soc}(M) = 0$. If M does not contain any maximal submodule, we set $\mathrm{Rad}(M) = M$.

In the next Proposition we list some important properties of the socle and of the radical of a module. We leave the proofs for exercise.

Proposition 11.11. *Let $M \in R$-*Mod.

1. $\mathrm{Soc}(M) = \oplus\{S | S$ *is a simple submodule of* $M\}$. *In particular,* $\mathrm{Soc}(M)$ *is a* semisimple *module.*
2. $\mathrm{Soc}(M) = \cap\{L | L$ *is an essential submodule of* $M\}$.
3. $\mathrm{Rad}(M) = \sum\{U | U$ *is a superfluous submodule of* $M\}$.
4. *Let $f : M \to N$. Let* $f(\mathrm{Soc}(M)) \leq \mathrm{Soc}(N)$ *and* $f(\mathrm{Rad}(M)) \leq \mathrm{Rad}(N)$.
5. *if $M = \oplus_{\lambda \in \Lambda} M_\lambda$, then* $\mathrm{Soc}(M) = \oplus_{\lambda \in \Lambda} \mathrm{Soc}(M_\lambda)$ *and* $\mathrm{Rad}(M) = \oplus_{\lambda \in \Lambda} \mathrm{Rad}(M_\lambda)$.
6. $\mathrm{Rad}(M/\mathrm{Rad}(M)) = 0$ *and* $\mathrm{Soc}(\mathrm{Soc}(M)) = \mathrm{Soc}(M)$.
7. *If M is finitely generated, then* $\mathrm{Rad}(M)$ *is a superfluous submodule of M.*

Remark 11.12. It is clear that the radical can be described also by

$$\mathrm{Rad}(M) = \{x \in M |\ \varphi(x) = 0 \text{ for every } \varphi : M \to S \text{ with } S \text{ simple}\}$$

Indeed, given $\varphi : M \to S$ with S simple, the kernel of φ is a maximal submodule of M. Conversely, if N is a maximal submodule of M, then consider $\pi : M \to M/N$ where M/N is simple.

A crucial role is played by the radical of the regular module ${}_RR$.

Definition 11.13. *Let R be a ring. The* Jacobson radical *of R is the ideal* $\mathrm{Rad}({}_RR)$. *It is denoted by* $\mathrm{J}(R)$.

By the Remarks 11.5 and 11.12, the Jacobson radical of R can be described as the intersection of the annihilators $\mathrm{Ann}_R(S)$ of the simple left R-modules. In particular it is a two-sided ideal of R.

Lemma 11.14. *For every $M \in R$-Mod, $\mathrm{J}(R)M \leq \mathrm{Rad}(M)$*

Proof. Since $\mathrm{J}(R)$ annihilates any simple module S, all homomorphisms $M \to S$ are zero on $\mathrm{J}(R)M$ so, by Remark 11.12, $\mathrm{J}(R)M \leq \mathrm{Rad}(M)$ □

Proposition 11.15 (Nakayma's Lemma)**.** *Let M be a finitely generated R-module. If L is a submodule of M such that $L + \mathrm{J}(R)M = M$, then $L = M$.*

Proof. $L + \mathrm{J}(R)M = M$ implies $L + \mathrm{Rad}(M) = M$ and since $\mathrm{Rad}(M)$ is superfluous in M (see Proposition 11.11) we get $L = M$. □

We conclude with the following characterization of $\mathrm{J}(R)$

Proposition 11.16. *$J(R) = \{r \in R | 1 - xr$ has a left inverse for any $x \in R\}$*

Exercise

Exercise 11.17. Let $M \in R$-Mod be finitely generated. Show that, for any $L < M$, there exists a maximal submodule of M containing L. In particular, $\mathrm{Rad}(M) < M$.

Exercise 11.18. Show that, for any simple module $S \in R$-Mod, $\mathrm{Ann}_R(S)$ is a two-sided ideal of R.

Exercise 11.19. Let $S \in R$-Mod be a simple module. Prove that its injective envelops $E(S)$ is indecomposable. Show also that, if S and T are non-isomorphic simple modules, then $E(S)$ and $E(T)$ are non-isomorphic.

Exercise 11.20. Let $E \in R$-Mod an indecomposable injective module. Show that E is the injective envelope of its socle. Deduce that its socle is a simple module.

Exercise 11.21. Let $p \in \mathbb{N}$ a prime and $M = \{\frac{a}{p^n} \in \mathbb{Q} \mid a \in \mathbb{Z}, n \in \mathbb{N}\}$.

(1) Verify that $\mathbb{Z} \leq M \leq \mathbb{Q}$ in $\mathbb{Z}$-Mod.
(2) Let $\mathbb{Z}_{p^\infty} = M/\mathbb{Z}$. Show that $\mathbb{Z}_{p^\infty}$ is a divisible group.
(3) show that any $L \leq \mathbb{Z}_{p^\infty}$ is cyclic, generated by an element $\frac{1}{p^l}$, $l \in \mathbb{N}$.

Conclude the the lattice of the subgroups of $\mathbb{Z}_{p^\infty}$ is a well-ordered chain and so $\mathbb{Z}_{p^\infty}$ does not have any maximal subgroup.

12. Local rings

Definition 12.1. *A ring R is a* local ring *if all the non-invertible elements form a proper ideal of R.*

In other words, setting $\mathrm{U}(R) = \{x \in R \mid x \text{ is invertible}\}$, R is a local ring if $R \setminus \mathrm{U}(R)$ is a left ideal of R. One easily shows that $R \setminus \mathrm{U}(R)$ is a left ideal if and only if it is a two-sided ideal of R (Verify!).

Proposition 12.2. *Let R be a local ring. Then*

(1) *$R \setminus \mathrm{U}(R)$ is the Jacobson radical $\mathrm{J}(R)$ of R.*
(2) *$R/\mathrm{J}(R)$ is a division ring.*
(3) *there is a unique simple module (modulo isomorphisms) in R-Mod, $S = R/\mathrm{J}(R)$. In particular $E(R/\mathrm{J}(R))$ is the minimal injective cogenerator of R-Mod.*
(4) *The unique idempotent elements in R are 0 and 1.*

Proof. 1) Given a ring R, any left ideal of R is contained in $R \setminus \mathrm{U}(R)$. So, if R is local, $R \setminus \mathrm{U}(R)$ is the unique maximal ideal of ${}_RR$. In particular $R \setminus \mathrm{U}(R)$ is the Jacobson radical $\mathrm{J}(R)$ of R.
2) is obvious, since every element in $R/\mathrm{J}(R)$ is invertible.
3) It follows since $\mathrm{J}(R)$ is the unique maximal ideal of R.
4) Let e an idempotent element in a ring R. Observe that from $e(1-e) = 0$, if e is invertible one gets $e = 1$. So, if R is local and e is a not invertible idempotent, then $e \in R \setminus \mathrm{U}(R) = \mathrm{J}(R)$ and so the idempotent $1 - e \in \mathrm{U}(R)$ (otherwise we would have $1 \in J(R)$). Hence, $1 - e = 1$ and so $e = 0$. We conclude that the only idempotents in R are the trivial ones, i.e. 0 and 1. $\square$

Remark 12.3. If R is a local ring, then ${}_RR$ is an indecomposable R-module, since the direct summands of ${}_RR$ correspond to the idempotent elements of R (see Exercise 6.10).

If $M \in R$-Mod and $\mathrm{End}_R(M)$ is a local ring, then M is indecomposable. Indeed, to any decomposition $M = N \oplus L$, we can associate an idempotent element $\pi_N \in \mathrm{End}_R(M)$, $\pi_N : M \to M$, $n + l \mapsto n$. Thus $\pi_N = 0$ or $\pi_N = \mathrm{id}_M$ in $\mathrm{End}_R(M)$, from which we get $N = 0$ or $N = M$, respectively.

13. Finite length modules

Let $M \in R$-Mod. A sequence $0 = N_0 \leq N_1 \leq \cdots \leq N_{s-1} \leq N_s = M$ of submodules of M is called a *filtration* of M, with *factors* N_i/N_{i-1}, $i = 1, \cdots, s$. The *length* of the filtration is the number of non-zero factors.

Consider now a filtration $0 = N'_0 \leq N'_1 \leq \cdots \leq N'_{t-1} \leq N_t = M$; it is a *refinement* of the latter one if $\{N_i \mid 0 \leq i \leq s\} \subseteq \{N'_i \mid 0 \leq i \leq t\}$.

Two filtrations of M are said *equivalent* if $s = t$ and there exists a permutation $\sigma : \{0, 1, \cdots, s\} \to \{0, 1, \cdots, s\}$ such that $N_i/N_{i-1} \cong N'_{\sigma(i)}/N'_{\sigma(i-1)}$, for $i = 1, \cdots, s$.

Finally, a filtration $0 = N_0 \leq N_1 \leq \cdots \leq N_{s-1} \leq N_s = M$ of M is a *composition series* of M if the factors N_i/N_{i-1}, $i = 1, \cdots, s$, are simple modules. In such a case they are called *composition factors* of M.

Theorem 13.1. *Any two filtrations of M admit equivalent refinements.*

Proof. The proof follows from the following Lemma: *Let $U_1 \leq U_2 \leq M$ and $V_1 \leq V_2 \leq M$. Then*

$$(U_1 + U_2 \cap V_2)/(U_1 + V_1 \cap U_2) \cong (U_2 \cap V_2)/(U_1 \cap V_2) + (U_2 \cap V_1) \cong (V_1 + U_2 \cap V_2)/(V_1 + U_1 \cap V_2)$$

In our setting, consider $0 = N_0 \leq N_1 \leq \cdots \leq N_{s-1} \leq N_s = M$ and $0 = L_0 \leq L_1 \leq \cdots \leq L_{s-1} \leq L_t = M$ two filtrations of M. For any $1 \leq i \leq s$ and $1 \leq j \leq t$ define $N_{i,j} = N_{i-1} + (L_j \cap N_i)$ and $L_{j,i} = L_{j-1} + (N_j \cap L_i)$. Then

$$0 = N_{1,0} \leq N_{1,1} \leq \cdots \leq N_{1,t} \leq N_{2,0} \leq \cdots \leq N_{2,t} \leq \ldots N_{s,t} = M$$

is a refinement of the first filtration with factors $F_{i,j} = N_{i,j}/N_{i,j-1}$ and

$$0 = L_{1,0} \leq L_{1,1} \leq \cdots \leq L_{1,s} \leq L_{2,0} \leq \cdots \leq L_{2,s} \leq \ldots L_{t,s} = M$$

is a refinement of the second filtration with factors $G_{j,i} = L_{j,i}/L_{j,i-1}$. Clearly the two refinements have the same length st and by the stated lemma $F_{i,j} \cong G_{j,i}$. □

As a corollary of the previous Theorem, we get the following crucial result, known as Jordan-Hölder Theorem:

Theorem 13.2 (Jordan-Hölder). *Let $M \in R$-Mod be a module with a composition series of length l. Then*

(1) *Any filtration of M has length at most l and it can be refined in a composition series of M.*
(2) *All the composition series of M are equivalent and have length l.*

Proof. The proof follows by the previous proposition, since a composition series does not admit any non trivial refinement. □

This leads to the following definition:

Definition 13.3. *A module $M \in R$-Mod is of* finite length *if it admits a composition series. The length l of any composition series of M is called the* length *of L, denoted by $l(M)$.*

Example 13.4. (1) Any vector space of finite dimension over a field K is a K-module of finite length. Its length coincides with its dimension.
(2) The regular module ${}_{\mathbb{Z}}\mathbb{Z}$ is not of finite length.

In the following proposition we collect some relevant properties of finite length modules: some of them are trivial, some of them need a short proof that we leave for exercise.

Proposition 13.5. *Let $M \in R$-Mod be a finite length module. Then*

(1) *M is finitely generated*
(2) *for any $N \leq M$, N and M/N are of finite length*
(3) *If $0 \to N \to M \to L \to 0$ is an exact sequence, then $l(M) = l(N) + l(L)$*
(4) *M is a direct sums of indecomposable submodules.*
(5) $\mathrm{Soc}(M)$ *is an essential submodule of M*
(6) *$M/\operatorname{Rad}(M)$ is semisimple (i.e. it is a direct sum of simple modules)*
(7) *M contains a finite number of simple modules*

Proof. 4) If M is indecomposable the statement is trivially true. Otherwise we argue by induction on $l(M)$. If $M = V_1 \oplus V_2$, by point 3) we get that $l(V_1) < l(M)$ and $l(V_2) < l(M)$, so V_1 and V_2 are direct sums of indecomposable submodules.
5) Any $L \leq M$ has a composition series, so it contains a simple submodule, which is of course also a simple submodule of M.
6) By induction on $l(M/\operatorname{Rad}(M))$
7) By construction $\mathrm{Soc}(M) = \sum S_\lambda$ where the S_λ are the simple submodules of M. Since $\mathrm{Soc}(M)$ is semisimple, we get $\mathrm{Soc}(M) = \oplus S_\lambda$. Since $\mathrm{Soc}(M)$ is finitely generated (by (1) and (2)), it has only a finite number of summands. □

For modules of finite length the converse of Remark 12.3 holds.

Lemma 13.6. *Let $M \in R$-Mod a module of finite length $l(M) = n$. Then, for any $f : M \to M$, one has $M = \operatorname{Im} f^n \oplus \operatorname{Ker} f^n$.*

Proof. Consider the sequence of inclusions $\cdots \leq \operatorname{Im} f^2 \leq \operatorname{Im} f \leq M$. Since M has finite length, the inclusions are trivial for almost every $i \in \mathbb{N}$. In particular, there exists m such that $\operatorname{Im} f^m = \operatorname{Im} f^{2m}$ and we can assume $m = n$. Let now $x \in M$: hence $f^n(x) = f^{2n}(y)$ for $y \in M$ and so $x = f^n(y) - (x - f^n(y)) \in \operatorname{Im} f^n + \operatorname{Ker} f^n$.

Moreover, from the sequence of inclusions $0 \leq \operatorname{Ker} f \leq \operatorname{Ker} f^2 \leq \cdots \leq M$, arguing as before we can assume $\operatorname{Ker} f^n = \operatorname{Ker} f^{2n}$. Consider now $x \in \operatorname{Im} f^n \cap \operatorname{Ker} f^n$. So $x = f^n(y)$ and $f^n(x) = f^{2n}(y) = 0$. Hence $y \in \operatorname{Ker} f^n$ and so $x = f^n(y) = 0$. □

Proposition 13.7. *Let $M \in R$-Mod an indecomposable module of finite length. Then* $\operatorname{End}_R(M)$ *is a local ring*

Proof. Let $f : M \to M$. Since M is indecomposable, by the previous lemma one easily conclude that f is a mono if and only if it is an epi if and only if it is an iso if and only if $f^m \neq 0$ for any $m \in \mathbb{N}$ (see Exercise 13.9).

Thus let $U = \{f \in \operatorname{End}_R(M) | f \text{ is invertible } \}$. Let us show that $\operatorname{End}_R(M) \setminus U$ is an ideal of $\operatorname{End}_R(M)$. So let f, g in $\operatorname{End}_R(M) \setminus U$. The crucial point is to show that $f + g$ is not invertible (see Exercise 13.9). If $f + g$ would be invertible, there would exist $h \in U$ such that $(f + g)h = \mathrm{id}_M$. Since $g \notin U$, then $gh \notin U$, so gh would be nilpotent. Let r such that $(gh)^r = 0$: from $(\mathrm{id}_M - gh)(\mathrm{id}_M + gh + (gh)^2 + \cdots + (gh)^{r-1}) = \mathrm{id}_M$ we would conclude $fh \in U$ and so $f \in U$. $\square$

Theorem 13.8 (Krull-Remak-Schimdt-Azumaya). *Let $M \cong A_1 \oplus A_2 \oplus \cdots \oplus A_m \cong C_1 \oplus C_2 \oplus \cdots \oplus C_n$ where $\operatorname{End}_R(A_i)$ is a local ring for any $i = 1, \cdots, m$ and C_j is indecomposable for any $j = 1, \cdots, n$. Then $n = m$ and there exists a bijection $\sigma : \{1, \cdots, n\} \to \{1, \cdots, n\}$ such that $A_i \cong C_{\sigma(i)}$ for any $i = 1, \cdots, n$.*

Proof. By induction on m.

If $m = 1$, then $M \cong A_1$ is indecomposable and so we conclude.

If $m > 1$, consider the equalities

$$\mathrm{id}_{A_m} = \pi_{A_m} i_{A_m} = \pi_{A_m} (\sum_{j=1}^{n} i_{C_j} \pi_{C_j}) i_{A_m} = \sum_{j=1}^{n} \pi_{A_m} i_{C_j} \pi_{C_j} i_{A_m},$$

where the π's and the i's are the canonical projections and inclusions. Since $\operatorname{End}_R(A_m)$ is local, and in any local ring the sum of not invertible elements is not invertible, there exist $\bar{j}$ such that $\alpha = \pi_{A_m} i_{C_{\bar{j}}} \pi_{C_{\bar{j}}} i_{A_m}$ is invertible. We can assume $\bar{j} = n$, and consider $\gamma = \alpha^{-1} \pi_{A_m} i_{C_n} : C_n \to A_m$. Since $\gamma \pi_{C_n} i_{A_m} = \alpha^{-1}$, we get that γ is a split epimorphism. Since C_n is indecomposable, we conclude γ is an iso, and so $C_n \cong A_m$. Then apply induction to get the thesis. $\square$

The previous theorem says that if M is a module which is a direct sum of modules with local endomorphism rings, then any two direct sum decompositions of M into indecomposable direct summands are isomorphic. We conclude that the modules of finite length admits a unique (modulo isomorphisms) decomposition in indecomposable submodules

Exercises

Exercise 13.9. Let M an indecomposable R- module of finite length and $f \in \operatorname{End}_R(M)$. Show that the following are equivalent:

(1) f is a mono
(2) f is an epi
(3) f is an iso
(4) f is not nilpotent.

In particular, if f is not invertible, then gf is not invertible for any $g \in \operatorname{End}_R(M)$. Which of the previous implications hold also if M is of finite length but not indecomposable?

Exercise 13.10. Let M be an R-module.

(1) Let $M_1, M_2 \leq M$ such that $M_1 + M_2 = M$. Show that $M/M_1 \cap M_2 \cong M_1/M_1 \cap M_2 \oplus M_2/M_1 \cap M_2$.
(2) Suppose $\operatorname{Rad}(M) = M_1 \cap M_2$, where M_1 and M_2 are maximal submodules of M. Show that $M/\operatorname{Rad}(M) = S_1 \oplus S_2$ where S_1 and S_2 are simple R-modules.
(3) Let M be a finite length R-module. Show that $M/\operatorname{Rad}(M)$ is semisimple.

14. Finite dimensional K-algebras

Definition 14.1. *Let K be a field. A K-algebra Λ is a ring with a map $K \times \Lambda \to \Lambda$, $k \mapsto ka$, such that Λ is a K-module and $k(ab) = a(kb) = (ab)k$ for any $k \in K$ and $a, b \in \Lambda$. Λ is finite dimensional if $\dim_K(\Lambda) < \infty$.*

In other words, a K-algebra is a ring with a further structure of K-vector space, compatible with the ring structure.

Remark 14.2. Any element $k \in K$ can be identify with an element of Λ by means of $K \times \Lambda \to \Lambda$, $k \mapsto k \cdot 1$. Thanks to this identification, we get that $K \leq \Lambda$ so any Λ-module is in particular a K-module.

Example 14.3.
(1) The ring $M_n(K)$ is a finite dimensional K-algebra. with $\dim_K(M_n(K)) = n^2$. Any element $k \in K$ is identified with the diagonal matrix with k on the diagonal elements.
(2) The ring $K[x]$ is a K-algebra, not finite dimensional.

Proposition 14.4. *Let Λ be a finite dimensional K-algebra. Then $M \in \Lambda\text{-Mod}$ is finitely generated if and only if $\dim_K(M) < \infty$.*

Proof. Assume $\dim_K(\Lambda) = n$ and $\{a_1, \ldots, a_n\}$ a K-basis.

If $\{m_1, \ldots, m_r\}$ is a set of generator of M as Λ-module, then one verifies that $\{a_i m_j\}_{i=1,\ldots,n}^{j=1,\ldots,r}$ is a set of generators for M as K-module.

Conversely, if M is generated by $\{m_1, \ldots, m_s\}$ as K-module, since $K \leq \Lambda$, one gets that M is generated by $\{m_1, \ldots, m_s\}$ also as Λ-module.

□

In the following we denote by Λ-mod the full subcategory of Λ-Mod consisting on the finitely generated Λ-modules.

Corollary 14.5. *Any finitely generated module $M \in \Lambda\text{-mod}$ is a finite length module, and $l(M) \leq \dim_K(M)$.*

Proof. Since any $M \in \Lambda$-mod is a finite dimensional vector space, M admits a composition series in K-mod of length n, where $\dim_K(M) = n$. So any filtration of M in Λ-Mod is at most of length n and any refinement is a refinement also in K-mod. Thus we conclude. □

Proposition 14.6. *Let $M, N \in \Lambda\text{-mod}$. Then $\mathrm{Hom}_\Lambda(M, N)$ is a finitely generated K-module. In particular, $\Gamma = \mathrm{End}_\Lambda(M)$ is a finite dimensional K-algebra and M_Γ is finitely generated.*

Proof. The K-module $\mathrm{Hom}_\Lambda(M, N)$ is a K-submodule of $\mathrm{Hom}_K(M, N)$, and the latter is finitely generated by a well-known result of linear algebra. Thus $\mathrm{Hom}_\Lambda(M, N)$ is finitely generated as K-module. In particular, $\Gamma = \mathrm{Hom}_\Lambda(M, M)$ is a finite dimensional K-algebra. Since M has a natural structure of right Γ-module and it is a finitely generated K-module, it is also a finitely generated Γ-module. □

In the sequel, let Λ be a finite dimensional K-algebra. We want to give a complete description of the simple, the indecomposable projective and the indecomposable injective modules in Λ-mod.

Since ${}_\Lambda\Lambda$ is of finite length, it admits a unique decomposition in indecomposable submodules. The indecomposable summands of a ring are in correspondence with the idempotent elements, so there exists a set $\{e_1, e_2, \ldots, e_n\}$ of idempotents of Λ such that ${}_\Lambda\Lambda = \Lambda e_1 \oplus \ldots \Lambda e_n$. Moreover we can assume $1 = e_1 + \cdots + e_n$ and one easily shows that $e_i e_j = 0$ for any $i \neq j$ (a set of idempotents with this property is called *orthogonal*). Finally since Λe_i are indecomposable, each idempototent e_i is *primitive* (i.e. it cannot be a sum of two non-zero orthogonal idempotents, see Exercise 14.7). Notice that $\Lambda_\Lambda = e_1\Lambda \oplus \cdots \oplus e_n\Lambda$ is a decomposition in indecomposable summands of the regular right module Λ_Λ. From this discussion it follows that, for $i = 1, \ldots, n$, the $P_i = \Lambda e_i$ are indecomposable projective left Λ-modules and the $Q_i = e_i\Lambda$ are indecomposable projective right Λ-modules.

Moreover, if $P \in \Lambda$-mod is an indecomposable projective, then P is a direct summand of Λ^m for a suitable $m > 0$ (See Exercise 8.11) . Since Λ^m is of finite length, the unique decomposition of Λ^m in indecomposable summands is $\Lambda^m = P_1^m \oplus \ldots P_n^m$, so we conclude that P is isomorphic to P_j for a suitable $j \in \{1, \ldots, n\}$

Consider now the functor $D : \Lambda\text{-mod} \to \text{mod-}\Lambda$, $M \mapsto D(M) = \mathrm{Hom}_K({}_\Lambda M, K)$. Notice that the functor D is well-defined, since $\mathrm{Hom}_K({}_\Lambda M, K)$ is a right Λ module and it is finitely generated since $\dim_K(\mathrm{Hom}_K({}_\Lambda M, K)) < \infty$. For simplicity, we denote by D the analogous functor $D : \text{mod-}\Lambda \to \Lambda\text{-mod}$, $N \mapsto D(N) = \mathrm{Hom}_K(N_\Lambda, K)$. For any $M \in \Lambda$-mod define the *evaluation morphism* $\delta_M : M \to D^2(M)$, $x \mapsto \delta_M(x)$, where $\delta_M(x) : D(M) \to K$, $\varphi \mapsto \varphi(x)$. One easily verify that δ_M is an isomorphism for any $M \in \Lambda$-mod. Similarly one define δ_N for any $N \in$ mod-Λ, which is an iso for any N.

It turns out that $\delta : 1 \to D^2$ is a natural transformation (see Definition 7.10) which defines a duality between Λ-mod and mod-Λ. Thanks to the properties of dualities described at the end of Section 7 , we get in particular that P is indecomposable projective in Λ-mod if and only if $D(P)$ is indecomposable injective in mod-Λ; dually, E is indecomposable injective in Λ-mod if and only if $D(E)$ is indecomposable injective in mod-Λ. Moreover S is simple in Λ-mod if and only if $D(S)$ is simple in mod-Λ.

Notice the dual concepts of cover and generator are the concepts of envelope and cogenerator, respectively. So, thanks to the duality (D, D), we conclude that $D(\Lambda_\Lambda)$ is the minimal injective cogenerator of Λ-mod and the $E_i = D(Q_i)$ are the unique indecomposable injective modules in Λ-mod. Observe that if S and T are non isomorphic simple modules in Λ-mod, then their injective envelopes $E(S)$ and $E(T)$ are non isomorphic indecomposable injective modules; moreover any indecomposable injective module E is the injective envelope of its simple socle (see Exercises 11.19 and 11.20). We conclude that in Λ-mod there are exactly n non-isomorphic simple modules, which are the socle of each indecomposable injective E_i, for $i = 1, \dots, n$.

One can easily verify that, given any $M \in \Lambda$-mod, $P(M)$ is a projective cover of M if and only if $D(P(M))$ is an injective envelope of $D(M)$. Hence, since in mod-Λ there exist injective envelopes, thanks to the duality, we get that any module in Λ-mod has a projective cover (i.e., Λ is a semiperfect ring, see Section 8) Let us see how to compute injective envelopes and projective covers.

In the sequel denote by $\mathrm{J} = \mathrm{J}(\Lambda) = \mathrm{Rad}({}_\Lambda\Lambda)$ the Jacobson radical of Λ. First observe that, by Lemma 11.14 and since J is a two-sided ideal, we get $J\Lambda e_i = Je_i \leq \mathrm{Rad}(\Lambda e_i)$ for any $i = 1, \dots, n$. Moreover recall that $J = \mathrm{Rad}({}_\Lambda\Lambda) = \mathrm{Rad}(\Lambda e_1) \oplus \cdots \oplus \mathrm{Rad}(\Lambda e_n)$ (see Proposition 11.11). Hence, since the sum of the $\mathrm{Rad}(\Lambda e_i)$ is direct and $Je_i \leq \mathrm{Rad}(\Lambda e_i)$, we get also $J = J1 = J(e_1 + \dots e_n) = Je_1 \oplus \dots Je_n$. Thus, $\dim_K(J) = \dim_K(Je_1) + \cdots \dim_K(Je_n) \leq \dim_K(\mathrm{Rad}(\Lambda e_1)) + \cdots + \dim_K(\mathrm{Rad}(\Lambda e_n)) = \dim_K(\mathrm{Rad}(\Lambda))$, from which we get $\dim_K(Je_i) = \dim_K(\mathrm{Rad}(\Lambda e_i))$ for any $i = 1, \dots, n$. We conclude that $Je_i = \mathrm{Rad}(\Lambda e_i)$ for any $i = 1, \dots, n$.

It can be proved that the same holds for any $M \in \Lambda$-mod, that is $JM = \mathrm{Rad}(M)$ for any $M \in \Lambda$-mod.

After this discussion, by Proposition 11.11 we get that $\mathrm{J}\, e_1$ is superfluous in Λe_i, so Λe_i is the projective cover of $\Lambda e_i / \mathrm{J}\, e_i$ (see Theorem 8.8). Moreover, by Proposition 13.5, $\Lambda e_i / \mathrm{J}\, e_i$ is semisimple so, since Λe_i is indecomposable, we get that $\Lambda e_i / \mathrm{J}\, e_i$ is a simple module (see Exercise 14.9). Notice that, since $\Lambda e_i \not\cong \Lambda e_j$ for $i \neq j$, we get $\Lambda e_i / \mathrm{J}\, e_i \not\cong \Lambda e_j / \mathrm{J}\, e_j$ for $i \neq j$. Then the $S_i = \Lambda e_i / \mathrm{J}\, e_i$, $i = 1, \dots n$ are non-isomorphic simple modules in Λ-mod. Since we already know that there are exactly n non-isomorphic simple modules, we conclude that $S_1, \cdots, S_n$ is a complete list of the non-isomorphic simple modules in Λ-mod. Similarly, $T_i = e_i\Lambda / e_i \mathrm{J}$ is a complete list of the simple modules in mod-Λ.

Arguing on the annihilators of the simple modules, it is not difficult to show that the action of the functor D on the simple modules respect the idempotents, that is $S_i = D(T_i)$ for any $i = 1, \cdots, n$. Since we already know that Q_i is the projective cover of T_i, we get that $E_i = D(Q_i)$ is the injective envelope of S_i for any $i = 1, \cdots, n$.

How to compute injective envelopes and projective covers for any $M \in \Lambda$-mod? Since M is of finite length, $M/\mathrm{Rad}(M)$ and $\mathrm{Soc}(M)$ are semisimple. Let $M/\mathrm{Rad}(M) = S_1 \oplus \cdots \oplus S_r$ (eventually with a certain multiplicity). Then $P(M) = P(S_1) \oplus \cdots \oplus P(S_r)$. Similarly, if $\mathrm{Soc}(M) = S_1 \oplus \cdots \oplus S_m$, then $E(M) = E(S_1) \oplus \cdots \oplus E(S_m)$. (see Exercises 14.10 and 14.11).

To conclude: in Λ-mod the simples are the $S_i = \Lambda e_i / \mathrm{J}\, e_i$, the indecomposable projectives are the $P_i = \Lambda e_i$, the indecomposable injectives are the $E_i = D(e_i\Lambda)$, for $i = 1, \dots, n$. The regular module ${}_\Lambda\Lambda$ is the minimal projetive generator of Λ-mod and $D(\Lambda_\Lambda)$ is the minimal injective cogenerator of Λ-mod. Moreover P_i is the projective cover of S_i and E_i is the injective envelope of S_i.

In mod-Λ the simples are the $T_i = \Lambda e_i / \mathrm{J}\, e_i = D(S_i)$, the indecomposable projectives are the $Q_i = e_i\Lambda$, the indecomposable injectives are the $F_i = D(\Lambda e_i)$. The regular module Λ_Λ is the minimal projetive generator of mod-Λ and $D({}_\Lambda\Lambda)$ is the minimal injective cogenerator of mod-Λ. Moreover Q_i is the projective cover of T_i and F_i is the injective envelope of T_i.

Exercises

Exercise 14.7. A idempotent element $e \in \Lambda$ is called *primitive* if it is not a sum of two non zero orthogonal idempotents. Show that Λe is indecomposable if and only if e is primitive.

Exercise 14.8. Find the decomposition in indecomposable summands of the $\mathbb{C}$-algebras:

(1) $M_2(\mathbb{C})$= the ring of 2×2 matrices with coefficients in $\mathbb{C}$
(2) R= the ring of the 2×2 upper triangular matrices with coefficients in $\mathbb{C}$

Exercise 14.9. Let Λ a finite dimensional algebra. Let $M = N_1 \oplus N_2$ and assume that P_1 and P_2 are projective covers of N_1 and N_2, respectively. Show that $P_1 \oplus P_2$ is the projective cover of M. Similarly, assume that E_1 and E_2 are the injective envelopes of N_1 and N_2, respectively, then $E_1 \oplus E_2$ is the injective envelope of M.

Exercise 14.10. Let $M \in \Lambda$-mod and $\mathrm{Soc}(M) = S_1 \oplus \dots S_r$. Show that there exists an essential monomorphism $0 \to M \to E(S_1) \oplus \cdots \oplus E(S_r)$ and conclude that $E(M) = E(\mathrm{Soc}(M)) = E(S_1) \oplus \cdots \oplus E(S_r)$.(Hint: $\mathrm{Soc}(M)$ is essential in M, so...)

Exercise 14.11. Let $M \in \Lambda$-mod and $M/\mathrm{Rad}(M) = S_1 \oplus \dots S_r$. Show that there exists a superfluous epimorphism $P(S_1) \oplus \cdots \oplus P(S_r) \to M \to 0$ and conclude that $P(M) = P(M/\mathrm{Rad}(M)) = P(S_1) \oplus \cdots \oplus P(S_r)$. (Hint: $\mathrm{Rad}(M)$ is superfluous in M, so...)