Representation theory of algebras

an introduction

Lidia Angeleri, Rosanna Laking, Francesca Mantese
University of Verona
Master Program Mathematics
2018/19

(updated on March 28, 2019)

Important: These notes will be updated on a regular basis during the course.
In the second part, many proofs are omitted or just sketched.
The complete arguments will be explained in the lectures!

Contents

1 RINGS

1.1 Reminder on rings

Recall that a *ring* $(R, +, \cdot, 0, 1)$ is given by a set R together with two binary operations, an addition $(+)$ and a 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 unity 1), and multiplication is left and right distributive over addition. A ring whose multiplicative structure is abelian is called a *commutative ring*.
Given two rings R, S, a map $\varphi : R \to S$ is a *ring homomorphism* if for any two elements $a, b \in R$ we have $\varphi(a + b) = \varphi(a) + \varphi(b), \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$, and $\varphi(1_R) = 1_S$.

Examples:

1. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are commutative rings.
2. Let k be a field; the ring $k[x_1, \ldots, x_n]$ of polynomials in the variables $x_1, \ldots, x_n$ 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.
4. Given an abelian group $(G, +)$, the group homomorphisms $f : G \to G$ form a ring $\operatorname{End} G$, called the *endomorphism ring* of G, with respect to the natural operations given by pointwise addition $f + g : G \to G$, $a \mapsto f(a) + g(a)$ and composition of maps $g \circ f : G \to G$, $a \mapsto g(f(a))$. The unity is given by the identity map $1_G : G \to G$, $a \mapsto a$.
5. Given a ring R, the opposite ring R^{op} has the same additive structure as R and opposite multiplication $(*)$ given by $a * b = b \cdot a$.

1.2 Finite dimensional algebras

Definition: Let k be a field. A *k-algebra* Λ is a ring with a map $k \times \Lambda \to \Lambda$, $(\alpha, a) \mapsto \alpha a$, such that Λ is a k-vector space and $\alpha(ab) = a(\alpha b) = (ab)\alpha$ for any $\alpha \in k$ 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: An element $\alpha \in k$ can be identified with an element of Λ by means of the embedding $k \to \Lambda$, $\alpha \mapsto \alpha \cdot 1$. Thanks to this identification, we get that $k \leq \Lambda$.

Examples: Let k be a field.

1. The ring $M_n(k)$ is a finite dimensional k-algebra with $\dim_k(M_n(k)) = n^2$. Any element $\alpha \in k$ is identified with the diagonal matrix with α on the diagonal elements.

2. The ring $k[x]$ is a k-algebra, it is not finite dimensional.

3. Given a finite group $G = \{g_1, \ldots, g_n\}$, let kG be the k-vector space with basis $\{g_1, \ldots, g_n\}$ and multiplication given by $(\sum_{i=1}^n \alpha_i g_i) \cdot (\sum_{j=1}^n \beta_j g_j) = \sum_{i,j=1}^n \alpha_i \beta_j g_i g_j$. Then kG is a finite dimensional k-algebra, called the *group algebra* of G over k.

1.3 Quivers and path algebras

Definition. A *quiver* $Q = \{Q_0, Q_1\}$ is an oriented graph where Q_0 is the set of vertices and Q_1 is the set of arrows $i \xrightarrow{\alpha} j$ between the vertices. If Q_0 and Q_1 are finite sets, then Q is called a *finite* quiver.

Examples: $\mathbb{A}_n : \underset{1}{\bullet} \xrightarrow{\alpha_1} \underset{2}{\bullet} \xrightarrow{\alpha_2} \underset{3}{\bullet} \ldots \bullet \xrightarrow{\alpha_{n-1}} \underset{n}{\bullet}$, or $\bullet \circlearrowleft \alpha$, or $\bullet \rightrightarrows \bullet$

Definition. Let $Q = \{Q_0, Q_1\}$ be a finite quiver.

(1) An ordered sequence of arrows $\underset{i}{\bullet} \xrightarrow{\alpha_1} \bullet \xrightarrow{\alpha_2} \bullet \ldots \bullet \xrightarrow{\alpha_n} \underset{j}{\bullet}$, denoted by $(i|\alpha_1, \ldots, \alpha_n|j)$, is called a *path* in Q. A path $(i|\alpha_1, \ldots, \alpha_n|i)$ starting and ending in the same vertex is called an *oriented cycle.* For each vertex i there is the *trivial (or lazy) path* $e_i = (i\|i)$.

(2) For a field k, let kQ be the k-vector space having the paths of Q as k-basis. We now define an algebra structure on kQ. Hereby, the multiplication of two paths p and p' with the end point of p' coinciding with the starting point of p will correspond to the composition of arrows.

For paths $p' = (k|\beta_1, \ldots, \beta_m|l)$, and $p = (i|\alpha_1, \ldots, \alpha_n|j)$ of Q we set

$$p \cdot p' = \begin{cases} (k|\beta_1, \ldots, \beta_m, \alpha_1, \ldots, \alpha_n|j) & \text{if } l = i \\ 0 & \text{else.} \end{cases}$$

In particular, the trivial paths satisfy $p \cdot e_i = e_j \cdot p = p$ and

$$e_i \cdot e_j = \begin{cases} e_i & \text{if } i = j \\ 0 & \text{else} \end{cases}$$

and the unity is given by $1_{kQ} = \sum_{i \in Q_0} e_i$. The algebra kQ is called the *path algebra* of Q over k. It is finite dimensional if and only if Q has no oriented cycles.

We simplify the notation and write $\alpha_n \ldots \alpha_1 = (i|\alpha_1, \ldots, \alpha_n|j)$.

Examples:

(1) $k\mathbb{A}_n$ is isomorphic to $\begin{pmatrix} k & & 0 \\ \vdots & \ddots & \\ k & \dots & k \end{pmatrix}$.

In fact, the only paths in $\mathbb{A}_n$ are the trivial paths and the paths $\alpha_{j-1}\dots\alpha_i = (i \mid \alpha_i\alpha_{i+1}\dots\alpha_{j-1} \mid j)$ for $1 \leq i < j \leq n$. So, if E_{ji} is the $n \times n$-matrix with 1 in the i-th entry of the j-th row and zero elsewhere, we obtain the desired isomorphism by mapping $e_i \mapsto E_{ii}$, and $\alpha_{j-1}\dots\alpha_i \mapsto E_{ji}$ for $1 \leq i < j \leq n$.

(2) The path algebra of the quiver $\bullet \circlearrowright \alpha$ is isomorphic to $k[x]$ via the assignment $e_1 \mapsto 1$, and $\alpha \mapsto x$.

(3) The path algebra of the quiver $\bullet \overset{\alpha}{\underset{\beta}{\rightrightarrows}} \bullet$ is called *Kronecker algebra.*

It is isomorphic to the triangular matrix ring $\begin{pmatrix} k & 0 \\ k^2 & k \end{pmatrix}$ via the assignment

$e_1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, $e_2 \mapsto \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$, $\alpha \mapsto \begin{pmatrix} 0 & 0 \\ (1,0) & 0 \end{pmatrix}$, $\beta \mapsto \begin{pmatrix} 0 & 0 \\ (0,1) & 0 \end{pmatrix}$

2 MODULES

2.1 Left and right modules

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

(L1) $1x = x$

(L2) $(rs)x = r(sx)$

(L3) $r(x+y) = rx + ry$

(L4) $(r+s)x = rx + sx$

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

Examples:

1. Any abelian group G is a left $\mathbb{Z}$-module by defining $nx = \underbrace{x + \cdots + x}_{n\ times}$ for $x \in G$ and $n > 0$, and correspondingly for $n \leq 0$.
2. Given a field k, any vector space V over k is a left k-module.
3. Any ring R is a left R-module, by using the left multiplication of R on itself. It is called the *regular* module.

4. Consider the zero element of the ring R. Then the abelian group $\{0\}$ is trivially a left R-module.

Remark. Consider M an abelian group with endomorphism ring $\operatorname{End} M$. Every ring homomorphism $\lambda : R \to \operatorname{End} M$, $r \mapsto \lambda(r)$ gives a structure of left R-module on M. Indeed, from the properties of ring homomorphisms it follows that for any $r, s \in R$ and $x, y \in M$

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

in other words, we can consider $\lambda(r)$ acting on the elements of M as a left multiplication by the element $r \in R$, and we can define $rx := \lambda(r)(x)$. Conversely, to any left R-module M, we can associate a ring homomorphism $\lambda : R \to \operatorname{End} M$ by defining $\lambda(r) : M \to M$, $x \mapsto rx$.

Similarly, we define right R-modules:

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

(R1) $x1 = x$

(R2) $x(rs) = (xr)s$

(R3) $(x + y)r = xr + yr$

(R4) $x(r + s) = xr + xs$

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

Remark (1) 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 (R1)–(R4) and so M is also a right R-module. The crucial point is that, in the second axiom, since R is commutative we have $x(rs) = (rs)x = (sr)x = s(rx) = (rx)s = (xr)s$.
(2) Consider M an abelian group with endomorphism ring $\operatorname{End} M$. Every ring homomorphism $\rho : R \to (\operatorname{End} M)^{op}$, $r \mapsto \rho(r)$ gives a structure of right R-module on M, and conversely, to any right R-module M, we can associate a ring homomorphism $\rho : R \to (\operatorname{End} M)^{op}$ by defining $\rho(r) : M \to M$, $x \mapsto xr$ (check!).

We will mainly deal with left modules. So, in the following, unless otherwise is stated, with *module* we always mean *left module*.

Remark. Given ${}_RM$, for any $x \in M$ and $r \in R$, we have

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

2.2 Submodules and quotient modules

Definition: 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 inherited from M). We write $L \leq M$.

Examples:

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 k-subspaces of V.
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: 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 $(r, \overline{x}) \mapsto \overline{rx}$ (indeed, 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 $rx - ry = r(x - y) \in L$, that is, $\overline{rx} = \overline{ry}$).

2.3 Homomorphisms of modules

Definition: 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 $r, s \in R$.

Remarks: (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 $\mathrm{Hom}_R(M, N) = \{f \mid f : M \to N \text{ is a homomorphism}\}$ 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 $\mathrm{End}_R(M) = \{f \mid f : M \to M \text{ is a homomorphism}\}$ has a natural structure of ring, called the *endomorphism ring* of M. The identity homomorphism $\mathrm{id}_M : M \to M$, $m \mapsto m$, is the unity of the ring.

Definition: Given a homomorphism $f \in \operatorname{Hom}_R(M, N)$, the *kernel* of f is the set $\operatorname{Ker} f = \{x \in M \mid f(x) = 0\}$. The *image* of f is the set $\operatorname{Im} f = \{y \in N \mid y = f(x) \text{ for } x \in M\}$. It is easy to verify that $\operatorname{Ker} f \leq M$ and $\operatorname{Im} f \leq N$. Thus we can define the *cokernel* of f as the quotient module $\operatorname{Coker} f = N/\operatorname{Im} f$.

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

Remarks: (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 $p : M \to M/L$, $m \mapsto \overline{m}$ which is the usual quotient map.
(2) For any M the trivial map $0 \to M$, $0 \mapsto 0$, is a monomorphism, and the trivial map $M \to 0$, $m \mapsto 0$, is an epimorphism.
(3) Of course, $f \in \operatorname{Hom}_R(M, N)$ is an isomorphism if and only if there exist $g \in \operatorname{Hom}_R(N, M)$ such that $gf = \operatorname{id}_M$ and $fg = \operatorname{id}_N$. In such a case g is unique, and we usually denote it as f^{-1}.

2.4 Homomorphism theorems

Proposition 2.4.1. (Factorization of homomorphisms) *Given $f \in \operatorname{Hom}_R(M, N)$ and a submodule $L \leq M$ which is contained in $\operatorname{Ker} f$, there is a unique homomorphism $\overline{f} \in \operatorname{Hom}_R(M/L, N)$ such that $\overline{f}\, p = f$. We have $\operatorname{Ker} \overline{f} = \operatorname{Ker} f/L$ and $\operatorname{Im} \overline{f} = \operatorname{Im} f$.*
In particular, f induces an isomorphism $M/\operatorname{Ker} f \cong \operatorname{Im} f$.

Proof. The induced map $\overline{f} : M/L \to N$, $\overline{m} \mapsto f(m)$ is a homomorphism. Moreover, when $L = \operatorname{Ker} f$ it is clearly a monomorphism, inducing an isomorphism $M/\operatorname{Ker} f \to \operatorname{Im} f$. □

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

Proposition 2.4.2. (Isomorphism theorems) (1) *If $L \leq N \leq M$, then*

$$(M/L)/(N/L) \cong M/N.$$

(2) *If $L, N \leq M$, denote by $L + N = \{m \in M \mid m = l + n \text{ for } l \in L \text{ and } n \in N\}$. Then $L + N$ is a submodule of M and*

$$(L + N)/N \cong L/(N \cap L).$$

2.5 Bimodules

Definition: Let R and S be rings. An abelian group M is an *R-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 ${}_RM_S$.

Examples: Let ${}_RM$ be a left R-module. Then M is a right $\mathrm{End}_R(M)^{op}$-module via the multiplication $mf = f(m)$ (check!) and we have a bimodule

$${}_RM_{\mathrm{End}_R(M)^{op}}.$$

Indeed $(rm)f = f(rm) = rf(m) = r(mf)$ for any $r \in R$, $m \in M$ and $f \in S$.

Given a bimodule ${}_RM_S$ and a left R-module N, the abelian group $\mathrm{Hom}_R(M, N)$ is naturally endowed with a structure of left S-module, by defining $(sf)(x) := f(xs)$ for any $f \in \mathrm{Hom}_R(M, N)$ and any $x \in M$. (crucial point: $(s_1(s_2f))(x) = (s_2f(xs_1)) = f(xs_1s_2) = ((s_1s_2)f)(x))$.
Similarly, if ${}_RN_T$ is a left R- right T-bimodule and ${}_RM$ is a left R-module, then $\mathrm{Hom}_R(M, N)$ is naturally endowed with a structure of right T-module, by defining $(ft)(x) := f(x)t$ (Check! crucial point: $(f(t_1t_2))(x) = f(x)(t_1t_2) = (f(x))t_1)t_2 = ((ft_1)(x))t_2 = ((ft_1)t_2)(x))$.
Moreover, if ${}_RM_S$ and ${}_RN_T$ are bimodules, we have an S-T-bimodule (check!)

$${}_S\,\mathrm{Hom}_R({}_RM_S, {}_RN_T)_T.$$

Arguing in a similar way for right R-modules, if ${}_SM_R$ and ${}_TN_R$ are bimodules, we have an T-S-bimodule

$${}_T\,\mathrm{Hom}_R({}_SM_R, {}_TN_R)_S$$

via $(tf)(x) = t(f(x))$ and $(fs)(x) = f(sx)$.

2.6 Sums and products of modules

Let I be a set and $\{M_i\}_{i\in I}$ a family of R-modules. The cartesian product

$$\prod_I M_i = \{(x_i) \mid x_i \in M_i\}$$

has a natural structure of left R-module, by defining the operations componentwise:

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

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

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

(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 $\prod_I M_i = \{(x_i) \mid x_i \in M_i\} = \oplus_I M_i$. For any component $j \in I$ there are canonical homomorphisms

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

called the *projection* on the j^{th}-component and the *injection* of the j^{th}-component. They are epimorphisms and monomorphisms, 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

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

Let ${}_R M$ 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

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

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 2.6.1. Let ${}_R M$ 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 *(innner) direct sum* of its submodules M_i. Often we omit the word "innner" and if $M = \sum_I M_i$ and α is an isomorphism, we say that M is the direct sum of the submodules M_i and we write $M = \oplus_I M_i$.

Similarly, given a family of modules $\{M_i\}_{i\in I}$ with the (outer) direct sum $M = \oplus_I M_i$, we can identify the M_i with their images under the injection in M and view M as an (inner) direct sum of these submodules.

2.7 Direct summands

Definition: (1) A submodule ${}_RL \leq {}_RM$ is a *direct summand* of M if there exists a submodule ${}_RN \leq {}_RM$ such that M is the direct sum of L and N. Then N is called a *complement* of L.
(2) A module M is said to be *indecomposable* if it only has the trivial direct summands 0 and M.

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

Remark 2.7.1. (1) Let ${}_RL, {}_RN \leq {}_RM$. Then $M = L \oplus N$ if and only if $L + N = M$ and $L \cap N = 0$.
(2) Let $f \in \operatorname{Hom}_R(L, M)$ and $g \in \operatorname{Hom}_R(M, L)$ be homomorphisms such that $gf = \mathrm{id}_L$. Then $M = \operatorname{Im} f \oplus \ker g$.

Examples:

1. Consider the $\mathbb{Z}$-module $\mathbb{Z}/6\mathbb{Z}$. Then $\mathbb{Z}/6\mathbb{Z} = 3\mathbb{Z}/6\mathbb{Z} \oplus 2\mathbb{Z}/6\mathbb{Z}$.
2. The regular module ${}_{\mathbb{Z}}\mathbb{Z}$ is indecomposable.
3. Let k be a field and V a k-module. Then, by a well-known result of linear algebra, any $L \leq V$ is a direct summand of V.
4. Let $R = \begin{pmatrix} k & 0 \\ k & k \end{pmatrix}$. Then $R = P_1 \oplus P_2$, where $P_1 = \{\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \mid a, b \in k\}$ and $P_2 = \{\begin{pmatrix} 0 & 0 \\ 0 & c \end{pmatrix} \mid c \in k\}$.

2.8 Representations of quivers

Definition. Let Q be a finite quiver without oriented cycles, k a field, and let $\Lambda = kQ$.

(1) A *(finite dimensional) representation* V of Q over k is given by a family of (finite dimensional) k-vector spaces $(V_i)_{i \in Q_0}$ indexed by the vertices of Q and a family of k-homomorphisms $(f_\alpha \colon V_i \to V_j)_{i \xrightarrow{\alpha} j \in Q_1}$ indexed by the arrows of Q.

(2) Given two representations V and V' of Q over k, a morphism $h : V \to V'$ is given by a family of k-homomorphism $(h_i \colon V_i \to V_i')_{i \in Q_0}$ such that the diagram

$$\begin{array}{ccc} V_i & \xrightarrow{f_\alpha} & V_j \\ {\scriptstyle h_i}\downarrow & & \downarrow{\scriptstyle h_j} \\ V_i' & \xrightarrow[f_\alpha']{} & V_j' \end{array}$$

commutes for all arrows $i \xrightarrow{\alpha} j \in Q_1$.

Remark: Every representation of a quiver Q gives rise to a module over the path algebra kQ, and morphisms of representations give rise to module homomorphisms between the corresponding modules.
Indeed, if $((V_i)_{i\in Q_0}, (f_\alpha\colon V_i \to V_j)_{i\xrightarrow{\alpha}j\in Q_1})$ is a representation, we consider the vector space

$$M := \bigoplus_{i\in Q_0} V_i$$

and we define a left kQ-module structure on it. For $v = (v_i)_{i\in Q_0}$, left multiplication by the lazy path is given by $e_i \cdot v = (0,\ldots,v_i,\ldots,0)$ and multiplication by a path $p = (i|\alpha_1,\ldots,\alpha_n|j)$ yields an element $p\cdot v$ with j-th entry $f_{\alpha_n}\ldots f_{\alpha_1}(v_i)$ and all other entries zero.
In other words, denoting by ι_j and π_i the canonical injections and projections in the j-th and on the i-th component, respectively, we have for the lazy paths

$$e_i \cdot v = \iota_i \pi_i(v)$$

and for $p = (i|\alpha_1,\ldots,\alpha_n|j)$

$$p\cdot v = \iota_j f_{\alpha_n}\ldots f_{\alpha_1}\pi_i(v).$$

Multiplication with an arbitrary linear combination of paths is defined correspondingly.

Conversely, every kQ-module gives rise to a representation, and module homomorphisms give rise to morphisms between the corresponding representations.
Indeed, if M is a left kQ-module, we set

$$V_i = e_i M$$

to get a family of vector spaces indexed over Q_0. Moreover, given an arrow $i \xrightarrow{\alpha} j$, we define a linear map

$$f_\alpha : e_i M \to e_j M,\ e_i m \mapsto e_j \alpha e_i m.$$

In this way we obtain a representation $((V_i)_{i\in Q_0}, (f_\alpha\colon V_i \to V_j)_{i\xrightarrow{\alpha}j\in Q_1})$ of Q.
The correspondence between modules and representations will be made more precise later.

Examples: (1) A representation of $\mathbb{A}_2 : 1 \xrightarrow{\alpha} 2$ has the form $V_1 \xrightarrow{f} V_2$ with k-vector spaces V_1, V_2 and a k-linear map $f : V_1 \to V_2$. The corresponding $k\mathbb{A}_2$-module is given by the vector space $M = V_1 \oplus V_2$ and the multiplication

$$e_1 \cdot (v_1, v_2) = (v_1, 0)$$

$$e_2 \cdot (v_1, v_2) = (0, v_2)$$

$$\alpha \cdot (v_1, v_2) = (0, f(v_1)).$$

Every finite dimensional representation corresponds to a matrix $A \in k^{n_2 \times n_1}$ where $n_i = \dim_k(V_i)$, and homomorphisms between two such representations, in terms of matrices A and A', are given by two matrices P, Q such that $PA = A'Q$. The representations are thus isomorphic if and only if there are matrices $P \in GL_{n_2}(K)$ and $Q \in GL_{n_1}(K)$ such that $A' = PAQ^{-1}$.

(2) A representation of the quiver $\bullet \overset{\alpha}{\underset{\beta}{\rightrightarrows}} \bullet$ has the form $V_1 \overset{f_\alpha}{\underset{f_\beta}{\rightrightarrows}} V_2$ where V_1, V_2 are k-vectorspaces and $f_\alpha, f_\beta : V_1 \to V_2$ are k-linear. In other words, every finite dimensional representation of $\bullet \overset{\alpha}{\underset{\beta}{\rightrightarrows}} \bullet$ corresponds to a pair of matrices (A, B) with $A, B \in k^{n_2 \times n_1}$ and $n_1, n_2 \in \mathbb{N}_0$. Moreover, isomorphism of two representations, in terms of matrix pairs (A, B) and (A', B') corresponds to the existence of two invertible matrices $P \in GL_n(K)$ and $Q \in GL_m(K)$ such that $A' = PAQ^{-1}$ and $B' = PBQ^{-1}$. So, the classification of the finite dimensional representations of $\bullet \rightrightarrows \bullet$ translates into the classification problem of "matrix pencils" considered by Kronecker in [**?**].

(3) A representation of Q : $\bullet \circlearrowleft \alpha$ is given as (V, f) with a vectorspace V and a linear map f. It corresponds to a module over the ring $k[x]$. Indeed, if M is a $k[x]$-module, then we obtain a representation of Q by setting $V = M$ and $f : M \to M$, $m \mapsto xm$.

3 PROJECTIVE MODULES, INJECTIVE MODULES

3.1 Exact sequences

Definition: A sequence of homomorphisms of R-modules

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

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 $0 \to L \stackrel{i}{\to} M \stackrel{p}{\to} M/L \to 0$, where i and p are the canonical inclusion and quotient homomorphisms, is short exact (Check!). Conversely, if $0 \to M_1 \stackrel{f}{\to} M_2 \stackrel{g}{\to} M_3 \to 0$ is a short exact sequence, then f is a monomorphism, g is an epimorphism, and $M_3 \cong \operatorname{Coker} f$ (check!).

Example 3.1.1. (1) Consider the representations $0 \stackrel{0}{\to} K$, $K \stackrel{1}{\to} K$, and $K \stackrel{0}{\to} 0$ of $\mathbb{A}_2$ together with the morphisms

$$\begin{array}{ccc} 0 & \xrightarrow{0} & K \\ {\scriptstyle 0}\downarrow & & \downarrow{\scriptstyle 1} \\ K & \xrightarrow[1]{} & K \end{array}$$

and

$$\begin{array}{ccc} K & \xrightarrow{1} & K \\ {\scriptstyle 1}\downarrow & & \downarrow{\scriptstyle 0} \\ K & \xrightarrow[0]{} & 0 \end{array}$$

They correspond to modules M_1, M_2, M_3 over $k\mathbb{A}_2$ and to homomorphisms $f : M_1 \to M_2$ and $g : M_2 \to M_3$ giving rise to a short exact sequence $0 \to M_1 \stackrel{f}{\to} M_2 \stackrel{g}{\to} M_3 \to 0$.
(2) For any $n \geq 2$ consider the short exact sequence $0 \to \mathbb{Z} \stackrel{n\cdot}{\to} \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \to 0$.

The following result is very useful:

Proposition 3.1.2. *Consider the commutative diagram with exact rows*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & L & \xrightarrow{f} & M & \xrightarrow{g} & N & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & L' & \xrightarrow{f'} & M' & \xrightarrow{g'} & N' & \longrightarrow & 0 \end{array}$$

If α and γ are monomorphisms (epimorphims, or isomorphisms, respectively), 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 monomorphism, we conclude $l = 0$ and so $m = 0$.

(2) Suppose α and γ are epimorphisms and let $m' \in M'$. Then $g'(m') = \gamma(g(m)) = g'(\beta(m))$; 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 $m' = \beta(m - f(l))$. □

3.2 Split exact sequences

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

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

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

$$\begin{array}{ccccccccc} 0 & \longrightarrow & L & \xrightarrow{f} & M & \xrightarrow{g} & N & \longrightarrow & 0 \\ & & \| & & \cong\downarrow\alpha & & \| & & \\ 0 & \longrightarrow & L & \xrightarrow{i_L} & L \oplus N & \xrightarrow{\pi_N} & N & \longrightarrow & 0 \end{array}$$

commutes. Then f is a *split monomorphism* and g a *split epimorphism.*

Proposition 3.2.1. *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 homomorphism* $\varphi : M \to L$ *such that* $\varphi f = \mathrm{id}_L$
3. *there exists a homomorphism* $\psi : N \to M$ *such that* $g\psi = \mathrm{id}_N$

Under these conditions, L and N are isomorphic to direct summands of M.

Proof. 1 ⇒ 2. Since the sequence splits, then there exists α as in Definition 3.2. Let $\varphi = \pi_L \circ \alpha$. So for any $l \in L$ we have $\varphi f(l) = \pi_L \alpha f(l) = \pi_L(l, 0) = l$.
1 ⇒ 3 Similar (Check!)
2 ⇒ 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

$$\begin{array}{ccccccccc} 0 & \longrightarrow & L & \xrightarrow{f} & M & \xrightarrow{g} & N & \longrightarrow & 0 \\ & & \| & & \downarrow\alpha & & \| & & \\ 0 & \longrightarrow & L & \xrightarrow{i_L} & L \oplus N & \xrightarrow{\pi_N} & N & \longrightarrow & 0 \end{array}$$

commutes. Finally, by Proposition 3.1.2, we conclude that α is an isomorphism.
2 ⇒ 3 Similar (check!) □

Example. The short exact sequence in Example 3.1.1 is not a split exact sequence.

3.3 Free modules and finitely generated modules

Definition: A module ${}_RM$ is said to be *generated* by a family $\{x_i\}_{i\in I}$ of elements of M if every $x \in M$ 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 $i \in I$. Then $\{x_i\}_{i\in I}$ is called a set of *generators* of M and we write $M =< x_i, i \in I >$.
If the coefficients r_i are uniquely determined by x, the set $\{x_i\}_{i\in I}$ is called a *basis* of M. The module M is said to be *free* if it admits a basis.

Proposition 3.3.1. *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 components zero 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 epimorphism 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 monomorphism. □

Given a free module M with basis $(x_i)_I$, 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, once we choose the $f(x_i)$, we define f on $x = \sum r_i x_i \in M$ as $f(x) = \sum r_i f(x_i)$ (which is well defined since $(x_i)_{i\in I}$ is a basis - notice the analogy with vector spaces!).

Proposition 3.3.2. *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 epimorphism and so $M \cong R^{(I)}/\operatorname{Ker}\alpha$ □

Definition: 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 3.3.2, a module ${}_RM$ 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 3.3.3. Let R be a ring.

1. The regular module ${}_RR$ is cyclic, generated by the unity element: ${}_RR =< 1 >$.
2. Let Λ be a finite dimensional k-algebra. Then a module ${}_\Lambda M$ is finitely generated if and only if $\dim_k(M) < \infty$.

   Indeed, assume $\dim_k(\Lambda) = n$, and let $\{a_1, \ldots, a_n\}$ be a k-basis of Λ.

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

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

Proposition 3.3.4. *Let ${}_R L \le {}_R M$.*

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 generators for M, then $\{\overline{x}_1, \dots, \overline{x}_n\}$ is a set of generators 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. □

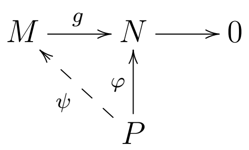
Notice that M finitely generated doesn't imply that L is finitely generated. For example, let R be the ring $R = k[x_i, i \in \mathbb{N}]$, and consider the regular module ${}_R R$ with its submodule $L =< x_i, i \in \mathbb{N} >$.

3.4 Projective modules

Definition: A module ${}_R P$ is *projective* if for any epimorphism $M \xrightarrow{g} N \to 0$ of left R-modules, the homomorphism of abelian groups

$$\mathrm{Hom}_R(P, g) : \mathrm{Hom}_R(P, M) \to \mathrm{Hom}_R(P, N),\ \psi \mapsto g\psi$$

is surjective, that is, for any $\varphi \in \mathrm{Hom}_R(P, N)$ there exists $\psi \in \mathrm{Hom}_R(P, M)$ such that $g\psi = \phi$.



Examples: Any free module is projective. Indeed, let $R^{(I)}$ a free R-module with $(x_i)_{i \in I}$ a basis. Given homomorphisms $M \xrightarrow{g} N \to 0$ and $\varphi : R^{(I)} \to N$, 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 $g\psi = \varphi$. It is clear from the construction that the homomorphism ψ is not unique in general.

Proposition 3.4.1. *Let P be a left R-module. 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 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 3.2.1 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 ${}_RN$. So let us consider the homorphisms

$$\begin{array}{ccccc} M & \xrightarrow{g} & N & \longrightarrow & 0 \\ & & \uparrow{\scriptstyle \varphi} & & \\ & & P & & \end{array} \quad \text{and} \quad \begin{array}{ccccc} M & \xrightarrow{g} & N & \longrightarrow & 0 \\ & {\scriptstyle \alpha}\nwarrow & \uparrow{\scriptstyle (\varphi,0)} & & \\ & & R^{(I)} & & \end{array}$$

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. □

Examples:

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 groups 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. The elements $e = \overline{3}$ and $f = \overline{4}$ are orthogonal idempotents (see Definition below) corresponding to this decomposition.

Definition. An element $e \in R$ is said to be *idempotent* if $e^2 = e$. Two idempotents $e, f \in R$ are said to be *orthogonal* if $ef = fe = 0$.

Remark 3.4.2. (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. Conversely, if $R = I \oplus J$, with I and J left ideals of R, then there exist orthogonal idempotents e and f such that $1 = e + f$, $I = Re$ and $J = Rf$.

(2) More generally, if $e_1, \ldots, e_n \in R$ are pairwise orthogonal idempotent elements such that $1 = e_1 + \ldots e_n$, then

$$R = Re_1 \oplus \ldots \oplus Re_n,$$

and every direct sum decomposition of the regular module ${}_RR$ arises in this way.

(3) If k is a field and $\Lambda = kQ$ is the path algebra of a quiver Q with $|Q_0| = n$, the lazy paths $e_1, \ldots, e_n$ are orthogonal idempotent elements of Λ as above. For each vertex

$i \in Q_0$, the paths starting in i form a k-basis of Λe_i. The representation corresponding to the module Λe_i is given by the vector spaces $V_j = e_j \Lambda e_i$ having as basis all paths starting in i and ending in j, and by the linear maps f_α corresponding to concatenation of paths with the arrow α. Moreover, $\operatorname{End}_\Lambda \Lambda e_i \cong e_i \Lambda e_i$ via $f \mapsto f(e_i)$ and if Q is acyclic, the latter is isomorphic to $ke_i \cong k$.

Example. (1) For $\Lambda = k\mathbb{A}_3$ the module Λe_1 corresponds to the representation

$$Ke_1 \overset{\alpha}{\to} K\alpha \overset{\beta}{\to} K\beta\alpha$$

which we write, up to isomorphism, as $K \to K \to K$.
(2) If $\Lambda = kQ$ is the Kronecker algebra with $Q : \bullet \underset{\beta}{\overset{\alpha}{\rightrightarrows}} \bullet$, then the representations corresponding to Λe_i are

$$\Lambda e_1 : K \underset{\beta}{\overset{\alpha}{\rightrightarrows}} K^2$$

$$\Lambda e_2 : 0 \rightrightarrows K.$$

Proposition 3.4.3. (Dual Basis Lemma) *A module $_RP$ is projective if and only if it has a* dual basis*, that is, a pair $(\,(x_i)_{i\in I},\, (\varphi_i)_{i\in I}\,)$ consisting of elements $(x_i)_{i\in I}$ in P and homomorphisms $(\varphi_i)_{i\in I}$ in $P^* = \operatorname{Hom}_R(P, R)$ such that every element $x \in P$ can be written as*

$$x = \sum_{i\in I} \varphi_i(x)\, x_i$$

with $\varphi_i(x) = 0$ for almost all $i \in I$.

Proof. Let P be projective and let $R^{(I)} \overset{\beta}{\to} P \to 0$ be a split epimorphism. Let $(e_i)_{i\in I}$ be the canonical basis of $R^{(I)}$ and denote $x_i = \beta(e_i)$. Observe that $\beta(\sum_i r_i e_i) = \sum_i r_i \beta(e_i) = \sum_i r_i x_i$. By Proposition 3.2.1, there exists $\varphi : P \to R^{(I)}$ such that $\beta\varphi = id_P$, which induces homomorphisms $\varphi_i = \pi_i \varphi \in P^*$ where π_i is the projection on the i-th component. Then $\varphi_i(x) \in R$ is zero for almost all $i \in I$, and $\varphi(x) = \sum \varphi_i(x) e_i$. Hence for any $x \in P$ one has $x = \beta\varphi(x) = \beta(\sum_i \varphi_i(x) e_i) = \sum_i \varphi_i(x) x_i$, so $((\varphi_i)_{i\in I}, (x_i)_{i\in I})$ satisfies the stated properties.
Conversely, let $((\varphi_i)_{i\in I}, (x_i)_{i\in I})$ satisfy the statement. Define $\beta : R^{(I)} \to P$ by $e_i \mapsto x_i$. The homomorphism β is an epimorphism since the family $(x_i)_{i\in I}$ generates P, and $\beta(\sum r_i e_i) = \sum r_i x_i$. Set $\varphi : P \to R^{(I)}$, $x \mapsto \sum \varphi_i(x) e_i$. Then for any $x \in P$ one gets $\beta\varphi(x) = \beta(\sum \varphi_i(x) e_i) = \sum \varphi_i(x) x_i = x$. By Proposition 3.2.1 we conclude that β is a split epimorphism and so P is projective. □

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

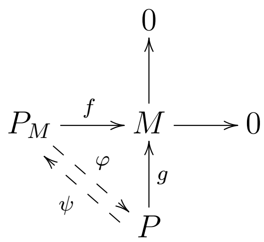
In particular, for any module ${}_RM$ there exists a short exact sequence $0 \to K \to P_0 \to M \to 0$, with P_0 projective. The same holds for the module K, and so, iterating the argument, we can construct an exact sequence

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

where all the P_i are projective. Such a sequence is called a *projective resolution* of P. It is clearly not unique.
It is natural to ask if, for a given module ${}_RM$, there exists a projective module P and a "minimal" epimorphism $P \to M \to 0$, in the sense that there is no proper direct summand P' of P with an epimorphism $f_{|P'} : P' \to M$. More precisely, we define:

Definition: (1) A homomorphism $f : M \to N$ is *right minimal* if any $g \in \mathrm{End}_R(M)$ such that $fg = f$ is an isomomorphism.
(2) A *projective cover* of M is a right minimal epimorphism $P_M \to M$ where P_M is a projective module.

Remark 3.4.4. Projective covers are "minimal" in the sense announced above. Indeed, consider another epimorphism $P \to M$ where P is a projective module. Since both 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, $\psi\varphi$ is an isomorphism. Then $\theta : P \to P_M$ as $\theta = (\psi\varphi)^{-1}\psi$ satisfies $\theta\varphi = id_P$, so φ is a split monomorphism and P_M is isomorphic to a direct summand of P (see Proposition 3.2.1). More precisely, $P = \mathrm{Im}\,\varphi \oplus \mathrm{Ker}\,\theta$ with $\mathrm{Im}\,\varphi \cong P_M$ and $g(\mathrm{Ker}\,\theta) = 0$.

In particular, if $g : P \to M$ is also a projective cover of M, then we can see as above that also $\varphi\psi$ is an isomorphism, so $\varphi = \psi^{-1}$ and P_M is isomorphic to P. We have shown that the projective cover is unique (up to isomorphism).

Observe that, given a module ${}_RM$, a projective cover for M need not exist. A ring over which any finitely generated module admits a projective cover is called *semiperfect*. If all modules admit a projective cover, then R is called *perfect*.

Definition. Suppose there exists a projective resolution of the module ${}_RM$

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

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

Examples. (1) The canonical epimorphism $\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ is not right minimal, and the $\mathbb{Z}$-module $\mathbb{Z}/2\mathbb{Z}$ has no projective cover.
(2) The exact sequence in Example 3.1.1 is a minimal projective resolution of M_3. Indeed, by Example 3.4.2(4) we can rewrite the sequence as

$$0 \to \Lambda e_2 \xrightarrow{f} \Lambda e_1 \xrightarrow{g} M_3 \to 0$$

where the first two terms are projective modules with endomorphism ring k. It follows that g is right minimal, thus a projective cover.

3.5 Injective modules

We now turn to the dual notion of an injective module. Observe that many results will be dual to those proved for projective modules.

Definition: A module ${}_RE$ is *injective* if for any monomorphism $0 \to L \xrightarrow{f} M$ of left R-modules, the homomorphism of abelian groups $\operatorname{Hom}_R(f, E) : \operatorname{Hom}_R(M, E) \to \operatorname{Hom}_R(L, E)$ is an epimorphism, that is for any $\varphi \in \operatorname{Hom}_R(L, E)$ there exists $\psi \in \operatorname{Hom}_R(M, E)$ such that $\psi f = \varphi$.

$$\begin{array}{ccccc} 0 & \longrightarrow & L & \xrightarrow{f} & M \\ & & \downarrow{\scriptstyle\varphi} & \swarrow{\scriptstyle\psi} & \\ & & E & & \end{array}$$

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

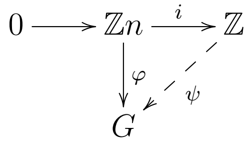
An abelian group G is *divisible* if, for any $n \in \mathbb{Z}$ and for any $g \in G$, there exists $t \in G$ such that $g = nt$. We are going to show that an abelian group is injective if and only if it is divisible. We need the following useful criterion to check whether a module is injective.

Lemma 3.5.1. (Baer's Criterion) *A module E is injective if and only if for any left ideal I of R and for any $\varphi \in \operatorname{Hom}_R(I, E)$ there exists $\psi \in \operatorname{Hom}_R(R, E)$ such that $\psi i = \varphi$, where i is the canonical inclusion $0 \to I \xrightarrow{i} R$.*

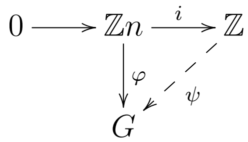
The lemma states that it suffices to check the extending property only for the left ideals of the ring. In particular, it says that E is injective if and only if for any ${}_RI \leq {}_RR$ and for any $h \in \operatorname{Hom}_R(I, E)$ there exists $y \in E$ such that $h(a) = ay$ for any $a \in I$.

Proposition 3.5.2. *An $\mathbb{Z}$-module G 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



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 Criterion. The ideals 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



commutes. Let $g \in G$ such that $\varphi(n) = g$. Since $\mathbb{Z}$ is a free $\mathbb{Z}$-module, we can define ψ by setting $\psi(1) = t$ where $g = nt$, 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.

Examples: (1) The $\mathbb{Z}$-module $\mathbb{Q}$ is injective.
(2) Let $p \in \mathbb{N}$ be a prime number and $M = \{\frac{a}{p^n} \in \mathbb{Q} \mid a \in \mathbb{Z}, n \in \mathbb{N}\}$. Then $\mathbb{Z} \leq M \leq \mathbb{Q}$, and $\mathbb{Z}_{p^\infty} = M/\mathbb{Z}$ is a divisible group, see Exercise **??**.
One can show that $\mathbb{Q}$ and $\mathbb{Z}_{p^\infty}$, p prime, are representatives of the indecomposable injective $\mathbb{Z}$-modules, up to isomorphism.

Remark 3.5.3. Any abelian group G embeds in an injective abelian group. Indeed, consider a short exact sequence $0 \to K \to \mathbb{Z}^{(I)} \to G \to 0$ and the canonical inclusion $0 \to \mathbb{Z} \to \mathbb{Q}$. One easily check that $\mathbb{Q}^{(I)}/K$ is divisible (check!) and so injective. Then we get the induced monomorphism $0 \to G \cong \mathbb{Z}^{(I)}/K \to \mathbb{Q}^{(I)}/K$.

Proposition 3.5.4. *Let R be a ring. If D is an injective $\mathbb{Z}$-module, 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 Criterion: let ${}_RI \leq {}_RR$ and $h : I \to \mathrm{Hom}_{\mathbb{Z}}(R, D)$ be an R-homomorphism. We have to find an element $y \in \mathrm{Hom}_{\mathbb{Z}}(R, D)$ such that $h(a) = ay$ for any $a \in I$. Notice that h defines a $\mathbb{Z}$-homomorphism $\gamma : I \to D$, $a \mapsto h(a)(1)$ 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 the element $\overline{\gamma} \in \mathrm{Hom}_{\mathbb{Z}}(R, D)$ satisfies $h(a) = a\overline{\gamma}$ for any $a \in I$, proving the claim. □

Corollary 3.5.5. *Every module $_RM$ embeds in an injective R-module.*

Proof. As an abelian group, M embeds in an injective abelian group D by Remark 3.5.3. In other words, there is a monomorphism of $\mathbb{Z}$-modules $0 \to M \xrightarrow{g} D$, from which we obtain a monomorphism of R-modules $0 \to \mathrm{Hom}_{\mathbb{Z}}(R_R, M) \to \mathrm{Hom}_{\mathbb{Z}}(R_R, D)$ given by $f \mapsto gf$. Now $E := \mathrm{Hom}_{\mathbb{Z}}(R_R, D)$ is an injective left R-module by Proposition 3.5.4. Moreover, there is an isomorphism of R-modules $\varphi : \mathrm{Hom}_R(R, M) \to M$, $f \mapsto f(1)$ (see Exercise **??**) yielding

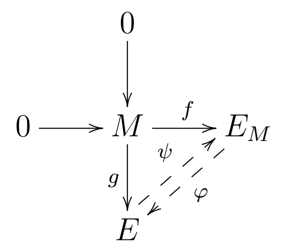
$$_RM \cong \mathrm{Hom}_R(R_R, M) \leq \mathrm{Hom}_{\mathbb{Z}}(R_R, M) \to E = \mathrm{Hom}_{\mathbb{Z}}(R_R, D)$$

which is the desired monomorphism. □

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

Definition: (1) A homomorphism $f : M \to N$ is *left minimal* if any $g \in \mathrm{End}_R(N)$ such that $gf = f$ is an isomomorphism.
(2) An *injective envelope* of M is a left minimal monomorphism $M \to E_M$ where E_M is an injective module.

Remark 3.5.6. Consider a diagram

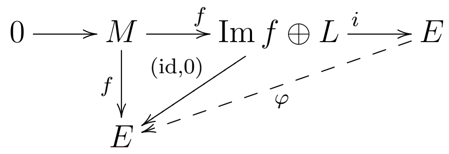


where $g : M \to E$ is another monomorphism where E is an injective module. Since E_M and E are both injective, there exist φ and ψ such that the diagram commutes. Hence $\psi g = f$ and $\varphi f = g$, so $\psi\varphi f = f$ and, since f is left minimal, we conclude that $\psi\varphi$ is an isomorphism. Then φ is a split monomorphism, and E_M is isomorphic to a direct summand of E.
In particular, if also g is an injective envelope of M, also $\varphi\psi$ is an isomorphism, so φ is an isomorphism and E_M is isomorphic to E. We have shown that the injective envelope is unique (up to isomorphisms).

We state a characterization of injective envelopes, for which we need the following notions.
Definition. (1) A submodule $_RN \leq {}_RM$ is *essential* if for any submodule $L \leq M$, $L \cap N = 0$ implies $L = 0$.
(2) A monomorphism $0 \to L \xrightarrow{f} M$ is *essential* if $\mathrm{Im}\, f$ is essential in M. Equivalently: every $g \in \mathrm{Hom}_R(M, N)$ with the property that gf is a monomorphism is itself a monomorphism (see Exercise **??**).

Theorem 3.5.7. *Let E be an injective module. Then $0 \to M \xrightarrow{f} E$ is an injective envelope of M if and only if f is an essential monomorphism.*

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

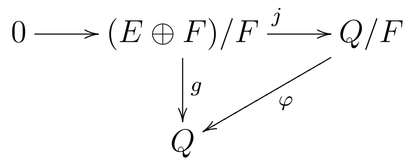


where i is the canonical inclusion of $\operatorname{Im} f \oplus L$ in E and φ exists since E is injective. Then $\varphi f = f$, and φ is an isomorphism, so $L = 0$.
Conversely, let $\operatorname{Im} f$ be essential in M and let $g \in \operatorname{End}_R(E)$ such that $gf = f$. Since f is an essential monomorphism, g is a monomorphism, hence a split monomorphism (see 3.5.9). Further, the direct summand $\operatorname{Im} g \overset{\oplus}{\leq} E$ of E contains the essential submodule $\operatorname{Im} f$, so it must have a trivial complement, that is, $\operatorname{Im} g = E$ and g is an isomorphism. □

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

Theorem 3.5.8. *Every module has an injective envelope.*

Proof. Let $_RM$ be a module; by Corollary 3.5.5 there exists an injective module Q such that $0 \to M \to Q$. Consider the set $\{E' \mid M \leq E' \leq Q \text{ and } M \text{ essential in } E'\}$. One easily checks that it is an inductive set, and by Zorn's Lemma, it contains a maximal element E. Let us show that E is injective by verifying that it is a direct summand of Q (see Exercise **??**). To this end, consider the set $\{F' \mid F' \leq Q \text{ and } F' \cap E = 0\}$. It is inductive so, again by Zorn's Lemma, it contains a maximal element F. We claim that $E \oplus F = Q$. Notice that there exists an obvious monomorphism $g : (E \oplus F)/F \cong E \leq Q$; further $(E \oplus F)/F \leq Q/F$ is an essential inclusion by the maximality of F (check!). We obtain the diagram



where j is the canonical inclusion, φ exists since Q is injective, and moreover, φ is a monomorphism since $\varphi j = g$ is a monomorphism and j is an essential monomorphism. Then also $E = \operatorname{Im} g = \varphi(E \oplus F/F)$ is essential in $\operatorname{Im} \varphi$. Since M is essential in E, we conclude that M is essential in $\operatorname{Im} \varphi$, and by the maximality of E, it follows $E = \operatorname{Im} \varphi$. Hence $\varphi(E \oplus F/F) = \varphi(Q/F)$. Since φ is a monomorphism we conclude $E \oplus F = Q$. □

Proposition 3.5.9. *Let $_RE$ be a module. 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

$$\begin{array}{ccccc} 0 & \longrightarrow & E & \xrightarrow{f} & M \\ & & {\scriptstyle \mathrm{id}_E}\downarrow & \swarrow {\scriptstyle \varphi} & \\ & & E & & \end{array}$$

where φ exists since E is injective. Since $\varphi f = \mathrm{id}_E$, by Proposition 3.2.1 we conclude that f is a split monomorphism.
$2 \Rightarrow 1$ By Corollary 3.5.5 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 **??**). □

Comparing the previous proposition with the analogous one for projective modules (Proposition 3.4.1), there is an evident difference. For projective modules, we saw that a special role is played by the projective generator ${}_RR$. Does a module with the dual property exist? We will see in **??** that such a module always exists.

Dually to the projective case, for any module ${}_RM$ 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.

4 ON THE LATTICE OF SUBMODULES OF M

Let R be a ring.

4.1 Simple modules

For a left R-module M, we consider the partially ordered set $\mathcal{L}_M = \{L \mid L \leq M\}$. Observe that $\mathcal{L}_M$ is a complete lattice, where for any $N, L \in \mathcal{L}$, the join is given by $\sup\{N, L\} = L + N$ and the meet by $\inf\{N, L\} = L \cap N$. The greatest element of $\mathcal{L}_M$ is M and the smallest if $\{0\}$.
Moreover, $\mathcal{L}_M$ satisfies the *Modular Law*: Given ${}_RA, {}_RB, {}_RC \leq {}_RM$ with $B \leq C$,

$$(A + B) \cap C = (A \cap C) + B.$$

It is natural to ask whether $\mathcal{L}$ has minimal or maximal elements. They are exactly the maximal submodules of M and the simple submodules of M, respectively. More precisely:

Definition: A module S is *simple* if $L \leq S$ implies $L = \{0\}$ or $L = S$.
Given a module ${}_RM$, a proper submodule ${}_RN < {}_RM$ is a *maximal submodule* of M if $N \leq L \leq M$ implies $L = N$ or $L = M$.

Examples:

1. Let k be a field. Then k is the unique simple k-module up to isomorphism.
2. Any abelian group $\mathbb{Z}/\mathbb{Z}p$ with p prime is a simple $\mathbb{Z}$-module. So there are infinitely many simple $\mathbb{Z}$-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.
4. The $\mathbb{Z}$-module $\mathbb{Q}$ has no maximal submodules, see Exercise **??**.
5. Let p be a prime number. The lattice of the subgroups of $\mathbb{Z}_{p^\infty}$ is a well-ordered chain, and $\mathbb{Z}_{p^\infty}$ has no maximal submodules, see Exercise **??**.

We have just seen that in general, it is not true that any module contains a simple or a maximal submodule. Nevertheless, we have the following important result.

Proposition 4.1.1. *Let R be a ring and ${}_RI < {}_RR$ a proper left ideal. There exists a maximal left ideal $\mathfrak{m}$ of R such that $I \leq \mathfrak{m} < R$. In particular R admits maximal left ideals.*
More generally, if M is a finitely generated left R-module, then every proper submodule of M is contained in a maximal submodule.

Proof. Let $\mathcal{F} = \{L \mid I \leq L < R\}$. 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.
For the second statement, see Exercise **??**. □

Examples: 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 4.1.2. Let $\mathfrak{m} \leq R$ be a maximal left ideal of R. Clearly $R/\mathfrak{m}$ is a simple R-module, and this shows that simple modules always exist over any ring R.
Conversely, if S is a simple module, any nonzero element $x \in S$ satisfies $S = Rx$, and $\mathrm{Ann}_R(x) = \{r \in R \mid rx = 0\}$ is the kernel of the epimorphism $\varphi : R \to S$, $1 \mapsto x$. Hence $\mathrm{Ann}_R(x)$ is a maximal left ideal of R and $S \cong R/\mathrm{Ann}_R(x)$.

Proposition 4.1.3. *The following statements are equivalent for a module ${}_RM$:*

1. *There is a family of simple submodules $(S_i)_{i\in I}$ of M such that $M = \sum_{i\in I} S_i$.*
2. *M is a direct sum of simple submodules.*
3. *Every submodule ${}_RL \leq {}_RM$ is a direct summand.*

Under these conditions, M is said to be *semisimple*.

Proof. Let us sketch the proof. In order to see that (1) implies (2) and (3), one uses Zorn's Lemma to show that for any ${}_RL \leq_R M$ there is a subset $J \subseteq I$ such that $M = L \oplus \bigoplus_{i\in J} S_i$.
(3)⇒(1): Using the Modular Law, we see that every submodule ${}_RN \leq {}_RM$ satisfies condition (3), that is, every submodule ${}_RL \leq {}_RN$ is a direct summand of N. Furthermore, if we consider a non-zero element $x \in M$ and choose $N = Rx$, then N contains a maximal submodule N' by Proposition 4.1.1, which then must be a direct summand of N. Since the complement of N' in N is simple, we conclude that Rx contains a simple submodule. Now consider the submodule $L = \sum_{i\in I} S_i$ defined as the sum of all simple submodules of M. We know that $M = L \oplus L'$ for some submodule L'. But by the discussion above L' cannot contain any nonzero element, hence $L' = 0$ and the claim is proven. □

4.2 Socle and radical

Definition: Let M be a left R-module. The *socle* of M is the submodule

$$\mathrm{Soc}(M) = \sum \{S \mid S \text{ is a simple submodule of } M\}.$$

The *radical* of M is the submodule

$$\mathrm{Rad}(M) = \bigcap \{N \mid N \text{ is a maximal submodule of } M\}.$$

In particular, if M does not contain any simple module, $\mathrm{Soc}(M) = 0$, and if M does not contain any maximal submodule, $\mathrm{Rad}(M) = M$.

Remark 4.2.1. (1) $\mathrm{Soc}(M)$ is the largest semisimple submodule of M.
This follows immediately from Proposition 4.1.3.
(2) $\mathrm{Rad}(M) = \{x \in M \mid \varphi(x) = 0 \text{ for every } \varphi : M \to S \text{ with } S \text{ simple}\}$.
Indeed, notice that the kernel of any homomorphism $\varphi : M \to S$ with S simple is a maximal submodule of M. Conversely, if N is a maximal submodule of M, then consider $\pi : M \to M/N$, keeping in mind that M/N is simple.

In order to study $\mathrm{Rad}\, M$, we need the following notion, which also leads to a characterization of projective covers dual to Theorem 3.5.7.
Definition. A submodule ${}_RN \leq {}_RM$ is *superfluous* if for any submodule $L \leq M$, $L + N = M$ implies $L = M$.

Theorem 4.2.2. *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.*

It follows from Proposition 4.1.1 that $\mathrm{Rad}(M)$ is a superfluous submodule of M whenever M is finitely generated. We collect some further properties of the socle and of the radical of a module in the proposition below.

Proposition 4.2.3. *Let M be a left R-module.*

1. $\mathrm{Soc}(M) = \bigcap\{L \mid L$ *is an essential submodule of* $M\}$.
2. $\mathrm{Rad}(M) = \sum\{U \mid U$ *is a superfluous submodule of* $M\}$.
3. $f(\mathrm{Soc}(M)) \leq \mathrm{Soc}(N)$ *and* $f(\mathrm{Rad}(M)) \leq \mathrm{Rad}(N)$ *for any* $f \in \mathrm{Hom}_R(M, N)$.
4. *If* $M = \oplus_{\lambda\in\Lambda} M_\lambda$, *then* $\mathrm{Soc}(M) = \bigoplus_{\lambda\in\Lambda} \mathrm{Soc}(M_\lambda)$ *and* $\mathrm{Rad}(M) = \bigoplus_{\lambda\in\Lambda} \mathrm{Rad}(M_\lambda)$.
5. $\mathrm{Rad}(M/\mathrm{Rad}(M)) = 0$ *and* $\mathrm{Soc}(\mathrm{Soc}(M)) = \mathrm{Soc}(M)$.

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

Proposition 4.2.4. *(1)* $\mathrm{Rad}({}_RR) = \bigcap\{\mathrm{Ann}_R(S) \mid S$ *is a simple left R-module* $\}$.
(2) $\mathrm{Rad}({}_RR) = \{r \in R \mid 1 - xr$ *has a (left) inverse for any* $x \in R\}$.
(3) $\mathrm{Rad}({}_RR) = \mathrm{Rad}(R_R)$ *is a two-sided ideal.*

Proof. (1) For any simple module S, consider $\mathrm{Ann}_R(S) = \bigcap_{x\in S} \mathrm{Ann}_R(x)$ of R, which is a two-sided ideal by Exercise **??**. The intersection of all annihilators $\mathrm{Ann}_R(S)$ of simple left R-modules coincides with $\mathrm{Rad}({}_RR)$ by Remarks 4.1.2 and 4.2.1.
(2) is Exercise **??**. In fact, one can even show that the elements $1 - xr$ are invertible: taking $r \in \mathrm{Rad}({}_RR)$ and $x \in R$, we have $s = xr \in \mathrm{Rad}({}_RR)$, and if a is a left inverse of $1 - s$, that is, $a(1 - s) = 1$, then $a = 1 + as = 1 - (-a)s$ has again a left inverse, which must coincide with its right inverse $1 - s$, showing that a and $1 - s$ are mutually inverse.
(3) It follows from (1) that $\mathrm{Rad}({}_RR)$ is a two-sided ideal of R. So, if $r \in \mathrm{Rad}({}_RR)$, and $x \in R$, then $rx \in \mathrm{Rad}({}_RR)$, and the element $1 - rx$ has a (right) inverse by (2). From the right version of statement (2) we infer $r \in \mathrm{Rad}(R_R)$. So $\mathrm{Rad}({}_RR) \subseteq \mathrm{Rad}(R_R)$, and the other inclusion follows by symmetric arguments. □

Definition: Let R be a ring. The ideal

$$J(R) = \mathrm{Rad}({}_R R) = \mathrm{Rad}(R_R)$$

is called *Jacobson radical* of R.

Lemma 4.2.5. *(1) For every module ${}_R M$ we have $\mathrm{J}(R)M \leq \mathrm{Rad}(M)$.*
(2) **(Nakayama'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. (1) Since $\mathrm{J}(R)$ annihilates any simple module S, all homomorphisms $\varphi : M \to S$ vanish on $\mathrm{J}(R)M$, so $\mathrm{J}(R)M \leq \mathrm{Rad}(M)$ by Remark 4.2.1.
(2) $L + \mathrm{J}(R)M = M$ implies $L + \mathrm{Rad}(M) = M$ and since $\mathrm{Rad}(M)$ is superfluous in M by Remark 4.2.1, we get $L = M$. □

Example 4.2.6. (1) $J(\mathbb{Z}) = \bigcap_{p \text{ prime}} p\mathbb{Z} = 0$.
(2) Let $\Lambda = kQ$ be the path algebra of a finite acyclic quiver over a field k.

(i) The Jacobson radical $J(\Lambda)$ is the ideal of Λ generated by all arrows. Hence, as a k-vectorspace, $\Lambda = (\oplus_{i \in Q_0} ke_i) \oplus J(\Lambda)$. Moreover, $\Lambda/J(\Lambda) \cong k^{|Q_0|}$ as k-algebras.

(ii) Let $i \in Q_0$ be a vertex, and denote by $\alpha_1, \ldots, \alpha_t$ the arrows $i \bullet \xrightarrow{\alpha_k} \bullet\, j_k$ of Q which start in i. Then

$$\mathrm{Rad}\,\Lambda e_i = Je_i = \bigoplus_{k=1}^{t} \Lambda e_{j_k} \alpha_k \cong \bigoplus_{k=1}^{t} \Lambda e_{j_k}$$

is the unique maximal submodule of Λe_i, and it is a projective module.

(iii) Let $i \in Q_0$ be a vertex. Then $\Lambda e_i / Je_i$ is simple. In particular, the projective module Λe_i is simple if and only if i is a sink of Q, that is, there is no arrow starting in i.

Indeed, let $i \in Q_0$ be a vertex. Then the vector space generated by all paths of length at least one starting in i is the unique maximal submodule of Λe_i, so it coincides with $\mathrm{Rad}\,\Lambda e_i$. Now use that $\Lambda = \bigoplus_{i \in Q_0} \Lambda e_i$ by Remark 3.4.2, hence $J(\Lambda) = \bigoplus_{i \in Q_0} \mathrm{Rad}\,\Lambda e_i$ by Proposition 4.2.3.

4.3 Local rings

Definition:
(1) A ring R is a *skew field* (or a *division ring*) if all non-zero elements are invertible.
(2) A ring R is *local* if it satisfies the equivalent conditions in the proposition below.

Proposition 4.3.1. *The following statements are equivalent for a ring R with $J = J(R)$.*

(1) R/J is a skew field.

(2) x or $1 - x$ is invertible for any $x \in R$.

(3) R has a unique maximal left ideal.

(3') R has a unique maximal right ideal.

(4) The non-invertible elements of R form a left (or right, or two-sided) ideal of R.

Proof. (1)⇒(2): If $x \in J$, then $1 - x$ is invertible by Proposition 4.2.4. If $x \notin J$, then $\overline{x} \neq 0$ is invertible in R/J, so there is $\overline{y} \in R/J$ such that $\overline{xy} = \overline{yx} = \overline{1}$. Then $1 - xy$ and $1 - yx$ belong to J, hence xy and yx are invertible. But then x is invertible, because it has a right inverse and a left inverse.
(2)⇒(3): Any maximal left ideal $\mathfrak{m}$ contains J. Conversely, if $r \in \mathfrak{m}$ and $x \in R$, then $xr \in \mathfrak{m}$ can't be invertible, so $1 - xr$ is invertible, and $r \in J$ by Proposition 4.2.4. Hence $\mathfrak{m} = J$ is the unique maximal left ideal.
(3)⇒(1): Assume that R has a unique maximal left ideal $\mathfrak{m}$. Then $\mathfrak{m} = J$, and R/J is a simple left module. Then every non-zero element $\overline{x} \in R/J$ satisfies $Rx = R/J$, so there is $y \in R$ such that $\overline{1} = y\overline{x} = \overline{yx}$. In other words, every non-zero element in R/J has a left inverse, and therefore an inverse (because the left inverse of $\overline{y}$ must coincide with its right inverse $\overline{x}$).
(1)⇔(3') is shown symmetrically.
(3)⇒(4): J is the set of all non-invertible elements of R. Indeed, J is a maximal left ideal and therefore it consists of non-invertible elements. Conversely, if $x \in R$ has no left inverse, then Rx is a proper left ideal of R and thus it is contained in the unique maximal left ideal J. If x has no right inverse, use the equivalent condition (3').
(4)⇒(2): otherwise $1 = x + (1 - x)$ would be non-invertible. □

Remark 4.3.2. Let R be a local ring.
(1) We have seen above that J is the ideal from conditions (3), (3') and (4) above.
(2) $S = R/\operatorname{J}(R)$ is the unique simple left (or right) R-module up to isomorphism, and $E(R/\operatorname{J}(R))$ is a minimal injective cogenerator.
(3) The unique idempotent elements in R are 0 and 1. Indeed, if e is idempotent, then $e(1 - e) = 0$. So, either e is invertible, and then $e = 1$, or $1 - e$ is invertible, and then $e = 0$.
(4) ${}_RR$ is an indecomposable R-module by Remark 3.4.2.