Representations

Mariano Suárez-Álvarez

May 11, 2015

Table of Revisions

Name	Rev	Last Author	Last Changed At
Document	432	mariano	2015-04-30 21:16:17
File ‘`reduction.tex`’	431	mariano	2015-04-28 17:19:00
File ‘`semisimple.tex`’	416	mariano	2015-04-17 17:28:33
File ‘`groups.tex`’	419	mariano	2015-04-20 20:54:18
File ‘`radical.tex`’	420	mariano	2015-04-21 20:22:25
File ‘`projectives.tex`’	425	mariano	2015-04-24 08:54:14
File ‘`ar.tex`’	432	mariano	2015-04-30 21:16:17
File ‘`homological.tex`’	428	mariano	2015-04-24 23:36:34
File ‘`references.tex`’	406	mariano	2015-04-10 08:30:04

CHAPTER 1

Reduction theorems

§1.1. Local algebras

1.1.1. Proposition. *Let A be a non-zero algebra. The following statements are equivalent:*

(a) *A has a unique maximal left ideal.*
(b) *The set of non-units of A is a left ideal.*
(c) *If $a \in A$, then one of a or $1 - a$ is invertible.*
(d) *A has a unique maximal right ideal.*
(e) *The set of non-units of A is a right ideal.*
(f) *The set of non-units of A is a two-sided ideal.*

A non-zero algebra which satisfies the conditions of this proposition is said to be ***local***.

Proof. (a) $\Rightarrow$ (b) Suppose that I is the unique maximal left ideal of A. If $x \in A$, we have that

$$x \in I \text{ iff } x \text{ does not have a left inverse,} \tag{1}$$

because I is a proper left ideal. We claim that

if x has a left inverse then it is in fact invertible.

Indeed, if $y \in A$ is such that $yx = 1$, to prove that x is invertible we need only show that y itself has a left inverse. Suppose then that y does *not* have a left inverse, so that by (1) we have $y \in I$. This together with (1) and the fact that I is a proper ideal implies that

$$\text{for all } u \in A, \text{ the element } 1 - uy \text{ has a left inverse.} \tag{2}$$

In particular, there exists a $z \in A$ such that $z(1 - xy) = 1$. As $z = 1 - (-zx)y$, the same observation tells us that there exists a $w \in A$ such that $wz = 1$. As

$$1 = wz = w(1 - (-zx)y) = w + wzxy = w + xy,$$

we in fact have that $w = 1 - xy$ and, therefore, that $(1 - xy)z = wz = 1$. Since $yx = 1$, we have $y(1 - xy) = 0$, and multiplying this equality on the right by z we find that

$y = 0$, which is absurd. We can thus conclude that y does have a left inverse, as we wanted.

Now the combination of (1) and (2) imply at once that

$x \in I$ *iff* x *is not invertible*

Of course, this proves (b).

(b) $\Rightarrow$ (c) Suppose the set of non-units of A is a left ideal I. If $a \in A$ and neither of a nor $1 - a$ is invertible, so that they both belong to I, then we have $1 = a + (1 - a) \in I$, and this is impossible.

(c) $\Rightarrow$ (a) Suppose that I and J are two distinct maximal left ideals of A. As $I + J$ is equal to A, there are $x \in I$ and $y \in J$ such that $x + y = 1$. It follows then that neither of x or $1 - x = y$ is invertible, contradicting the hypothesis (c).

This establishes the equivalence of the first three statements listed in the proposition. As statement (c) is left-right symmetric, it follows immediately that these three statements are equivalent to the remaining two. □

1.1.2. Proposition. *An algebra is local if all its elements are either invertible or nilpotent*

Proof. Suppose A is an algebra satisfying that condition and let $x \in A$ be a non-unit, so that there exists a positive integer k such that $x^k = 0$. A direct computation shows then that $\sum_{i=0}^{k-1} x^i$ is an inverse for $1 - x$. It follows that the algebra is then local, according to Proposition 1.1.1. □

§1.2. Indecomposable modules

1.2.1. A module M is ***indecomposable*** if it is non-zero and there do not exist proper submodules P and Q such that $M = P \oplus Q$.

1.2.2. Indecomposability of a module can be very neatly expressed in terms of its endomorphism algebra, as we see in the next result. Recall that an element e of an algebra Λ is ***idempotent*** if $e^2 = e$; of course, the elements 0 and 1 are idempotent, and we call them the ***trivial*** idempotents.

Proposition. *A module is indecomposable iff its endomorphism algebra has no non-trivial idempotent elements.*

Proof. Let M be a module. If it is decomposable, there exist proper submodules $P, Q \subseteq M$ such that $M = P \oplus Q$ and there is an endomorphism $e : M \to M$ such that $e(p) = p$ for all $p \in P$ and $e(q) = 0$ for all $q \in Q$. It is easy to check that e is a non-trivial idempotent in the endomorphism algebra $\mathsf{End}(M)$.

Conversely, suppose that $e \in \mathsf{End}(M)$ is a non-trivial idempotent and let us consider the submodules $P = \ker e$ and $Q = \operatorname{im} e$ of M. If $m \in P \cap Q$, then there is an $n \in M$ such that $m = e(n)$, because $m \in P$, and since $m \in Q$ we have that $0 = e(m) = e^2(n) = e(n) = m$: it follows that $P \cap Q = 0$. On the other hand, if $m \in M$, then we have that the element $q = e(m)$ is in Q, that the element $p = m - e(m)$ is in P, since $e(p) = e(m) - e^2(m) = 0$, and that $m = p + q$. We thus see that $M = P \oplus Q$. As e is neither 0 nor 1, we have that both P and Q are proper submodules and we can conclude that M is decomposable. □

1.2.3. The following nice and useful result was proved by Hans Fitting in [Fit1935].

Proposition (Fitting's lemma). *If M is a module and $f : M \to M$ is an endomorphism, then there are submodules P and Q in M with $M = P \oplus Q$ and such that*

- *$f(P) \subseteq P$ and $f(Q) \subseteq Q$,*
- *$f|_P : P \to P$ is an automorphism, and*
- *$f|_Q : Q \to Q$ is nilpotent.*

Proof. Since M is finite-dimensional, the two chains

$$M \supseteq \operatorname{im} f \supseteq \operatorname{im} f^2 \supseteq \operatorname{im} f^3 \supseteq \cdots$$

and

$$0 \subseteq \ker f \subseteq \ker f^2 \subseteq \ker f^2 \subseteq \cdots$$

of submodules of M must eventually stabilize, and there exists a positive integer n such that $\operatorname{im} f^m = \operatorname{im} f^n$ and $\ker f^m = \ker f^n$ for all $m \geq n$.

We let $P = \operatorname{im} f^n$ and $Q = \ker f^n$. We have $f(P) = f(\operatorname{im} f^n) = \operatorname{im} f^{n+1} = \operatorname{im} f^n = P$ and, since $f^n(f(Q)) = f^{n+1}(\ker f^n) = 0$, we have $f(Q) \subseteq Q$. The definition of P makes it clear that the restriction $f|_Q : Q \to Q$ is nilpotent and the restriction $f|_Q : P \to P$ is an isomorphism because it is, as we have seen, surjective. We are left, therefore, with proving that $M = P \oplus Q$.

Suppose first that $x \in P \cap Q$. As $x \in P$, there exists a $y \in M$ with $x = f^n(y)$, and as $x \in Q$, we have that $0 = f^n(x) = f^{2n}(y)$. This tells us that $y \in \ker^{2n} = \ker f^n$ and thus $x = f^n(y) = 0$. It follows that $P \cap Q = 0$. On the other hand, we have a short exact sequence

$$0 \longrightarrow \ker f^n \hookrightarrow M \xrightarrow{f^n} \operatorname{im} f^n \longrightarrow 0$$

so that $\dim M = \dim P \oplus Q$. This completes the proof. □

1.2.4. Proposition. *An algebra A is local iff its only idempotent elements are* 0 *and* 1*.*

It should be emphasized that for this to be true we need the algebra A to be finite-dimensional.

Proof. Suppose first that A is local. If $e \in A$ is idempotent, then $e(1-e) = 0$. The third statement of Proposition 1.1.1 tells us that one of e or $1 - e$ is invertible, so we see that either $e = 0$ or $e = 1$.

Next, let us suppose that the only idempotents in A are the trivial ones, and let $x \in A$ be a non-unit. The map $f : y \in A \mapsto yx \in A$ is a morphism of modules to which we can apply Proposition 1.2.3: it tells us that there are left ideals P and Q in A with $A = P \oplus Q$, $Px \subseteq P$, $Qx \subseteq Q$, and such that the map $y \in Q \mapsto yx \in Q$ is bijective and there is a positive integer k such that $Qx^k = 0$.

In particular, there are $p \in P$ and $q \in Q$ such that $1 = p + q$. Since $p = p1 = p^2 + pq$ and P and Q are left ideals, we have that $pq \in P \cap Q = 0$ and therefore $p^2 = p$, that is, p is idempotent. The hypothesis implies then that one of p or q is equal to 1, so that either $P = A$ or $Q = A$.

If $Q = A$, then $x^k = 1x^k \in Ax^k = 0$ and x is nilpotent. Suppose now instead that $P = A$. The map f is then a bijection and there exists a $y \in A$ such that $yx = 1$. As $(xy)^2 = xyxy = xy$, the element xy is idempotent. It cannot be equal to 1, for then x would be invertible against our hypothesis, so it vanishes, and then $x = x1 = xyx = 0$.

We conclude that A satisfies the condition of Proposition 1.1.2, so that it is local. $\square$

1.2.5. Proposition. *A module M is indecomposable iff its endomorphism algebra $\mathsf{End}_A(M)$ is local.*

Proof. This follows at once from Proposition 1.2.2 and Proposition 1.2.4 $\square$

§1.3. The radical of ${}_A\mathsf{mod}$

1.3.1. If M and N are modules, the ***radical*** of $\hom(M, N)$ is the set $\mathsf{rad}(M, N)$ of the morphisms $f : N \to N$ such that whenever Z is an indecomposable module and $u : Z \to M$ and $v : N \to Z$ are morphisms, the composition

$$Z \xrightarrow{u} M \xrightarrow{f} N \xrightarrow{v} Z$$

is *not* an isomorphism.

1.3.2. Proposition. *The radical rad is an ideal of the category ${}_A\mathsf{mod}$. In other words, if M and N be modules then:*

(*i*) *The subset $\mathsf{rad}(M, N)$ of $\hom(M, N)$ is a subspace.*

(*ii*) *If P is a module, $f \in \mathsf{rad}(M, N)$ and $g \in \hom(N, P)$, then $gf \in \mathsf{rad}(M, P)$.*

(*iii*) *If P is a module $f \in \mathsf{rad}(M, N)$ and $g \in \hom(P, M)$, then $fg \in \mathsf{rad}(P, N)$.*

Proof. (*i*) Let $f, g \in \mathsf{rad}(M, N)$ and let $\lambda \in \Bbbk$. Let Z be an indecomposable module and let $u : Z \to M$ and $v : N \to Z$ be morphisms. As f and g are in $\mathsf{rad}(M, N)$, we have that vfu and vgu are non-invertible elements of the algebra $\mathsf{End}(Z)$. As this algebra is local, the set of its non-invertible elements is an ideal and then $v(f + \lambda g)u = vfu + \lambda vgu$ is also non-invertible. This shows that $f + \lambda g$ is in $\mathsf{rad}(M, N)$.

(*ii*) Let P be a module and let $f \in \mathsf{rad}(M, N)$ and $g \in \mathsf{hom}(N, P)$. If Z is an indecomposable module and $u : Z \to M$ and $v : P \to Z$ are morphisms, then the composition

$$Z \xrightarrow{u} M \xrightarrow{gf} P \xrightarrow{v} Z$$

is equal to the composition

$$Z \xrightarrow{u} M \xrightarrow{f} N \xrightarrow{vg} Z$$

which is not an isomorphism because $f \in \mathsf{rad}(M, N)$. It follows that $gf \in \mathsf{rad}(M, P)$, as we were to show. The proof of (*iii*) is similar. □

1.3.3. Proposition. *Let* r *be an ideal of* ${}_A\mathsf{mod}$. *Let* M *and* N *be two modules. If* $M_1, \dots, M_n$ *are submodules of* M *and* $N_1, \dots, N_m$ *are submodules of* N *such that* $M = \bigoplus_{i=1}^n M_i$ *and* $N = \bigoplus_{j=1}^m N_i$, *then the canonical isomorphism*

$$\phi : \mathsf{hom}_A(M, N) \to \bigoplus_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}} \mathsf{hom}_A(M_i, N_i)$$

restricts to an isomorphism

$$\mathsf{r}_A(M, N) \to \bigoplus_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}} \mathsf{r}_A(M_i, N_i)$$

This applies, in particular, when $\mathsf{r} = \mathsf{rad}$, of course.

Proof. For each $i \in \{1, \dots, n\}$ we have morphisms $q_i^M : M_i \to M$ and $p_i^M : M \to M_i$, the canonical inclusions and the canonical projections, such that $\mathrm{id}_M = \sum_{i=1}^n q_i p_i$, $p_i q_i = \mathrm{id}_{M_i}$ for all $i \in \{1, \dots, n\}$, and $p_i q_j = 0$ if $i, j \in \{1, \dots, n\}$ are different. Similarly, we have morphisms $q_j^N : N_j \to N$ and $p_j^N : N \to N_j$ for each $j \in \{1, \dots, m\}$ with analogous properties. The isomorphism ϕ of the statement is the map such that $\phi(f) = (p_j^N f q_i^M)_{1 \leq i \leq n, 1 \leq j \leq m}$ for all $f \in \mathsf{hom}_A(M, N)$.

If f is in $\mathsf{r}_A(M, N)$, then $p_j^N f p_i^M \in \mathsf{r}_A(M_n, N_j)$ for all $i \in \{1, \dots, n\}$ and all $j \in \{1, \dots, m\}$, because r is an ideal. This means that the isomorphim ϕ maps $\mathsf{r}_A(M, N) \subseteq \mathsf{hom}_A(M, N)$ into the direct sum $\bigoplus_{1 \leq i \leq n, 1 \leq j \leq m} \mathsf{r}_A(M_i, N_i)$. On the other hand, if $g = (f_{i,j})_{1 \leq i \leq n, 1 \leq j \leq m}$ is an element of that direct sum, then the morphism $f = \sum_{1 \leq i \leq n, 1 \leq j \leq m} q_j^N f_{i,j} p_i^M$ belongs to $\mathsf{r}_A(M, N)$, because r is an ideal, and for each $i \in \{1, \dots, n\}$ and each $j \in \{1, \dots, m\}$ we have that

$$p_j^N f q_i^M = \sum_{\substack{1 \leq k \leq n \\ 1 \leq l \leq m}} p_j^N q_l^N f_{k,l} p_k^M q_i^M = \Big(\sum_{1 \leq j \leq m} p_j^N q_j^N \Big) f_{i,j} \Big(\sum_{1 \leq i \leq n} p_i^M q_i^M \big) = f_{i,j}.$$

This shows that $\phi(f) = g$ and allows us to conclude that the image of $\mathsf{r}_A(M, N)$ by ϕ is precisely $\bigoplus_{1 \leq i \leq n, 1 \leq j \leq m} \mathsf{r}_A(M_i, N_i)$ □

1.3.4. Proposition. *If M and N are indecomposable modules, then* $\mathsf{rad}(M, N)$ *is the set of elements of* $\mathsf{hom}(M, N)$ *which are not isomorphisms.*

Proof. Let $f \in \mathsf{hom}(M, N)$. If f is an isomorphism, then the composition

$$M \xrightarrow{\mathrm{id}_M} M \xrightarrow{f} N \xrightarrow{f^{-1}} M$$

is an isomorphism, so that $f \notin \mathsf{rad}(M, N)$. Conversely, if $f \notin \mathsf{rad}(M, N)$ then there exist an indecomposable module Z and morphisms $u : Z \to M$ and $v : N \to Z$ such that the composition

$$Z \xrightarrow{u} M \xrightarrow{f} N \xrightarrow{v} Z$$

is an isomorphism. Let h be its inverse. The map $uhvf$ is an idempotent element of $\mathsf{End}(M)$, since

$$uhvf \cdot uhvd = u(hvfu)hvd = uhvd,$$

and as that algebra is local it follows that $uhvf$ is 0 or id_M. If we had $uhvf = 0$, then we would have that

$$u = u\,\mathrm{id}_Z = uhvfu = 0\,u = 0,$$

which is impossible. We thus see that $uhvf = \mathrm{id}_M$ and, in particular, that f is injective. A similar reasoning starting from the fact that $fuhv$ is an idempotent element of $\mathsf{End}(N)$ concludes that f is also surjective, so that f is an isomorphism, as we wanted. □

1.3.5. Proposition. *If M and N are modules, then a morphism $f : M \to N$ is in* $\mathsf{rad}_A(M, N)$ *iff for all morphisms $h : N \to M$ the map $\mathrm{id}_M - hf : M \to M$ is an isomorphism.*

Proof. Let us write $\mathsf{rad}'(M, N)$ the subset of $\mathsf{hom}_A(M, N)$ of morphisms $f : M \to N$ such that for all morphisms $h : M \to N$ the map $\mathrm{id}_M - hf$ is invertible in $\mathsf{End}_A(M)$. We have to prove that $\mathsf{rad}'(M, N) = \mathsf{rad}(M, N)$ for all modules M and N, and we start by showing that rad' is an ideal of the category ${}_A\mathsf{mod}$. Fix modules M, N and P.

- Let $f \in \mathsf{rad}'(M, N)$ and $g \in \mathsf{hom}_A(N, P)$. If $h : P \to M$ is a morphism, then $\mathrm{id}_M - hgf$ is invertible in $\mathsf{End}_A(M)$ because $f \in \mathsf{rad}'(M, N)$. This shows that $gf \in \mathsf{rad}'(M, P)$.
- Let now $f \in \mathsf{rad}'(M, N)$ and $g \in \mathsf{hom}_A(P, M)$. If $h : N \to P$ is a morphism, then the hypothesis on f implies that there exists a $\phi \in \mathsf{End}_A(M)$ such that $\phi(\mathrm{id}_M - ghf) = (\mathrm{id}_M - ghf)\phi = \mathrm{id}_M$. Using this, we see that

  $$(\mathrm{id}_P - hfg)(\mathrm{id}_P + hf\phi g) = \mathrm{id}_P - hfg + hf\phi g - hfghf\phi g = \mathrm{id}_P$$

  and

  $$(\mathrm{id}_P + hf\phi g)(\mathrm{id}_P - hfg) = \mathrm{id}_P - hfg + hf\phi g - hf\phi ghfg = \mathrm{id}_P,$$

  so that $\mathrm{id}_P - hfg$ is invertible in $\mathsf{End}_A(P)$. This shows that $fg \in \mathsf{rad}'(P, N)$.

- Finally, suppose that $f, f' \in \mathsf{rad}'(M,N)$ and let $h : N \to M$ be a morphism. Since $f \in \mathsf{rad}'(M,N)$, there exists an isomophism $\phi : M \to M$ such that $\phi(\mathrm{id}_M - hf) = \mathrm{id}_M$ and, since $f' \in \mathsf{rad}'(M,N)$, there exists an isomorphism $\psi : M \to M$ such that $\psi(\mathrm{id}_M - \phi hf) = \mathrm{id}_M$. It follows that

$$\psi\phi(\mathrm{id}_M - h(f+f')) = \psi\phi(\mathrm{id}_M - hf) - \psi\phi hf' = \psi - \psi\phi hf' = \mathrm{id}_M$$

  and, as $\psi\phi$ is an isomorphism, this implies that $\mathrm{id}_M - h(f+f')$ is an isomorphism.

Let us next show that if M is indecomposable then $\mathsf{rad}(M,N) = \mathsf{rad}'(M,N)$. First, if $f \in \mathsf{rad}(M,N)$ and $h : N \to M$ is a morphism, then it follows from the definition of rad that $hf \in \mathsf{End}_A(M)$ is not an isomorphism and, as $\mathsf{End}_A(M)$ is a local algebra, Proposition 1.1.1 allows us to conclude that $\mathrm{id}_M - hf$ is an isomorphism. We therefore have $f \in \mathsf{rad}'(M,N)$. Conversely, suppose that $f \in \mathsf{rad}'(M,N)$ and, to reach a contradiction, that $f \notin \mathsf{rad}(M,N)$, so that there are an indecomposable module Z and morphisms $u : Z \to M$ and $v : N \to Z$ such that vfu is an isomorphism and, in particulat, there is a $w \in \mathsf{End}_A(Z)$ such that $wvfu = \mathrm{id}_Z$. As $f \in \mathsf{rad}'(M,N)$, the map $\mathrm{id}_M - uwvf$ is invertible and there exists a $\phi \in \mathsf{End}_A(M)$ such that $(\mathrm{id}_M - uwvf)\phi = \mathrm{id}_M$. It follows that

$$\begin{aligned} 0 &= (\mathrm{id}_Z - wvfu)(\mathrm{id}_Z + wvf\phi u) \\ &= \mathrm{id}_Z - wvfu + wvf(\mathrm{id}_M - uwvf)\phi u \\ &= \mathrm{id}_Z \end{aligned}$$

and this is absurd because Z is not the zero module.

Finally, let M and N be arbitrary. Suppose that $M_1, \ldots, M_n$ are indecomposable submodules of M such that $M = \bigoplus_{i=1}^n M_i$ and for each $i \in \{1, \ldots, n\}$ let $p_i : M \to M_i$ be the canonical projection corresponding to this direct sum decomposition and $p_i^* : \mathsf{hom}_A(M_i, N) \to \mathsf{hom}_A(M,N)$ the induced map. We know from Proposition 1.3.3 that $\mathsf{rad}(M,N) = \sum_{i=1}^n p_i^*(\mathsf{rad}(M_i,N))$. On the other hand, since rad' is also an ideal of ${}_A\mathsf{mod}$, the same proposition tells us that $\mathsf{rad}'(M,N) = \sum_{i=1}^n p_i^*(\mathsf{rad}'(M_i,N))$. Since $\mathsf{rad}'(M_i,N) = \mathsf{rad}'(M_i,N))$ for each $i \in \{1, \ldots, n\}$ because the M_i are indecomposable, the equality $\mathsf{rad}(M,N) = \mathsf{rad}'(M,N)$ follows at once. □

§1.4. The Krull-Remak-Schmidt theorem

1.4.1. The following fundamental result is due to Wolfgang Krull [Kru1925], Robert Remak [Rem1911] y Otto Schmidt [Sch1929] :

Theorem. *If M is a non-zero module, then there exist a non-negative integer r, pairwise non-isomorphic indecomposable modules $M_1, \dots, M_r$ and positive integers $a_1, \dots, a_r$ such that*

$$M \cong M_1^{a_1} \oplus \cdots \oplus M_r^{a_r}.$$

This direct sum decomposition is unique in the following sense: if s is a non-negative integer, $N_1, \dots, N_s$ pairwise non-isomorphic indecomposable modules and $b_1, \dots, b_s$ positive integers such that $M \cong N_1^{b_1} \oplus \cdots \oplus N_s^{b_s}$, then $s = r$ and there is a permutation σ of $\{1, \dots, r\}$ such that $N_i \cong M_{\sigma(i)}$ and $b_i = a_{\sigma(i)}$ for each $i \in \{1, \dots, r\}$.

Proof. In order to prove the existence of the direct sum decomposition we proceed by induction on $\dim M$. If $\dim M = 1$, the module M is clearly indecomposable and there is nothing to do, so we may assume that $\dim M > 1$. If M is indecomposable, then again there is nothing to be done. If it is instead decomposable, then there are proper submodules M' and M'' of M such that $M = M' \oplus M''$ and, since $\dim M' < \dim M$ and $\dim M'' < \dim M$, the induction hypothesis implies that both M and M' can be written as a direct sum of indecomposable submodules. We thus see that the same is true of M.

Let now r be a positive integer, let $M_1, \dots, M_r$ be pairwise non-isomorphic indecomposable modules, and let $a_1, \dots, a_r$ be positive integers such that

$$M \cong M_1^{a_1} \oplus \cdots \oplus M_r^{a_r}.$$

Let Z be an indecomposable module. We have direct sum decompositions

$$\mathsf{hom}(Z, M) \cong \bigoplus_{i=1}^{r} \mathsf{hom}(Z, M_i)^{a_i}, \qquad \mathsf{rad}(Z, M) \cong \bigoplus_{i=1}^{r} \mathsf{rad}(Z, M_i)^{a_i}$$

which are compatible in the obvious sense, so that there is an isomorphism

$$\mathsf{top}(Z, M) \cong \bigoplus_{i=1}^{r} \mathsf{top}(Z, M_i)^{a_i}. \tag{3}$$

If $i \in \{1, \dots, r\}$, we know from Proposition 1.3.4 that $\mathsf{top}(Z, M_i) = 0$ iff $Z \ncong M_i$, and it follows from this and the direct sum decomposition (3) that

- if $Z \ncong M_i$ for all $i \in \{1, \dots, r\}$, then $\mathsf{top}(Z, M) = 0$, and
- if $i \in \{1, \dots, r\}$ and $Z \cong M_j$ then

$$a_j = \frac{\dim \mathsf{top}(Z, M)}{\dim \mathsf{top}(Z, Z)}.$$

We can then conclude that in every decomposition of M as a direct sum of indecomposable modules there are exactly $\dim \operatorname{top}(Z, M) / \dim \operatorname{top}(Z, Z)$ summands isomorphic to any given indecomposable module Z. The last claim of the theorem follows from this. □

§1.5. The Jordan-Hölder theorem

1.5.1. A module M is ***simple*** if it has exactly two submodules, which are then necessarily the zero submodule and M itself and, as they are different, moreover, we must have $M \neq 0$.

1.5.2. If M is a module, a ***composition series*** for M is a finite strictly ascending chain

$$0 = M_0 \subsetneq M_1 \subsetneq M_2 \subsetneq \cdots \subsetneq M_n = M$$

of submodules of M such that for each $i \in \{1, \dots, n\}$ the quotient M_i / M_{i-1} is simple, and the number n is the ***length*** of the composition series.

1.5.3. Proposition. *Every module admits a composition series.*

Proof. Let us show that a module M admits a composition series proceeding by induction on its dimension. If $M = 0$, there is nothing to do, so we suppose that $\dim M > 0$. Let $M' \subsetneq M$ be a proper maximal submodule; such a thing exists, for M does have proper submodules. As $\dim M' < \dim M$, we may assume inductively that M' admits a composition series

$$0 = M_0 \subsetneq M_1 \subsetneq M_2 \subsetneq \cdots \subsetneq M_n = M',$$

and since M' is a maximal submodule the quotient M/M' is simple. It follows then that

$$0 = M_0 \subsetneq M_1 \subsetneq M_2 \subsetneq \cdots \subsetneq M_n \subsetneq M$$

is a composition series for M. □

1.5.4. Proposition. *If M is a module, M', M'' and N are submodules of M and $M' \subseteq M''$, then*

$$M' + M'' \cap N = M'' \cap (M' + N) \tag{4}$$

and there is a short exact sequence of the form

$$0 \longrightarrow \frac{M'' \cap N}{M' \cap N} \xrightarrow{f} \frac{M''}{M'} \xrightarrow{g} \frac{M'' + N}{M' + N} \longrightarrow 0$$

Proof. Let us show the equality (4). If $x \in M'' \cap (M' + N)$, then $x \in M''$ and there exist $m' \in M$ and $n \in N$ such that $x = m' + n$. It follows from this that $x - m' = n \in N$ and $x - m' \in M'' + M' \subseteq M''$, so $x - m \in N \cap M$ and $x = m' + (x - m') \in M' + M'' \cap N$. Conversely, suppose that $x \in M' + M'' \cap N$, so that there exist $m' \in M'$ and $y \in M'' \cap N$ such that $x = m' + y$. As $y \in M''$, we have $x = m' + y \in M' + M'' = M''$ and, as $y \in N$, also $x = m' + y \in M' + N$: we thus see that $x \in M'' \cap (M' + N)$.

We define maps f and g to construct the sequence of the proposition simply putting $f(x + M' \cap N) = x + N'$ for all $x \in M'' \cap N$ and $g(x + M') = x + M' + N$ for all $x \in M''$. The verification that $g \circ f = 0$ and that the maps f an g are injective and surjective, respectively is immediate, and the exactness at M''/M' of the sequence is easily seen to be precisely the content of the equality (4) we have just established. □

1.5.5. The following theorem —for the case of groups— was originally proved by Camille Jordan [Jor1989] and Otto Hölder [Höl1889].

Theorem. *Let M be a module. If*

$$0 = M_0 \subsetneq M_1 \subsetneq M_2 \subsetneq \cdots \subsetneq M_n = M$$

and

$$0 = M'_0 \subsetneq M'_1 \subsetneq M'_2 \subsetneq \cdots \subsetneq M'_m = M$$

are two composition series for M, then $n = m$ and there is a permutation σ of $\{1, \dots, n\}$ such that $M'_{\sigma(i)}/M'_{\sigma(i)-1} \cong M_i/M_{i-1}$ for all $i \in \{1, \dots, n\}$.

Proof. We proceed by induction on n. If $n = 1$, then M is simple and there exactly one composition series for M, so there is nothing to prove. We may assume, then, that $n > 1$.

We have a chain of submodules

$$M_{n-1} = M_{n-1} + M'_0 \subseteq M_{n-1} + M'_1 \subseteq M_{n-1} + M'_2 \subseteq \cdots \subseteq M_{n-1} + M'_m = M_n$$

of M. Since M_n/M_{n-1} is simple, exactly *one* of these inclusions is strict, that is, there exists a $i_0 \in \{1, \dots, m\}$ such that

$$\frac{M_{n-1} + M'_{i_0}}{M_{n-1} + M'_{i_0-1}} \cong \frac{M_n}{M_{n-1}} \neq 0, \tag{5}$$

and

$$\frac{M_{n-1} + M'_i}{M_{n-1} + M'_{i-1}} \cong 0 \text{ for all } i \in \{1, \dots, m\} \setminus \{i_0\}. \tag{6}$$

On the other hand, if $i \in \{1, \dots, m\}$ we have a short exact sequence, constructed as in Proposition 1.5.4, of the form

$$0 \longrightarrow \frac{M_{n-1} \cap M'_i}{M_{n-1} \cap M'_{i-1}} \longrightarrow \frac{M'_i}{M'_{i-1}} \longrightarrow \frac{M_{n-1} + M'_i}{M_{n-1} + M'_{i-1}} \longrightarrow 0$$

and, since the quotient M'_i/M'_{i-1} is simple, exactly one of $(M_{n-1} \cap M'_i)/(M_{n-1} \cap M'_{i-1})$ or $(M_{n-1} + M'_i)/(M_{n-1} + M'_{i-1})$ is zero and the other is isomorphic to M'_i/M'_{i-1}. In view of (5) and (6), we see that

$$\frac{M_{n-1} + M'_{i_0}}{M_{n-1} + M'_{i_0-1}} \cong \frac{M'_{i_0}}{M'_{i_0-1}}, \qquad \frac{M_{n-1} \cap M'_{i_0}}{M_{n-1} \cap M'_{i_0-1}} \cong 0$$

and for all $i \in \{1, \dots, n\} \setminus \{i_0\}$

$$\frac{M_{n-1} + M'_i}{M_{n-1} + M'_{i-1}} \cong 0, \qquad \frac{M_{n-1} \cap M'_i}{M_{n-1} \cap M'_{i-1}} \cong \frac{M'_i}{M'_{i-1}}.$$

We thus see that

$$\begin{aligned} 0 = M_{n-1} \cap M'_0 \subseteq M_{n-1} \cap M'_1 \subseteq M_{n-1} \cap M'_2 \subseteq \cdots \\ \cdots \subseteq M_{n-1} \cap M'_{i_0-1} \subseteq M_{n-1} \cap M'_{i_0+1} \subseteq \cdots \\ \cdots \subseteq \cdots \subseteq M_{n-1} \cap M'_m = M_{n-1} \end{aligned} \tag{7}$$

is a composition series for M_{n-1} of length $m-1$ whose successive simple quotients are isomorphic to

$$\frac{M'_1}{M'_0}, \quad \dots, \quad \frac{M'_{i_0-1}}{M'_{i_0-2}}, \quad \frac{M_{n-1} \cap M'_{i_0+1}}{M_{n-1} \cap M'_{i_0-1}}, \quad \frac{M'_{i_0+2}}{M'_{i_0+1}}, \quad \dots, \quad \frac{M'_m}{M'_{m-1}}.$$

We know that $M_{n-1} \cap M'_{i_0-1} = M_{n-1} \cap M'_{i_0}$ and $M_{n-1} \cap M'_{i_0+1} = M_{n-1} \cap M'_{i_0}$, so that

$$\frac{M_{n-1} \cap M'_{i_0+1}}{M_{n-1} \cap M'_{i_0-1}} \cong \frac{M_{n-1} \cap M'_{i_0+1}}{M_{n-1} \cap M'_{i_0}} \cong \frac{M'_{i_0+1}}{M'_{i_0}}.$$

On the other hand,

$$0 = M_0 \subsetneq M_1 \subsetneq M_2 \subsetneq \cdots \subsetneq M_{n-1} \tag{8}$$

is also composition series for M_{n-1} of length $n-1$. We can therefore use our induction hypothesis to compare (7) and (8) and conclude that $n-1 = m-1$, so that $n = m$, and that there is a bijection $\sigma : \{1, \dots, n-1\} \to \{1, \dots, i_0-1, i_0+1, \dots, n\}$ such that $M'_{\sigma(i)}/M'_{\sigma(i)-1} \cong M_i/M_{i-1}$ for all $i \in \{1, \dots, n-1\}$. Clearly, we can extend σ to a permutation of $\{1, \dots, n\}$ by setting $\sigma(n) = i_0$ and then we also have $M'_{\sigma(n)}/M'_{\sigma(n)-1} = M'_{i_0}/M'_{i_0-1}$. This permutation σ satisfies the conditions required by the theorem. □

1.5.6. An immediate consequence of Theorem 1.5.5 is that all composition series for a module M have the same length, which we may therefore call unambiguously the ***length*** of M and write it $\ell(M)$. This function of modules is additive in the following sense:

1.5.7. Proposition. *If*

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

is a short exact esquence of modules, then we have that

$$\ell(M) = \ell(M') + \ell(M'').$$

Proof. If

$$0 = M'_0 \subsetneq M'_1 \subsetneq M'_2 \subsetneq \cdots \subsetneq M'_n = M'$$

and

$$0 = M''_0 \subsetneq M''_1 \subsetneq M''_2 \subsetneq \cdots \subsetneq M''_m = M''$$

are composition series for M and for M'', respectively, then

$$\begin{multlined} 0 = f(M'_0) \subsetneq f(M'_1) \subsetneq f(M'_2) \subsetneq \cdots \\ \cdots \subsetneq f(M'_{n-1}) \subsetneq f(M'_n) = g^{-1}(M''_0) \subsetneq g^{-1}(M''_1) \subsetneq g^{-1}(M''_2) \subsetneq \cdots \\ \cdots \subsetneq g^{-1}(M''_{m-1}) \subsetneq g^{-1}(M''_m) = g^{-1}(M'') = M \end{multlined} \tag{9}$$

is a composition series for M. Indeed, we have that $f(M'_i)/f(M'_{i-1}) \cong M'_i/M'_{i-1}$ for each $i \in \{1, \dots, n\}$ and $g^{-1}(M''_j)/g^{-1}(M''_{j-1}) \cong M''_j/M''_{j-1}$ for each $j \in \{1, \dots, m\}$, so that all the successive quotients in the chain (9) are simple. As this composition series has length $n + m$, this proves the proposition. □

§1.6. Grothendieck groups

1.6.1. Let $\mathscr{A}$ be an additive category. A ***short exact sequence*** of $\mathscr{A}$ is a diagram

$$0 \longrightarrow X \xrightarrow{i} Y \xrightarrow{p} Z \longrightarrow 0$$

such that i is a kernel for p and p is a cokernel for i. We say that this short exact sequence is ***isomorphic*** to another short exact sequence

$$0 \longrightarrow X' \xrightarrow{i'} Y' \xrightarrow{p'} Z' \longrightarrow 0$$

if there exist isomorphisms $f : X \to X'$, $g : Y \to Y'$ and $h : Z \to Z'$ in $\mathscr{A}$ which render the following diagram commutative.

$$\begin{tikzcd} 0 \arrow[r] & X \arrow[r, "i"] \arrow[d, "f"'] & Y \arrow[r, "p"] \arrow[d, "g"'] & Z \arrow[r] \arrow[d, "h"'] & 0 \\ 0 \arrow[r] & X' \arrow[r, "i'"] & Y' \arrow[r, "p'"] & Z' \arrow[r] & 0 \end{tikzcd}$$

Isomorphism of short exact sequences is an equivalence relation.

If X and Y are objects of $\mathscr{A}$, there are morphisms

$$\begin{tikzcd} X \arrow[r, shift left, "i_1"] & X \oplus Y \arrow[l, shift left, "q_1"] \arrow[r, shift right, "q_2"'] & Y \arrow[l, shift right, "i_2"'] \end{tikzcd}$$

in $\mathscr{A}$ such that $q_1 i_1 = \mathrm{id}_X$, $q_2 i_2 = \mathrm{id}_Y$, $i_1 q_1 + i_2 q_2 = \mathrm{id}_{X \oplus Y}$ $q_2 i_1 = 0$ and $q_1 i_2 = 0$, and using these relations it is easy to check that

$$0 \longrightarrow X \xrightarrow{i_1} X \oplus Y \xrightarrow{q_2} Y \longrightarrow 0$$

is a short exact sequence. We say that a short exact sequence is ***split*** if it is isomorphic to one of this form .

1.6.2. Let $\mathscr{A}$ be an essentially small additive category and let $\mathscr{E}$ be a class of short exact sequences of $\mathscr{A}$ which closed under isomorphism; we call the elements of $\mathscr{E}$ the ***$\mathscr{E}$-admissible short exact sequences***. If X is an object of $\mathscr{A}$, we write $[X]$ the isomorphism class of X and we let $L(\mathscr{A})$ be the free abelian group with basis the set of isomorphism classes of the objects of $\mathscr{A}$. The ***Grothedieck group*** of the pair[1] $(\mathscr{A}, \mathscr{E})$ is the quotient $K(\mathscr{A}, \mathscr{E})$ of $L(\mathscr{A})$ by the subgroup generated its elements of the form $[Y] - [X] - [Z]$ for which there is an $\mathscr{E}$-admissible short exact sequence

$$0 \longrightarrow X \longrightarrow Y \longrightarrow Z \longrightarrow 0$$

We write $\pi : L(\mathscr{A}) \to K(\mathscr{A}, \mathscr{E})$ the canonical projection and if X is an object of $\mathscr{A}$ we denote $[\![X]\!]$ the image of $[X]$ under π.

1.6.3. The key property of this construction is the following:

Proposition. *Let $\mathscr{A}$ be an essentially small additive category and let $\mathscr{E}$ be a class of short exact sequences of $\mathscr{A}$ which is closed under isomorphism. Let G is an abelian group and suppose that $\phi : \mathsf{obj}\,\mathscr{A} \to G$ is a function such that*

- *if X and Y are objects of $\mathscr{A}$ such that $X \cong Y$, then $\phi(X) = \phi(Y)$, and*
- *whenever*

  $$0 \longrightarrow X \longrightarrow Y \longrightarrow Z \longrightarrow 0$$

  is an $\mathscr{E}$-admissible short exact sequence, we have $\phi(Y) = \phi(X) + \phi(Y)$.

Then there exists a unique group homomorphism $\bar{\phi} : K(\mathscr{A}, \mathscr{E}_0) \to G$ such that

$$\bar{\phi}([\![X]\!]) = \phi(X)$$

for all objects X of $\mathscr{A}$.

[1] One usually imposes more conditions on the class $\mathscr{E}$ of short exact sequences in order to obtain a theory of Grothedieck groups $K(\mathscr{A}, \mathscr{E})$ with good formal properties, but we will not need this for our purposes. It is often the case that one requires the pair $(\mathscr{A}, \mathscr{E})$ to be an *exact category*; we refer to the nice monograph [Büh2010] by Theo Bühler on the subject.

Proof. Since the set of elements of the form $[\![X]\!]$ with X an object of $\mathscr{A}$ generates the group $K(\mathscr{A},\mathscr{E})$, it is clear that if there is at most one such morphism ϕ'', so we need only prove the existence claim.

Let $[\mathscr{A}]$ denote the set of isomorphism classes of objects of $\mathscr{A}$. The first condition imposed on the function ϕ implies that there is a function $\phi_1 : [\mathscr{A}] \to G$ such that $\phi_1([X]) = \phi(X)$ for each object X of $\mathscr{A}$. As $[\mathscr{A}]$ is a basis for $L(\mathscr{A})$, there is a unique group morphism $\phi_2 : L(\mathscr{A}) \to G$ such that $\phi_2([X]) = \phi(X)$ for all objects X of $\mathscr{A}$. If

$$0 \longrightarrow X \longrightarrow Y \longrightarrow Z \longrightarrow 0$$

is an $\mathscr{E}$-admissible short exact sequence, then the second condition imposed on ϕ tells us that $\phi_2([Y] - [X] - [Z]) = 0$ and this implies that ϕ_2 vanishes on the kernel of the canonical projection $\pi : L(\mathscr{A}) \to K(\mathscr{A},\mathscr{E})$. It follows that there is a unique group morphism $\bar{\phi} : K(\mathscr{A},\mathscr{E}) \to G$ such that $\phi_2 = \bar{\phi}\pi$. In particular, we have $\bar{\phi}([\![X]\!]) = \phi_2([X]) = \phi(X)$ for all objects X of $\mathscr{A}$, and thus $\bar{\phi}$ has the required property. □

1.6.4. Proposition. *Let A be a finite dimensional algebra, let ${}_A\mathsf{mod}$ be the category of finite-dimensional A-modules, let $\mathscr{E}_0$ be the class of all short exact sequences of ${}_A\mathsf{mod}$, and let ${}_A\mathsf{ind}$ be a set of representatives for the isomorphism classes of indecomposable modules. The Grothendieck group $K({}_A\mathsf{mod},\mathscr{E}_0)$ is free with the set $\mathscr{B} = \{[\![M]\!] : M \in {}_A\mathsf{ind}\}$ as a basis.*

Proof. Write $K = K({}_A\mathsf{mod},\mathscr{E}_0)$ for simplicity. If M and N are modules, we have that

$$[\![M \oplus N]\!] = [\![M]\!] + [\![N]\!] \tag{10}$$

in K because $\mathscr{E}_0$ contains a short exact sequence of the form

$$0 \longrightarrow M \longrightarrow M \oplus N \longrightarrow N \longrightarrow 0$$

Notice that this implies, in particular, that $[\![0]\!] = 0$ in K: indeed, putting $M = N = 0$ in (10) we see that $[\![0]\!] = [\![0 \oplus 0]\!] = 2[\![0]\!]$, because $0 \cong 0 \oplus 0$.

It is clear that K is generated by the set of its elements of the form $[\![M]\!]$ with $M \in {}_A\mathsf{mod}$. Now if M is a non-zero module we know from Theorem 1.4.1 that there exist a positive integer r, pairwise distinct $M_1, \dots, M_r \in {}_A\mathsf{ind}$ and positive integers $a_1, \dots, a_r$ such that $M \cong M_1^{a_1} \oplus \cdots \oplus M_r^{a_r}$, and it follows from the equality (10) that in K we have

$$[\![M]\!] = a_1[\![M_1]\!] + \cdots + a_r[\![M_r]\!]$$

This shows that the group K is in fact generated by its subset $\mathscr{B}$. To complete the proof of the proposition, we have to show that the set $\mathscr{B}$ is linearly independent.

Let U be an indecomposable module. If M is a module, the uniqueness part of Theorem 1.4.1 tells us that there exists a maximal integer $\mu_U(M)$ such that $U^{\mu_U(M)}$ is isomorphic to a direct summand of M. It is clear that if M' is another module and $M' \cong M$, then we have $\mu_U(M) = \mu_U(M')$. On the other hand, if M and N are modules, it also follows from Theorem 1.4.1 that $\mu_U(M \oplus N) = \mu_U(M) + \mu_U(N)$, and an inmediate consequence of this is that if

$$0 \longrightarrow X \longrightarrow Y \longrightarrow Z \longrightarrow 0$$

is a split short exact sequence in ${}_A\mathsf{mod}$ then $\mu_U(Y) = \mu_U(X) + \mu_U(Z)$. We are thus in position to apply Proposition 1.6.3 to conclude that there is a group homomorphism $\bar{\mu}_U : K \to \mathbb{Z}$ such that $\bar{\mu}_U(\llbracket M \rrbracket) = \mu_U(M)$ for all modules M.

Notice that it follows at once from the definition of the function μ_U that if V is another indecomposable module, then $\bar{\mu}_U(\llbracket V \rrbracket)$ is 1 or 0, according to whether V and U are isomorphic or not.

Let now $Z_1, \dots, Z_r$ be distinct elements of ${}_A\mathsf{ind}$, let $a_1, \dots, a_r$ be integers, and suppose that $a_1\llbracket Z_1 \rrbracket + \cdots + a_r\llbracket Z_r \rrbracket = 0$. If $i \in \{1, \dots, r\}$ we find that $a_i = 0$ by applying the morphism $\bar{\mu}_{Z_i}$ to both sides of that equality. This proves the set $\mathscr{B}$ is linearly independent. □

1.6.5. Proposition. *Let A be a finite dimensional algebra, let ${}_A\mathsf{mod}$ be the category of finite-dimensional A-modules, let $\mathscr{E}_\infty$ be the class of all short exact sequences of ${}_A\mathsf{mod}$, and let ${}_A\mathsf{simp}$ be a set of representatives for the isomorphism classes of simple modules. The Grothendieck group $K({}_A\mathsf{mod}, \mathscr{E}_\infty)$ is free with the set $\mathscr{B} = \{\llbracket S \rrbracket : S \in {}_A\mathsf{simp}\}$ as a basis.*

Proof. Let us write $K = K({}_A\mathsf{mod}, \mathscr{E}_\infty)$. We claim that the set $\mathscr{B}$ generates K as an abelian group. To see this we will show that $\llbracket M \rrbracket$ is in the span $\langle \mathscr{B} \rangle$ of $\mathscr{B}$ for all modules M proceeding by induction on the length $\ell(M)$. If $\ell(M) = 0$, then $M = 0$, and just as in the proof of Proposition 1.6.4 we see that $\llbracket M \rrbracket = 0$, so there is nothing to be done in this case.

Let us therefore suppose that $\ell(M) > 0$. There exists, in particular, a submodule $M' \subseteq M$ such that $\ell(M') = \ell(M) - 1$, so that inductively $\llbracket M \rrbracket \in \langle \mathscr{B} \rangle$, and the quotient M/M' is simple. There exists then an $S \in {}_A\mathsf{simp}$ and a short exact sequence of the form

$$0 \longrightarrow M' \longrightarrow M \longrightarrow S \longrightarrow 0$$

in $\mathscr{E}_\infty$, and this implies that $\llbracket M \rrbracket = \llbracket M' \rrbracket + \llbracket S \rrbracket \in \langle \mathscr{B} \rangle$. This proves our claim.

To complete the proof of the proposition, we have to show that the set $\mathscr{B}$ is linearly independent in K. Let us fix a simple module S. If M is a module, then we know that there exists a composition series

$$0 = M_0 \subsetneq M_1 \subsetneq M_2 \subsetneq \cdots \subsetneq M_n = M$$

and that the number $\nu_S(M) = |\{i \in \{1, \dots, n\} : M_i/M_{i-1} \cong S\}|$ depends only on M and not on the particular composition series chosen. This defines a function $\nu_S : \mathsf{obj}\,{}_A\mathsf{mod} \to \mathbb{Z}$, and it is clear that it has the property that $\nu_S(M) = \nu_S(M')$ whenever M and M' are isomorphic objects of $\mathscr{A}$.

Suppose now that

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

is a short exact sequence in ${}_A\mathsf{mod}$ and that

$$0 = M'_0 \subsetneq M'_1 \subsetneq M'_2 \subsetneq \cdots \subsetneq M'_n = M'$$

and

$$0 = M''_0 \subsetneq M''_1 \subsetneq M''_2 \subsetneq \cdots \subsetneq M''_m = M''$$

are composition series for M and for M'', respectively. As we noted in the proof of Proposition **1.5.7**, it follows that

$$\begin{aligned}0 = f(M'_0) \subsetneq f(M'_1) \subsetneq f(M'_2) \subsetneq \cdots \\ \cdots \subsetneq f(M'_{n-1}) \subsetneq f(M'_n) = g^{-1}(M''_0) \subsetneq g^{-1}(M''_1) \subsetneq g^{-1}(M''_2) \subsetneq \cdots \\ \cdots \subsetneq g^{-1}(M''_{m-1}) \subsetneq g^{-1}(M''_m) = g^{-1}(M'') = M\end{aligned}$$

is a composition series for M, with succesive quotients $f(M'_i)/f(M'_{i-1}) \cong M'_i/M'_{i-1}$ for each $i \in \{1, \ldots, n\}$ and $g^{-1}(M''_j)/g^{-1}(M''_{j-1}) \cong M''_j/M''_{j-1}$ for each $j \in \{1, \ldots, m\}$. As a consequence of this, we see that

$$\begin{aligned}\nu_S(M) &= |\{i \in \{1, \ldots, n\} : M'_i/M'_{i-1} \cong S\}| + |\{j \in \{1, \ldots, m\} : M''_j/M''_{j-1} \cong S\}| \\ &= \nu_S(M') + \nu_S(M'').\end{aligned}$$

We can therefore conclude, thanks to Proposition **1.6.3**, that there is a group morphism $\bar{\nu}_S : K \to \mathbb{Z}$ such that $\bar{\nu}_S(\llbracket M \rrbracket) = \nu_S(M)$ for all modules M.

We are now in position to prove the liner independence of the set $\mathscr{B}$. Let $S_1, \ldots, S_r$ be distinct elements of ${}_A\mathsf{simp}$ and let $a_1, \ldots, a_r$ be integers such that

$$a_1\llbracket S_1 \rrbracket + \cdots + a_r\llbracket S_r \rrbracket = 0$$

in K. If $i, j \in \{1, \ldots, r\}$ we have $\bar{\nu}_{S_i}(\llbracket S_j \rrbracket) = \nu_{S_i}(S_j) = \delta_{i,j}$, so applying the morphism $\bar{\nu}_{S_i}$ to both sides of the equality (5) we see at once that $a_i = 0$ for each $i \in \{1, \ldots, r\}$. $\square$

CHAPTER 2

Semisimple algebras

§2.1. Simple modules

2.1.1. Proposition.

(*i*) *If I is a left ideal in A, then A/I is a simple module iff I is a maximal left ideal.*

(*ii*) *There exist simple modules.*

Proof. The first statement is a consequence of the bijection between the set of submodules of A/I and the left ideals of A containing I. The second follows from the first simply because we know there are maximal left ideals in A. □

2.1.2. The following simple but fundamental result is due to Issai Schur [Sch1905].

Proposition. *Let S and S' be simple modules and let M be an arbitrary module.*

(*i*) *A morphism $f : S \to M$ is either zero or injective.*

(*ii*) *A morphism $f : M \to S$ is either zero or surjective.*

(*iii*) *A morphism $f : S \to S'$ is either zero or an isomorphism.*

Proof. The first two statements follow at once from the fact that 0 is the unique proper submodule of S and the third one from the other two. □

2.1.3. Corollary. *The endomorphism algebra of a simple module is a division algebra.*

Proof. This follows at once from the third part of Proposition 2.1.2. □

§2.2. Semisimple modules

2.2.1. A module is ***semisimple*** if it is a sum of simple submodules.

2.2.2. Proposition. *Let M be a module and suppose $\{S_i\}_{i \in I}$ is a family of simple submodules of M such that $M = \sum_{i \in I} S_i$. If $N \subseteq M$ is a submodule, then there exists a subset $J \subseteq I$ such that $M = N \oplus \bigoplus_{j \in J} S_j$. In particular, every submodule of M is a direct summand.*

Proof. Let $\mathscr{J}$ be the set of subsets $J \subseteq I$ such that the sum $N + \sum_{j \in J} S_j$ is direct. As $\varnothing \in \mathscr{J}$, we have $\mathscr{J} \neq \varnothing$. On the other hand, as M is finite-dimensional and each simple module has positive dimension, there exists a $J \in \mathscr{J}$ maximal with respect to inclusion. Let $M' = N + \sum_{j \in J} S_j$; this sum is in fact direct because $J \in \mathscr{J}$.

Let $i \in I$. As S_i is simple, the intersection $S_i \cap M'$ is either zero or equal to S_i. In the first case, the sum $M' + S_i = N + \sum_{j \in J \cup \{i\}} S_j$ would be direct, contradicting our choice of J, so we must have that $S_i \subseteq M'$. We thus see that $M = \sum_{i \in I} S_i \subseteq M'$ and, therefore, that $M' = M$. This proves the proposition. □

2.2.3. Lemma. *If M is a module such that every submodule is a direct summand, then every non-zero submodule of M contains a simple submodule.*

Proof. Let M' is a non-zero submodule of M, so that there exists an $m \in M' \setminus 0$. The annihilator $\mathsf{ann}(m) = \{a \in A : a = 0\}$ is a left ideal in A and it is is therefore contained in a maximal left ideal I of A. It follows that Im is a maximal submodule of Am. The hypothesis on M implies that there is a submodule M' in M such that $M = Im \oplus M'$ and using the modular law from Proposition 1.5.4 we see that $Am = M \cap Am = (Im \oplus L) \cap Am = Im \oplus (L \cap Am)$; in particular, the intersection $L \cap Am \cong Am/Im$ is simple. As $L \cap Am$ is contained in M', this proves the lemma. □

2.2.4. Proposition. *If M is a module, the following statements are equivalent:*

(*a*) *M is semisimple.*

(*b*) *M is the direct sum of a family of simple submodules.*

(*c*) *Every submodule of M is a direct summand.*

Proof. The implication (a) $\Rightarrow$ (b) is the special case of Proposition 2.2.2 in which $N = 0$ and the converse implication is trivial. The implication (a) $\Rightarrow$ (c) is the last claim of Proposition 2.2.2, so we are left with proving that (c) $\Rightarrow$ (a).

Suppose then that M satisfies the condition (c) and let $M' \subseteq M$ be the sum of all simple submodules of M. The hypothesis implies that there exists a submodule M'' of M such that $M = M' \oplus M''$. If M'' were non-zero, it would follow from Lemma 2.2.3 that it contains a simple submodule S, and this is absurd as we would then have that $M' \cap M'' \supseteq S \neq 0$. We must therefore have $M'' = 0$, so that in fact $M = M'$, and this tells us that M is semisimple. □

2.2.5. Corollary. *Every submodule of a semisimple module is itself semisimple. More precisely, if M be a module, $\{S_i\}_{i \in I}$ a family of simple submodules of M such that $M = \sum_{i \in I} S_i$, and N a submodule of M, then there exists a subset $J \subseteq J$ such that $N \cong \bigoplus_{j \in J} S_j$.*

Proof. It is enough to prove the second statement. From Proposition 2.2.4 we know that N is a direct summand of M, so there exists a submodule P of M such that $M = N \oplus P$. On the other hand, Proposition 2.2.2 tells us that there is a subset $J \subseteq I$ such that $M \cong P \oplus \bigoplus_{j \in J} S_j$. It follows then that $N \cong M/P \cong \bigoplus_{j \in J} S_j$. □

2.2.6. Corollary. *If*

$$0 \longrightarrow M' \xrightarrow{f} M \longrightarrow M'' \longrightarrow 0$$

is a short exact sequence of modules and M is semisimple, then the short exact sequence splits and both M' and M'' are semisimple.

Proof. The submodule $f(M')$ of M is a direct sumand because M is semisimple, so there is a submodule N of M such that $M = f(M) \oplus N$. As f is injective the correstriction $f : M' \to f(M')$ is an isomorphism and it has an inverse $g : f(M') \to M'$. It follows at once that the map $r = \begin{pmatrix} g & 0 \end{pmatrix} : M = f(M') \oplus N \to M'$ is such that $rs = \mathrm{id}_{M'}$, so the short exact sequence splits. In particular, there is an isomorphism $M \cong M' \oplus M''$ and M' and M'' are isomorphic to submodules of M which are, according to Corollary 2.2.5, semisimple. This proves the result. $\square$

§2.3. Semisimple algebras

2.3.1. An algebra A is ***semisimple*** if the left module ${}_AA$ is semisimple.

2.3.2. Recall than an algebra is ***simple*** if it does not have non-zero proper bilateral ideals.

Proposition. *Let A be a simple algebra. Then A is a semisimple algbra and all its simple modules are isomorphic. If S is a simple module, then $D = \mathsf{End}(S)$ is a division algebra and there exists a positive integer n such that $A \cong M_n(D^{\mathsf{op}})$ and we have $\dim S = n \dim D$.*

Proof. Let I be a non-zero left ideal of A of minimal dimension; clearly, I is simple as a module. The vector space $X = \hom(I, A)$ is non-zero, because it contains the non-zero morphism given by the inclusion $I \hookrightarrow A$, and finite-dimensional. Let $\mathscr{B} = \{\phi_1, \dots, \phi_n\}$ be a basis for X, write $I^n = I \oplus \cdots \oplus I$ and consider the morphism

$$\phi : (x_1, \dots, x_n) \in I^n \mapsto \phi_1(x_1) + \cdots + \phi_n(x_n) \in A.$$

The image $\phi(I^n)$ of ϕ is of course a left ideal in A, but it is in fact also a right ideal. Indeed, let $a \in A$. If $i \in \{1, \dots, n\}$, the function $\psi_i : x \in I \mapsto \phi_i(x)a \in A$ is a morphism of modules so, since $\mathscr{B}$ is a basis for $\hom(I, A)$, there exist scalars $\alpha_{i,1}, \dots, \alpha_{i,n} \in \Bbbk$ such that $\psi_j = \sum_{j=1}^n \alpha_{i,j}\phi_i$. It follows then that for each $x = (x_1, \dots, x_n) \in I^n$ we have that

$$\phi(x)a = \sum_{i=1}^n \phi_i(x_i)a = \sum_{i=1}^n \sum_{j=1}^n \alpha_{i,j}\phi_j(x_i) = \sum_{j=1}^n \phi_j\left(\sum_{i=1}^n \alpha_{i,j}x_i\right) \in \phi(I^n),$$

and this shows that $\phi(I^n)a \subseteq \phi(I^n)$.

We have $I \subseteq \phi(I^n)$, so that $\phi(I^n) \neq 0$. As we are supposing that A is a simple algebra, we must then have that $\phi(I^n) = A$, that is, that the map ϕ is surjective. In particular, there is an $x_0 \in I^n$ such that $\phi(x_0) = 1$ and we can define a morphism $\psi : a \in A \mapsto ax_0 \in I^n$. As $\phi\psi = \mathrm{id}_A$, the map ψ is injective and we see that A is isomorphic to a submodule of the semisimple module I^n. Corollary 2.2.5 tells us then that A itself is isomorphic to a direct sum I^m for some $m \leq n$ and, in particular, that it is a semisimple module. The algebra A is thus semisimple and from the module isomorphism $A \cong I^m$ we obtain algebra isomorphisms

$$A^{\mathsf{op}} \cong \mathsf{End}(A) \cong \mathsf{End}(I^m) \cong M_m(\mathsf{End}(I)),$$

so that $A \cong M_m(\mathsf{End}(I))^{\mathsf{op}} \cong M_m(\mathsf{End}(I)^{\mathsf{op}})$. Because of Corollary 2.1.3 and the fact that I is a simpl module, we know that $D = \mathsf{End}(I)$ is a division algebra. We thus see that $A \cong M_m(D^{\mathsf{op}})$. In particular, we have $\dim A = m^2 \dim D$. As $A \cong I^m$, we also have that $\dim A = m \dim I$, we find that $\dim I = m \dim D$.

Finally, if S is an arbitrary simple module and $s \in S \setminus 0$, the map $a \in A \mapsto as \in S$ is surjective and its kernel is the annihilator left ideal $\mathsf{ann}(s) = \{a \in A : as = 0\}$. There is therefore a short exact sequence

$$0 \longrightarrow \mathsf{ann}(s) \longrightarrow A \longrightarrow S \longrightarrow 0$$

and it splits in view of Corollary 2.2.6. It follows that S is isomorphic to a submodule of $A \cong I^m$. Corollary 2.2.5 and the fact that S is simple then imply that in fact $S \cong I$. This proves that all simple modules are isomorphic and completes the proof of the proposition. □

2.3.3. The following theorem, due to Joseph Wedderburn [Wed1908] and later generalized to artinian rings by Emil Artin [Art1927], is a central piece of modern algebra.

Theorem. *Let A be a finite dimensional algebra. The following statements are equivalent:*

(*a*) *A is semisimple.*

(*b*) *Every A-module is semisimple.*

(*c*) *There exist positive integers r and $n_1, \dots, n_r$ and finite-dimensional division algebras $D_1, \dots, D_r$ such that there is an algebra isomorpism $A \cong M_{n_1}(D_1) \times \cdots \times M_{n_r}(D_r)$.*

Proof. To be done □

2.3.4. The definition of semisimplicity for algebras involves only the structure of the algebra as a left module over itself, and we could of course develop a symmetric theory for right modules. The next result shows that this will not produce a new class of algebras.

Corollary. *An algebra is semisimple iff the right A-module A_A is a sum of simple right submodules.*

Proof. Indeed, the third statement of Theorem 2.3.3 is clearly symmetric. □

2.3.5. In the special case where the ground field is algebraically closed, we have a simpler description of semisimple algebras, which is a consequence of the following simple result.

Proposition. *If the ground field $\Bbbk$ is algebraically closed, then every finite-dimensional division algebra is isomorphic to $\Bbbk$ itself.*

Proof. Let D be finite-dimensional division algebra. Let $x \in D$, let $\phi : \Bbbk[X] \to D$ be the unique algebra morphism such $\phi(X) = x$ and let $p \in \Bbbk[X]$ be such that $\ker \phi = (p)$. If p were reducible, so that we had two non-constant polynomials $p_1, p_2 \in \Bbbk[X]$ with $p = p_1 p_2$, then we would have $0 = p(x) = p_1(x)p_2(x)$: this is impossible because $p_1(x)$ and $p_2(x)$ are both non-zero. It follows that p is reducible and the ideal $\ker \phi$ prime and, therefore, maximal. We thus see that the image $\Bbbk(x)$ of ϕ, being isomorphic to $\Bbbk[x]/\ker \phi$, is a field. It is, in fact, a finite extension of $\Bbbk$. As $\Bbbk$ is algebraically closed, this tells us that $\Bbbk(x) = \Bbbk$ and, in particular, that $x \in \Bbbk$. We conclude from this that $D = \Bbbk$. □

2.3.6. Corollary. *If the ground field $\Bbbk$ is algebraically closed, a finite-dimensional algebra is semisimple iff there exist positive integers $r, n_1, \dots, n_r$ with $A \cong M_{n_1}(\Bbbk) \times \cdots \times M_{n_r}(\Bbbk)$.*

Proof. Proposition 2.3.5 tells us that there are no non-trivial finite-dimensional division algebras, so the corollary follows at once from Theorem 2.3.3. □

2.3.7. A different direction in which we can specialize Theorem 2.3.3 is the following:

Proposition. *A finite-dimensional commutative algebra is semisimple iff it is a finite direct product of finite extensions of the group field.*

Proof. Indeed, we know from Theorem 2.3.3 that an algebra A is semisimple if it is a finite direct product of algebras of the form $M_n(D)$ with n a positive integer and D a finite-dimensional division algebra. Clearly, A will be commutative iff all the factors are commutative, and a matrix algebra $M_n(D)$ is commutative iff $n = 1$ and D is itself commutative. To complete the proof, we need only notice that a finite-dimensional commutative division algebra is the same thing as a finite extension of the ground field. □

2.3.8. Proposition. *Let A be an algebra. The following statements are equivalent:*

(*a*) *A is semisimple.*
(*b*) *Every short exact sequence of A-modules splits.*
(*c*) *Every A-module is projective.*
(*d*) *Every A-module is injective.*

Proof. To be done □

2.3.9. A module over a semisimple algebra is a direct sum of simple submodules. While the Krull-Remak-Schmidt Theorem 1.4.1 tells us that the isomorphism types of the summands is determined by the module, it is not true that the summands themselves are determined. There is a coarser direct sum decomposition available whose summands *are* well-determined and which is often useful:

Proposition. *Let A be a semisimple algebra, let $(S_1, \dots, S_r)$ be a complete system of repre-*

sentatives of the isomorphism classes of simple A-modules and for each $i \in \{1, \dots, r\}$ let $D_i = \mathsf{End}_A(S_i)$, so that S_i is an (A, D_i^{op})-bimodule in the usual way.

(*i*) *If M is an A-module, there exists a unique r-tuple $(M_1, \dots, M_n)$ of A-submodules of M such that $M = \bigoplus_{i=1}^{r} M_i$ and for each $i \in \{1, \dots, r\}$ there exists a non-negative integer m_i such that $M_i \cong S_i^{m_i}$.*

(*ii*) *For each $i \in \{1, \dots, n\}$ there is a unique linear map $\varepsilon_i : S_i \otimes_{D_i^{\mathsf{op}}} \mathsf{hom}_A(S_i, M) \to$ such that $\varepsilon_i(s \otimes f) = f(s)$ for all $s \in S_i$ and all $f \in \mathsf{hom}_A(S_i, M)$, this map is a morphism of A-modules, and its image is precisely the submodule M_i. The morphism*

$$\varepsilon = (\varepsilon_1, \dots, \varepsilon_n) : \bigoplus_{i=1}^{n} S_i \otimes_{D_i^{\mathsf{op}}} \mathsf{hom}_A(S_i, M) \to M$$

is an isomorphism of A-modules.

Proof. (*i*) Let $i \in \{1, \dots, r\}$ and consider the sum M_i of all sumodules of M which are isomorphic to S_i; it follows from Proposition 2.2.2 that $M_i \cong S_i^{m_i}$ for some non-negative integer m_i.

To be done □

§2.4. Three criteria for semisimplicity

von Neumann regular algebras

2.4.1. If A is an algebra, we say that an element $x \in A$ is ***von Neumann regular*** if there exists a $y \in A$ such that $xyx = x$, and we say that A itself is a ***von Neumann regular algebra*** if all of its elements are von Neumann regular. For brevity, we will say simply ***regular*** instead of von Neumann regular.

This condition on rings was introduced by John von Neumann in [vN1936] in the context of his work on algebras of operators.

2.4.2. Proposition.

(*i*) *A division algebra is regular.*

(*ii*) *If A is a regular algebra and $e \in A$ is an idempotent element, then eAe is a regular algebra.*

(*iii*) *If A and B are regular algebras, then the direct product $A \times B$ is a regular algebra.*

Proof. (*i*) Let A be a division algebra and let $x \in A$. If $y \in A$ is such that $yx = 1$, then $xyx = x1 = x$. We thus see that A is regular.

(*ii*) Let $x \in eAe$. As A is regular, there exists a $y \in A$ such that $xyx = x$. If we put $y' = eye$, which is an element of eAe, then we have $xy'x = x$ because $xe = x = ex$, and we see that x is regular also as an element of eAe.

(*iii*) Let $x = (a, b) \in A \times B$. Since A and B are regular, there exist $c \in A$ and $d \in B$ such that $aca = c$ and $bdb = b$, and it follows from this that the element $y = (c, d)$ satifies the equation $xyx = x$. The algebra $A \times B$ is therefore regular. $\square$

2.4.3. Proposition. *If A is a regular algebra and n is a positive integer, then the matrix algebra $M_n(A)$ is regular.*

Proof. We follow the argument given by Irving Kaplansky in his book [Kap1969, §II.2], starting with the following observation of McCoy:

> *x, y are elements of an algebra such that $xyx - x$ is a regular, then x is regular.*

Indeed, if z is such that $(xyx - x)z(xyx - x) = xyx - x$, then

$$x(y - z - yxzxy + yxz + zxy)x = x.$$

Next, we prove the following special case of the proposition:

$$\text{if } A \text{ is a regular algebra, then } M_2(A) \text{ is also regular.} \tag{11}$$

Let $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M_2(A)$. As A is regular, there exists an $r \in A$ such that $crc = c$, and then

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 & r \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} - \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} arc - a & ard - b \\ 0 & crd - d \end{pmatrix}$$

In view of McCoy's observation, it follows that to show that $M_2(A)$ regular it is enough to show that its elements of the form $\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$ are regular. The hypothesis on A implies that there are s, $t \in A$ such that $asa = a$ and $dtd = d$, and then

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} s & 0 \\ 0 & t \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} - \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 0 & axb - b \\ 0 & 0 \end{pmatrix},$$

and McCoy's observation again tells us that it is enough to show that the elements of $M_2(A)$ of the form $\left(\begin{smallmatrix} 0 & b \\ 0 & 0 \end{smallmatrix}\right)$ are regular. If now $u \in A$ is such that $bub = b$, we have

$$\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ u & 0 \end{pmatrix}\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}.$$

This proves the statement (11).

An obvious induction using the fact that for every algebra Λ and every positive integer m there is an isomorphism $M_2(M_m(\Lambda)) \cong M_{2m}(\Lambda)$ and the result (11) we have just proved establishes that

$$\text{if } A \text{ is a regular algebra and } m \text{ a positive integer, then } M_{2^m}(A) \text{ is a regular algebra.} \tag{12}$$

Finally, let us tackle the proposition in its full generality. Let n be a positive integer and let m be a positive integer such that $2^m \geq n$. The matrix

$$e = \begin{pmatrix} I_n & 0 \\ 0 & 0 \end{pmatrix}$$

with square diagonal blocks of size n and $2^m - n$, respectively, is an idempotent element of $M_{2^m}(A)$, and one can immediately check that $eM_{2^m}(A)e$ is isomorphic as an algebra to $M_n(A)$, so the second part of Proposition 2.4.2 and the claim (12) taken together imply that $M_n(A)$ is a regular algebra. □

2.4.4. Proposition. *An algebra is regular iff every left ideal is generated by an idempotent element.*

Proof. Let first A be a regular algebra and let I be a left ideal in A. To show that I is generated by an idempotent element it will be enough that we show that this is true if I is either of the form Ax or of the form $Ax_1 + Ax_2$, for I is finitely generated and we can use this two cases to prove the general case by induction.

If there is an $x \in A$ such that $I = Ax$ and $y \in A$ is such that $xyx = x$, then the element $e = yx$ is idempotent, we have $x = xyx \in Ae$ and $e \in Ax$, so that $I = Ae$.

Suppose now instead there are $x_1, x_2 \in A$ such that $I = Ax_1 + Ax_2$. By what we have shown already, we know that there exists an idempotent element $e_1 \in A$ such that $Ax_1 = Ae_1$. We have

$$Ax_2 = Ax_2 1 = Ax_2(e_1 + (1 - e_1)) \subseteq Ax_2e_1 + Ax_2(1 - e_1)$$

and $Ax_2(1 - e_1) \subseteq Ax_2 + Ax_2e_1 \subseteq Ae_1 + Ax_2 = I$, so that

$$I = Ae_1 + Ax_2 \subseteq Ae_1 + Ax_2e_1 + Ax_2(1 - e_1) = Ae_1 + Ax_2(1 - e_1) \subseteq I.$$

Thus $I = Ae_1 + Ax_2(1 - e_1)$. As before, we know there is an idempotent element $e_2 \in A$ such that $Ax_2(1 - e_1) = Ae_2$. Since $Ae_2e_1 = Ax_2(1 - e_1)e_1 = 0$, we have $e_2e_1 = 0$. Let now $e_3 = (1 - e_1)e_2$. Computing, we see that e_3 is idempotent, $e_1e_3 = e_3e_1 = 0$. Also, we have $Ae_3 = A(1 - e_1)e_2 \subseteq Ae_2$ and

$$Ae_2 = Ae_2e_2 = Ax_2(1 - e_1)e_2 = Ax_2e_3 \subseteq Ae_3,$$

so that in fact $Ae_2 = Ae_3$. It follows that $I = Ae_1 + Ae_3$. If we now let $e = e_1 + e_3$, then e is also idempotent and $I = Ae$. This completes the proof of the necessity of the condition.

Conversely, suppose that every left ideal is generated by an idempotent element and let $x \in A$. If $e \in A$ is an idempotent such that $Ax = Ae$, then there exist $y, z \in A$ such that $x = ze$ and $e = yx$ and we have that $xyx = zee = ze = x$. The algebra A is thus regular. □

2.4.5. Proposition. *A finite dimensional algebra is semisimple iff it is regular.*

Proof. Let A be a algebra. If I is a left ideal, then Proposition 2.4.4 tells us that there exists an idempotent element $e \in A$ such that $I = Ae$. If we put $J = A(1-e)$, it is easy to see that $A = I \oplus J$, and this means that I is a direct summand of A. In view of Proposition 2.2.4, it follows from this that A is a semisimple algebra.

Conversely, if A is semisimple then we know from Theorem 2.3.3 that it is isomorphic to a finite direct product of matrix algebras over division algebras, and then A is regular because of the results of Propositions 2.4.2 and 2.4.3. □

The trace form

2.4.6. If A is an algebra, there is an algebra homomorphism $\lambda : A \to \mathsf{End}_{\Bbbk}(A)$ such that $\lambda(a)(b) = ab$ for all $a, b \in A$. Since A is finite-dimensional, we obtain a bilinear mapping $(-,-) : A \times A \to \Bbbk$ setting for all $a, b \in A$

$$(a, b) = \operatorname{tr} \lambda(ab).$$

We call $(-,-)$ the ***trace form*** of A.

2.4.7. Lemma. *The trace form $(-,-) : A \times A \to \Bbbk$ of an algebra A is symmetric and associative, so that*

$$(a, b) = (b, a), \qquad\qquad (ab, c) = (a, bc)$$

for all a, b, $c \in A$.

Proof. Let a, b and c be elements of A. We have

$$\operatorname{tr} \lambda(ab) = \operatorname{tr} \lambda(a) \circ \lambda(b) = \operatorname{tr} \lambda(b) \circ \lambda(a) = \operatorname{tr} \lambda(ab)$$

because of the cyclic property of the trace, so that $(a, b) = (b, a)$. On the other hand, that $(ab, c) = (a, bc)$ follows immediately from the associativity of A. □

2.4.8. Lemma. *Let A be an algebra. If I is a bilateral ideal in A, then the orthogonal complement $I^\perp$ of I with respect to the trace form is also a bilateral ideal.*

Proof. If $a \in A$ and $y \in I^\perp$, we have

$$(x, ay) = (xa, y) = 0$$

and

$$(x, ya) = (ya, x) = (y, ax) = (ax, y) = 0$$

for all $x \in I$, so that $ay, ya \in I^\perp$. □

2.4.9. Theorem. *Let A be an algebra. If the trace form of A is non-degenerate, then A is semisimple.*

Proof. If the algebra A is simple, then Proposition 2.3.2 tells us that it is semisimple. We may then suppose that A is not simple. In particular, there is then a minimal non-zero bilateral ideal I in A. From Lemma 2.4.8 we know that $I^\perp$ is also a bilateral ideal and, since we are assuming that the trace form is non-degenerate, we have that $A = I \oplus I^\perp$. In particular, there are elements $e \in I$ and $f \in I^\perp$ such that $1 = e + f$. It is easy to check that, with respect to the multiplication of A, both I and $I^\perp$ are unitary associative algebras —whose unit elements are e and f, respectively. As I is a minimal ideal of A, it is a simple algebra and it is, again by Proposition 2.3.2, semisimple. On the other hand, the trace form of the algebra $I^\perp$ is the restriction of the trace form of A and it is non-degenerate. As $\dim I^\perp < \dim A$, by induction we may assume that $I^\perp$ is a semisimple algebra, and then A, which is isomorphic as an algebra to the dirct product of I and $I^\perp$, is also semisimple. □

2.4.10. The converse of Theorem 2.4.9 is not true without extra conditions. To see this we start with a lemma from linear algebra.

Lemma. *Suppose that the characteristic of the ground field $\Bbbk$ is zero. Let V be a finite-dimensional vector space and let $f : V \to V$ be a linear map. If $\operatorname{tr} f^n = 0$ for all $n \geq 1$, then the map f is nilpotent.*

Proof. Let K be an extension field of $\Bbbk$ such that the characteristic polynomial $\chi_f \in \Bbbk[X]$ of f factors in $K[X]$ as a product of linear factors, let $\lambda_1, \dots, \lambda_s$ be the distinct non-zero roots of that polynomial in K and let $m_1, \dots, m_s$ be their respective multiplicities, which are *positive* integers. We want to show that $s = 0$ or, in other words, that the characteristic polynomial has no non-zero roots, as this implies that $\chi_f = X^{\dim V}$ and, in view of the Cayley-Hamilton theorem, that f is nilpotent.

For each $i \in \{1, \dots, s\}$ we have that

$$0 = \operatorname{tr} f^n = \sum_{i=1}^{s} \lambda_i^n k_i.$$

If we view these s equalities as a homogeneous system of linear equations for the integers $k_1, \dots, k_s$, the matrix of coefficients is the Vandermonde matrix for the scalars $\lambda_1, \dots, \lambda_s$, which has non-zero determinant. It follows that, as elements of K, we have $k_1 = \cdots = k_s = 0$. As the characteristic of $\Bbbk$ is zero, this is only possible if we have $s = 0$, as we wanted. □

2.4.11. We can now prove a partial converse to Theorem 2.4.9:

Proposition. *If A is semisimple algebra and the characteristic of the ground field $\Bbbk$ is zero, then the trace form of A is non-degenerate.*

Proof. We have to show that the orthogonal complement $A^\perp$ is zero, so we fix $x \in A^\perp$ and prove that $x = 0$.

As $x \in A^\perp$, for all $n \geq 0$ we have $0 = (x, x^n) = \operatorname{tr} \lambda(x^{n+1}) = \operatorname{tr} \lambda(x)^{n+1}$. It follows from this and Lemma 2.4.10 that $\lambda(x)$ is a nilpotent endomorphism of A, and this implies in turn that x is a nilpotent element of A. Let k be a positive integer such $x^k = 0$.

Suppose that $S \subseteq A$ is a simple submodule. We cannot have $xS = S$ —for then by iteration we would have that $0 = x^k S = S$, which is absurd— so we must have $xS = 0$. Now, as A is semisimple, there exists a family $\mathscr{S}$ of simple submodules of A such that $A = \sum_{S \in \mathscr{S}} S$, and then $x \in xA = \sum_{S \in S} xS = 0$. □

Specialization

2.4.12. Let $f : \mathcal{O} \to F$ be a morphism of commutative rings. As we can view F as a right $\mathcal{O}$-module, for each $\mathcal{O}$-module V we can construct a F-module $V_F = F \otimes_{\mathcal{O}} V$, which we say is obtained from V by ***extending scalars*** along the morphism f, and the function $f_V : v \in V \to 1 \otimes v \in V_F$, which is a morphism of $\mathcal{O}$-modules. If V is $\mathcal{O}$-free, then V_F is F-free and, in fact, if $\mathscr{B}$ is an $\mathcal{O}$-basis for V then the restriction of f_V to $\mathscr{B}$ is injective and the image $f_V(\mathscr{B})$ is an F-basis for V_F; in particular, we have in this case that $\operatorname{rank}_F V_F = \operatorname{rank}_{\mathcal{O}} V$.

Similarly, we can extend scalars on morphisms: if $\phi : V \to W$ is a morphism of $\mathcal{O}$-modules, we say that the morphism $f_*(\phi) = \mathrm{id}_F \otimes \phi : V_F \to_F$ of F-modules is obtained from ϕ by changing scalars along f.

2.4.13. If $\mathcal{O}$ is a commutative ring and V is a free $\mathcal{O}$-module of finite rank, there is a trace function $\operatorname{tr}_{V/\mathcal{O}} : \operatorname{End}_{\mathcal{O}}(V) \to \mathcal{O}$. This function is compatible with extension of scalars:

Lemma. *Let $f : \mathcal{O} \to F$ be a morphism of commutative rings. If V is a free $\mathcal{O}$-module of finite rank, then the following diagram commutes*

$$\begin{array}{ccc} \operatorname{End}_{\mathcal{O}}(V) & \xrightarrow{\operatorname{tr}_{V/\mathcal{O}}} & \mathcal{O} \\ {\scriptstyle f_*}\downarrow & & \downarrow{\scriptstyle f} \\ \operatorname{End}_F(V_F) & \xrightarrow{\operatorname{tr}_{V_F/F}} & F \end{array}$$

We emphasize that this statement makes sense since, as we observed in 2.4.12, the hypothesis on V implies that the F-module V_F is free of finite rank, so that the function $\operatorname{tr}_{V_F/F}$ is defined.

Proof. To be done □

2.4.14. If $f : \mathcal{O} \to F$ is a morphism of commutative rings and A is an $\mathcal{O}$-algebra, then the F-module A_F is an F-algebra with multiplication uniquely determined by the condition that $x \otimes a \cdot y \otimes b = xy \otimes ab$ for all $x, y \in F$ and all $a, b \in A$. In this situation, the morphism $f_A : A \to A_F$ of $\mathcal{O}$-modules defined in 2.4.12 is a morphism of $\mathcal{O}$-algebras.

2.4.15. Let A is an $\mathcal{O}$-algebra which as an $\mathcal{O}$-module is free of finite rank. Just as in 2.4.6, we have a morphism $\lambda : A \to \mathsf{End}_{\mathcal{O}}(A)$ of $\mathcal{O}$-algebras such that $\lambda(a)(b) = ab$ and an $\mathcal{O}$-bilinear map $(-,-) : A \times A \to \mathcal{O}$, the trace form of A, such that $(a,b) = \mathsf{tr}\,\lambda(ab)$ for all $a, b \in A$. If $\mathscr{B} = \{a_1, \dots, a_n\}$ is an ordered $\mathcal{O}$-basis for A, the ***discriminant*** of A with respect to the basis $\mathscr{B}$ is the determinant

$$\mathsf{Disc}(A, \mathscr{B}) = \det((a_i, a_j))_{1 \le i,j \le n} \in \mathcal{O}.$$

2.4.16. Proposition. *Let $f : \mathcal{O} \to F$ be a morphism of commutative rings and let A be an $\mathcal{O}$-algebra which as an $\mathcal{O}$-module is free of finite rank. If $\mathscr{B}$ is an ordered $\mathcal{O}$-basis for A, then the restriction of $f_A : A \to A_F$ to $\mathscr{B}$ is injective, the set $f_A(\mathscr{B})$ is an F-basis for A_F and we have that $f(\mathsf{Disc}(A, \mathscr{B})) = D(A_F, f_A(\mathscr{B}))$.*

Proof. To be done $\square$

2.4.17. Corollary. *Let $\mathcal{O}$ be a commutative ring, let A be an $\mathcal{O}$-algebra which as an $\mathcal{O}$-module is free of finite rank, and let $\mathscr{B}$ be an ordered $\mathcal{O}$-basis for A. If $\mathfrak{p}$ is a prime ideal in $\mathcal{O}$ such that $\mathsf{Disc}(A, \mathscr{B}) \notin \mathfrak{p}$ and we let $F = \mathsf{Frac}\,\mathcal{O}/\mathfrak{p}$ and $f : \mathcal{O} \to F$ be the natural map, then the F-algebra A_F is semisimple.*

Proof. To be done $\square$

2.4.18. Corollary. *Let $\mathcal{O}$ be a commutative ring and let A be an $\mathcal{O}$-algebra which as an $\mathcal{O}$-module is free of finite rank. If there exists a morphism $f : \mathcal{O} \to F$ of rings with codomain a field of characteristic zero such that the F-algebra A_F is semisimple, then for every $\mathcal{O}$-basis $\mathscr{B}$ for A we have $D(A, \mathscr{B}) \neq 0$.*

Proof. To be done $\square$

2.4.19. It follows at once from Corollaries 2.4.17 and 2.4.18 that under the hypothesis of the latter we have, for each prime ideal $\mathfrak{p}$ of $\mathcal{O}$ which does not contain $D(A, \mathscr{B})$ and $f : \mathcal{O} \to K = \mathsf{Frac}\,\mathcal{O}/\mathfrak{p}$ the natural map, that the algebra A_K is semisimple. In particular, if $\mathcal{O}$ is an integral domain we can take here $\mathfrak{p} = 0$, so that $K = \mathsf{Frac}\,\mathcal{O}$ is just the field of fractions of $\mathcal{O}$.

2.4.20. Let us present an application of these results. We let q be a variable, let $\Bbbk$ be a field of characteristic zero, let A be a $\Bbbk[q]$-algebra which as a $\Bbbk[q]$-module is free of finite rank n and let $\mathscr{B} = \{a_1, \dots, a_n\}$ be a $\Bbbk[q]$-basis for A. There are then polynomials $c^k_{i,j} \in \Bbbk[q]$ for each i, j, $k \in \{1, \dots, n\}$ sch that $a_i a_j = \sum_{k=1}^n c^k_{i,j} a_k$.

For each $\varepsilon \in \Bbbk$ there is a unique morphism of $\Bbbk$-algebras $\mathsf{ev}_\varepsilon : \Bbbk[q] \to \Bbbk$ such that $\mathsf{ev}_\varepsilon(q) = \varepsilon$; if $h \in \Bbbk[q]$, then $\mathsf{ev}_\varepsilon(h)$ is simply the evaluation $h(\varepsilon)$ of the polynomial h at ε and it follows from this that $\ker \mathsf{ev}_\varepsilon$ is the ideal $(q - \varepsilon)$. We let A_ε be the algebra obtained from A by extending scalars along ev_ε. As a $\Bbbk$-vector space it is $\Bbbk \otimes_{\Bbbk[q]} A$, with $\Bbbk$ viewed as a $\Bbbk[q]$-module through ev_ε. If for each $i \in \{1, \dots, n\}$ we write $a^\varepsilon_i = 1 \otimes a_i \in A_\varepsilon$, then the set $\mathscr{B}_\varepsilon = \{a^\varepsilon_1, \dots, a^\varepsilon_n\}$ is a $\Bbbk$-basis for A_ε and the multiplication in A_ε is such that for all $i, j \in \{1, \dots, n\}$ we have

$$a_i^\varepsilon a_j^\varepsilon = \sum_{k=1}^{n} c_{i,j}^k(\varepsilon)\, a_k^\varepsilon. \tag{13}$$

Suppose now that there exists an $\varepsilon_0 \in \Bbbk$ such that the algebra A_{ε_0} is semisimple. It follows from Corollary 2.4.18 that $\delta = \mathsf{Disc}(A, \mathscr{B})$ is a non-zero element of $\Bbbk[q]$. As such, we know that there exist a finite set $E \subseteq \Bbbk$ such that $\mathsf{ev}_\varepsilon(\delta) = \delta(\varepsilon) \neq 0$ if $\varepsilon \in \Bbbk \setminus E$ and, therefore, $\delta \notin \ker \mathsf{ev}_\varepsilon$. If $\varepsilon \in \Bbbk \setminus E$ we have $\mathsf{Frac}\, \Bbbk[q] / \ker \mathsf{ev}_\varepsilon \cong \Bbbk$ and the natural map $\Bbbk[q] \to \mathsf{Frac}\, \Bbbk[q] / \ker \mathsf{ev}_\varepsilon$ corresponds under this isomorphism precisely to the evaluation map ev_ε. We can therefore conclude from Corollary 2.4.17 that the algebra A_ε is semisimple for all $\varepsilon \in \Bbbk \setminus E$.

We can view the $\Bbbk[q]$-algebra A as a providing a family of $\Bbbk$-algebras $\mathscr{A} = (A_\varepsilon)_{\varepsilon \in \Bbbk}$. That A be a $\Bbbk[q]$-algebra then tells us that the algebras in this family $\mathscr{A}$ «depend polynomially on the parameter ε», as reflected by the fact exhibited in equation (13) that the structure coefficients of the algebras in the family are obtained by evaluating certain fixed polynomials. Our observations can therefore be stated as follows:

> *if one of the algebras in a polynomial family of algebras is semisimple, then almost of them —that is, all of them except at most a finite number— are in fact semisimple.*

We will use this in a concrete non-trivial situation in Section 3.8 in Chapter 3.

§2.5. Exercises

2.5.1. If A is an algebra and M is a semisimple module, the algebra $\mathsf{End}_A(M)$ is semisimple.

2.5.2. An algebra is semisimple if it has a faithful semisimple module.

2.5.3. Prove the following famous theorem of William Burnside [Bur1905]:

> *If $\Bbbk$ is an algebraically closed field, V a finite-dimensional vector space and $A \subseteq \mathsf{End}_\Bbbk(V)$ a subalgebra such that V has no proper non-zero subspace which is invariant under all elements of A, then in fact $A = \mathsf{End}_\Bbbk(V)$.*

See [Lam1998] for a modern exposition of this result in terms of linear algebra.

2.5.4. Let V be a finite-dimensional $\mathbb{C}$-vector space endowed with an inner product $\langle -, - \rangle$ and for each $a \in \mathsf{End}_\mathbb{C}(V)$ let $a^* \in \mathsf{End}_\mathbb{C}(V)$ be the map adjoint to a, so that $\langle a(x), y \rangle = \langle x, a^*(y) \rangle$ for all x, $y \in V$. We say that a subalgebra $A \subseteq \mathsf{End}_\mathbb{C}(V)$ is ***-closed*** if $a^* \in A$ whenever $a \in A$. If that is the case, then A is semisimple.

2.5.5. (*i*) Let A be a simple algebra and let V be a finite-dimensional vector space. If ϕ, $\psi : A \to \mathsf{End}_{\Bbbk}(V)$ are algebra morphisms, then there exists an isomorphism $u : V \to V$ of vector spaces such that $\phi(a) = u^{-1}\psi(a)u$ for all $a \in A$.

(*ii*) Every algebra automorphism of $M_n(\Bbbk)$ is inner.

CHAPTER 3

Group algebras

§3.1. Representation of groups

3.1.1. If G is a group, the ***group algebra*** of G is the algebra $\Bbbk G$ which as a vector space has the set underlying G as a basis and whose multiplication $\mu : \Bbbk G \times \Bbbk G \to \Bbbk G$ is the unique bilinear function such that $\mu(g, h) = gh$ for each g, $h \in G$. It is easy to see that the unit element 1 of G is the unit element of $\Bbbk G$ and it is obvious that $\Bbbk G$ is finite-dimensional iff G is finite.

3.1.2. Proposition.

(*i*) *If G and H are groups and $f : G \to H$ is a morphism of groups, then there is exactly one linear map $\bar{f} : \Bbbk G \to \Bbbk H$ such that $\bar{f}(g) = f(g)$ for all $g \in G$, and it is a morphism of algebras.*

(*ii*) *There is a functor $F : \mathsf{Grp} \to \mathsf{Alg}$ from the category of groups to that of algebras such that for each group G we have $F(G) = \Bbbk G$ and for each morphism of groups $f : G \to H$ we have $F(f) = \bar{f} : \Bbbk G \to \Bbbk H$*

Proof. (*i*) Let G, H and f be as in the statement. Since G is a basis of the vector space $\Bbbk G$, we know that there exists a linear map $\bar{f} : \Bbbk G \to \Bbbk H$ such that $\bar{f}(g) = f(g)$ for each $g \in G$ and that there is exactly one such map. Since G is a basis of its domain, to check that $\bar{f}$ is a morphism of algebras it is enough to verify that $\bar{f}(gh) = \bar{f}(g)\bar{f}(h)$ for all $g, h \in G$, and that is clear in view of the fact that f is a morphism of groups.

(*ii*) We need to check that whenever G is a group we have $\overline{\mathrm{id}_G} = \mathrm{id}_{\Bbbk G}$ and that for each pair $f : G \to H$ and $g : H \to K$ of composable morphisms of groups we have $\overline{g \circ f} = \overline{g} \circ \overline{f}$, and both points are clear. □

3.1.3. If A is an algebra, we let $A^\times$ be its group of unit. If $f : A \to B$ is a morphism of algebras, then $f(A^\times) \subseteq B^\times$ and the restriction $f^\times = f|_{A^\times} : A^\times \to B^\times$ is a morphism of groups. In this way we obtain a functor $(-)^\times : \mathsf{Alg} \to \mathsf{Grp}$, as one easily check.

3.1.4. The next proposition exhibits the characteristic property of the group algebra of a group, which is behind our interest in it.

Proposition. *Let G be a group, let $\Bbbk G$ be its group algebra and let A be an algebra.*

(*i*) *If* $f : \Bbbk G \to A$ *is a morphism of algebras, then* $f(G) \subseteq A^\times$ *and the restriction* $f|_G : G \to A^\times$ *is a morphism of groups.*

(*ii*) *The function*

$$\Phi_{G,A} : f \in \mathsf{hom}_{\mathsf{Alg}}(\Bbbk G, A) \mapsto f|_G \in \mathsf{hom}_{\mathsf{Grp}}(G, A^\times).$$

that we obtain in this way is a natural bijection, so that the functor $\mathsf{Grp} \to \mathsf{Alg}$ *of Proposition 3.1.2 is a left adjoint to the functor* $(-)^\times : \mathsf{Alg} \to \mathsf{Grp}$ *of 3.1.3.*

Proof. The claims of part (*i*) follow at once from our observations of 3.1.3 and the obvious fact that $G \subseteq (\Bbbk G)^\times$. That the function $\Phi_{G,A}$ depends naturally on both G and A is also clear, so we need only show that that function is bijective. We do so by constructing an inverse.

Suppose that $f : G \to A^\times$ is a morphism of groups. Since G is a basis of the vector space $\Bbbk G$ and $A^\times \subseteq A$, there is a unique linear map $\bar{f} : \Bbbk G \to A$ such that $\bar{f}(g) = f(g)$ for all $g \in G$. This map $\bar{f}$ is a morphism of algebras: indeed, if $g, h \in G$ we have

$$\bar{f}(gh) = f(gh) = f(g)f(h) = \bar{f}(g)\bar{f}(h)$$

because f is a morphism of groups, and the claim follows from this since G is a basis of $\Bbbk G$. We can therefore define a function

$$\Psi_{G,A} : f \in \mathsf{hom}_{\mathsf{Grp}}(G, A^\times) \mapsto \bar{f} \in \mathsf{hom}_{\mathsf{Alg}}(\Bbbk G, A),$$

which turns out to be the desired inverse for $\Phi_{G,A}$. □

3.1.5. If G is a group, a ***representation*** of G is a pair (V, ρ) with V a vector space and $\rho : G \to \mathsf{GL}(V)$ a morphism of groups. The ***trivial representation*** of G is the representation $(\Bbbk, \rho)$ with $\rho : G \to \mathsf{GL}(V)$ the trivial morphism.

If (V, ρ) and (V', ρ') are representations of G, then a ***morphism*** of representations $f : (V, \rho) \to (V', \rho')$ is a linear function $f : V \to V'$ such that $f \circ \rho(g) = \rho'(g) \circ f$ for all $g \in G$. It is easy to check that the representations of G and the morphisms thereof are the objects and morphisms of a category, which we denote ${}_G\mathsf{Rep}$. We say that a representation (V, ρ) is finite-dimensional if the vector space is finite-dimensional, and we write ${}_G\mathsf{rep}$ the full subcategory of ${}_G\mathsf{Rep}$ spanned by the finite-dimensional representations. We will almost always write a representation (V, ρ) simply as V, and if we need to mention the morphism ρ we will write it ρ_V.

3.1.6. Proposition. *Let* G *be a group. If* V *is a vector space, the group of units of* $\mathsf{End}_\Bbbk(V)$ *is* $\mathsf{GL}(V)$, *and we write* Φ_V *the bijection* $\Phi_{G,\mathsf{End}_\Bbbk(V)}$ *constructed in Proposition 3.1.4.*

(*i*) *If* (V, ϕ) *is a* $\Bbbk G$*-module, then* $(V, \Phi_V(\phi))$ *is a representation of* G.

(*ii*) *If* $f : (V, \phi) \to (V', \phi')$ *is a morphism of* $\Bbbk G$*-modules, then the linear map* $f : V \to V'$ *is also a morphism* $(V, \Phi_V(\phi)) \to (V', \Phi_{V'}(\phi'))$ *of representations of* G.

(*iii*) *There is a functor* $F : {}_{\Bbbk G}\mathsf{Mod} \to {}_G\mathsf{Rep}$ *such that*

- *for each* $\Bbbk G$*-module* (V,ϕ) *we have* $F(V,\phi) = (V, \Phi_V(\phi))$*, and*
- *for each morphism* $f : (V,\phi) \to (V',\phi')$ *of* $\Bbbk G$*-modules, the morphism*

$$F(f) : F(V, \Phi_V(\phi)) \to (V', \Phi_{V'}(\phi'))$$

  is the linear map f*.*

This functor is an isomorphism *of categories and, moreover, it restricts to an isomorphism* ${}_{\Bbbk G}\mathsf{mod} \to {}_G\mathsf{rep}$ *of the subcategories of finite dimensional modules and representations.*

In view of this result, we may identify the concepts of representation of a group and of module over the group algebra of that group. We will switch from one description to the other implicitly whenever this is convenient.

Proof. Since Φ_V is a function $\mathsf{hom}_{\mathsf{Alg}}(\Bbbk G, \mathsf{End}_{\Bbbk}(V)) \to \mathsf{hom}_{\mathsf{Grp}}(G, \mathsf{GL}(V))$, the claim of part (*i*) is clear. If f is as in part (*ii*), so that $f \circ \phi(x) = \phi'(x) \circ f$ for all $x \in \Bbbk G$, we have

$$f \circ \Phi_V(\phi)(g) = f \circ \phi(g) = \phi'(g) \circ f = \Phi_{V'}(\phi')(g) \circ f$$

for each $g \in G$, and this means that $f : (V, \Phi_V(\phi)) \to (V', \Phi_{V'}(\phi'))$ is a morphism of representations of G, as stated. To prove part (*iii*) we have to check that F is indeed a functor, which is immediate, and to construct an inverse $K : {}_G\mathsf{Rep} \to {}_{\Bbbk G}\mathsf{Mod}$. If (V,ρ) is a representation of G, then $\Phi_V^{-1}(\rho) : \Bbbk G \to \mathsf{End}_{\Bbbk}(V)$ is a morphism of algebras, and we may put $K(V,\rho) = (V, \Phi_V^{-1})(\rho)$. On the other hand, if $f : (V,\rho) \to (V',\rho')$ is morphism of representations of G, then it is easy to check, much as before, that the linear map $f : V \to V'$ is also a morphism of $\Bbbk G$-modules $(V, \Phi_V^{-1}(\rho)) \to (V', \Phi_{V'}^{-1}(\rho'))$, so we may put $K(f) = f$. We are left with the verification that this does in fact define a functor K, that the compositions $K \circ F$ and $F \circ K$ are the identity functors of ${}_{\Bbbk G}\mathsf{Mod}$ and of ${}_G\mathsf{Rep}$, respectively, and that $F({}_{\Bbbk G}\mathsf{mod}) = {}_G\mathsf{rep}$, which is trivial. □

3.1.7. If G is a group, we write $\mathsf{cl}(g)$ the conjugacy class of an element $g \in G$, $\mathsf{cl}(G)$ the set of conjugacy classes of G and $\mathsf{cl}_f(G)$ the subset of $\mathsf{cl}(G)$ consisting of the finite conjugacy classes; of course, if G is finite we have $\mathsf{cl}_f(G) = \mathsf{cl}(G)$. If $c \in \mathsf{cl}_f(G)$ we consider the element $z_c = \sum_{g \in c} g \in \Bbbk G$.

Lemma. *Let* G *be a group. The set* $\{z_c : c \in \mathsf{cl}_f(G)\}$ *is a basis for the center* $\mathsf{Z}(\Bbbk G)$ *of the group algebra* $\Bbbk G$*.*

Proof. Let $x = \sum_{g \in G} x_g g$ be an element of $\Bbbk G$, with $x_g \in \Bbbk$ for each $g \in G$ and $x_g = 0$ for almost all $g \in G$. Since G generates the algebra $\Bbbk G$ as a vector space we have that $x \in \mathsf{Z}(\Bbbk G)$ iff $hx = xh$ for all $h \in G$ or, equivalently, if $hxh^{-1} = x$ for all $h \in G$.

If $h \in G$, then $hxh^{-1} = \sum_{g \in G} x_g hgh^{-1} = \sum_{g \in G} x_{h^{-1}gh} g$, so we have that $x \in \mathsf{Z}(\Bbbk G)$ iff $x_g = x_{h^{-1}gh}$ for all $g, h \in G$, and this happens iff the function $g \in G \mapsto x_g \in \Bbbk$ is constant on conjugacy classes, that is, if there exists a function $\xi : \mathsf{cl}(G) \to \Bbbk$ such that $x_g = \xi(\mathsf{cl}(g))$ for each $g \in G$. In particular, this makes it clear that $z_c \in \mathsf{Z}(\Bbbk G)$ for each conjugacy class $c \in \mathsf{cl}_f(G)$.

Suppose that $x = \sum_{g\in G} x_g g$, with the scalars x_g as above, is in $\mathsf{Z}(\Bbbk G)$, so that there exist such a function $\xi : \mathsf{cl}(G) \to \Bbbk$ such that $x_g = \xi(\mathsf{cl}(g))$ for all $g \in G$. If $c \in \mathsf{cl}(G)$ is an infinite conjugacy class, then $\xi(c) = 0$, for otherwise we would have $x_g = \xi(c) \neq 0$ for all the infinitely many elements $g \in c$, which is absurd. It follows then immediately that we have $x = \sum_{c\in\mathsf{cl}_f(G)} \xi(c) z_c$. We can therefore conclude that the set $\{z_c : c \in \mathsf{cl}_f(G)\}$ spans the center $\mathsf{Z}(\Bbbk G)$ and, as it is clearly linearly independent, it is a basis. □

§3.2. Semisimple group algebras

3.2.1. The following important result of Heinrich Maschke [Mas1899, Mas1898] shows that groups provide interesting examples of semisimple algebras.

Theorem. *If G is a finite group whose order is not divisible by the characteristic of the ground field $\Bbbk$, then the group algebra $\Bbbk G$ is semisimple.*

Proof. Let M be a $\Bbbk G$-module. We will prove that M is semisimple using the characterization of semisimplicity provided by Proposition 2.2.4. Let $N \subseteq M$ be a $\Bbbk G$-submodule and let $i : N \to M$ be the inclusion map, which is a morphism of modules. There exists a linear map $r : M \to N$ such that $ir = \mathrm{id}_N$ and, since G is finite and $|G|$ is an invertible element of $\Bbbk$, we may consider the linear map $\bar{r} : M \to N$ such that

$$\bar{r}(m) = \frac{1}{|G|}\sum_{g\in G} gr(g^{-1}m)$$

for each $m \in M$. This map is a morphism of $\Bbbk G$-modules: indeed, if $h \in G$ we have

$$\bar{r}(hm) = \frac{1}{|G|}\sum_{g\in G} gr(g^{-1}hm) = \frac{1}{|G|}\sum_{k\in G} hkr(k^{-1}m) = h\bar{r}(m),$$

and this is enough to show that $\bar{r}$ is $\Bbbk G$-linear, as G spans $\Bbbk G$ as a vector space. On the other hand, if $n \in N$ we have

$$\bar{r}i(n) = \frac{1}{|G|}\sum_{g\in G} gr(g^{-1}i(n)) = \frac{1}{|G|}\sum_{g\in G} gri(g^{-1}n) = \frac{1}{|G|}\sum_{g\in G} gg^{-1}n = n$$

since the map i is $\Bbbk G$-linear and $ri = \mathrm{id}_N$. It follows from this that we have a direct sum decomposition $M = N \oplus \ker \bar{r}$ of M as a direct sum of $\Bbbk G$-modules and, in particular, that N is a direct summand of M. □

3.2.2. From Theorem 2.3.3 we can extract significant information about the modules of a semisimple group algebra.

Proposition. *Let G be a finite group whose order is not divisible by the characteristic of the ground field $\Bbbk$, so that the group algebra $\Bbbk G$ is semisimple. There exists a finite set $\{S_1, \dots, S_r\}$ which is a complete system of representatives for the isomorphism classes of simple $\Bbbk G$-modules. There are positive integers $n_1, \dots, n_r$ such that there is an isomorphism of modules*

$$\Bbbk G \cong S_1^{n_1} \oplus \cdots \oplus S_r^{n_r}$$

and, if we let $D_i = \mathsf{End}_{\Bbbk G}(S_i)$ for each $i \in \{1, \dots, r\}$, an isomorphism of algebras

$$\Bbbk G \cong M_{n_1}(D_1^{\mathsf{op}}) \times \cdots \times M_{n_r}(D_r^{\mathsf{op}}). \tag{14}$$

Moreover, we have that:

(*i*) $|G| = \sum_{i=1}^{r} n_i^2 \dim D_i$;

(*ii*) $r \leq |\mathsf{cl}(G)|$ *and if $\Bbbk$ is algebraically closed we in fact the equality holds;*

(*iii*) *for each $i \in \{1, \dots, r\}$ we have $n_i \dim D_i = \dim S_i$;*

(*iv*) *if $\Bbbk$ is algebraically closed, then for each $i \in \{1, \dots, r\}$ we have $n_i = \dim S_i$.*

Proof. We have to prove (*i*)–(*iii*), as the rest follows at once from Theorem 2.3.3. The equality in (*i*) can be obtained simply by computing dimensions over $\Bbbk$ on both sides of the isomorphism (14), the statement (*iii*) follows directly from the last claim of Proposition 2.3.2 and the statement (*iv*) is a consequence of (*iii*) and the fact that when $\Bbbk$ is algebraically closed every finite-dimensional division algebras is one-dimensional, which is the content of Proposition 2.3.5.

For every algebra Λ we have that $\mathsf{Z}(\Lambda^{\mathsf{op}}) = \mathsf{Z}(\Lambda)$ and, if n is a positive integer, that $\mathsf{Z}(M_n(\Lambda)) \cong \mathsf{Z}(\Lambda)$, so the center of the algebra appearing on the right hand side of (14) is isomorphic to $\mathsf{Z}(D_1) \times \cdots \times \mathsf{Z}(D_r)$ and therefore it has dimension equal to $\sum_{i=1}^{r} \dim \mathsf{Z}(D_i)$. On the other hand, it follows from lemma 3.1.7 that $\dim \mathsf{Z}(\Bbbk G) = |\mathsf{cl}(G)|$, so from the isomorphism (14) we see that

$$|\mathsf{cl}(G)| = \sum_{i=1}^{r} \dim \mathsf{Z}(D_i). \tag{15}$$

For each $i \in \{1, \dots, r\}$ we have $\dim \mathsf{Z}(D_i) \geq 1$, since $0 \neq 1_{S_i} \in \mathsf{Z}(D_i)$, so this equality tells us that $r \leq |\mathsf{cl}(G)|$. Moreover, if $\Bbbk$ is algebraically closed, we must have $\dim \mathsf{Z}(D_i) = 1$ for all $i \in \{1, \dots, r\}$, as in that case each $\mathsf{Z}(D_i)$ is a finite extension of $\Bbbk$ —which must therefore be trivial— and then the equality (15) becomes simply $|\mathsf{cl}(G)| = r$, as claimed in (*ii*). □

§3.3. One-dimensional modules

3.3.1. It is easy to describe the one-dimensional modules of a group algebra, and in fact this does not require any hypothesis on the field.

Proposition. *Let G be a finite group and let G' be its derived subgroup.*

(*i*) *If S is a one-dimensional representation of G, there exists a function $\chi_S : G \to \Bbbk^\times$ such that $gx = \chi_S(g)x$ for all $g \in G$ and all $x \in S$, and this function is a morphism of groups.*

(*ii*) *If S and S' are one-dimensional representations of G, then we have $\chi_S = \chi_{S'}$ iff $S \cong S'$.*

(*iii*) *Conversely, if $\chi : G \to \Bbbk^\times$ is a morphism of groups, there exists a simple module S such that $\chi_S = \chi$.*

(*iv*) *There are $|\mathsf{hom}_{\mathsf{Grp}}(G/G', \Bbbk^\times)|$ isomorphism classes of one-dimensional representations of G.*

Proof. (*i*) Let S be a one-dimensional representation of G and fix $x_0 \in S \setminus 0$. Since $\{x_0\}$ is then a basis of S as a vector space, for each $g \in G$ there exists a scalar $\chi_S(g) \in \Bbbk$ such that $gx_0 = \chi_S(g)x_0$, and this scalar is not zero since $x_0 = g^{-1}gx_0 = \chi_S(g^{-1})\chi_S(g)x_0$, so that $\chi_S(g^{-1})\chi_S(g) = 1$ in $\Bbbk$. We obtain in this way a funcion $\chi_S : G \to \Bbbk^\times$. It is immediate that we actually have taht $gy = \chi_S(g)y$ for all $g \in G$ and all $y \in S$; this implies, in particular, that the function χ_S does not depend on the choice of x_0.

We have that $\chi_S(1_G) = 1_\Bbbk$ and if g, $h \in G$, we have that $ghx_0 = \chi_S(gh)x_0$ and, on the other hand, that

$$ghx_0 = g(hx_0) = \chi_S(h)gx_0 = \chi_S(g)\chi_S(h)x_0,$$

so $\chi_S(gh) = \chi_S(g)\chi_S(h)$. This shows that χ_S is a morphism of groups.

(*ii*) Let S and S' be two one-dimensional representations of G. If there is an isomorphism $f : S \to S'$ of representations and $x_0 \in S \setminus 0$, for all $g \in G$, we have that

$$\chi_{S'}(g)f(x_0) = gf(x_0) = f(gx_0) = f(\chi_S(g)x_0) = \chi_S(g)f(x_0)$$

and, since $f(x_0) \neq 0$, it follows that $\chi_{S'} = \chi_S$.

Conversely, suppose that $\chi_S = \chi_{S'}$. Let $x_0 \in S \setminus 0$ and $y_0 \in S' \setminus 0$ and consider the unique linear map $f : S \to S'$ such that $f(x_0) = y_0$. if $g \in G$, then we have that

$$f(gx_0) = f(\chi_S(g)x_0) = \chi_S(g)f(x_0) = \chi_S(g)y_0 = \chi_{S'}(g)y_0 = fy_0 = gf(x_0)$$

and, since $\{x_0\}$ spans S, this is enough to conclude that f is $\Bbbk G$-linear so that it is in fact an isomorphism of representations.

(*iii*) Let $\chi : G \to \Bbbk^\times$ be a morphism of groups, let $S = \Bbbk$ and define $\rho : G \to \mathsf{End}_\Bbbk(S)$ sso that $\rho(g)(x) = \chi(g)x$ for all $g \in G$ and all $x \in S$. It is easy to check that ρ is a morphism of groups, so that (S, ρ) is a representation of G. It is a simple representation simply because $\dim S = 1$, and it is clear that $\chi_S = S$.

(*iv*) Let $\mathscr{S}$ be the set of isomorphism classes of one-dimensional representations of G; if S is such a representation, let us write as usual $[S]$ its isomorphism class. It is clear from (*i*), (*ii*) that there is a injective function $c : \mathscr{S} \to \hom_{\mathsf{Grp}}(G, \Bbbk^\times)$ such that for each one-dimensional representation S te have $c([S]) = \chi_S$, and it follows from (*iii*) that it is also surjective, so that it is in fact a bijection. On hte other hand, if $\pi : G \to G/G'$ is the canonical projection, we know that the function

$$\pi^* : \chi \in \hom_{\mathsf{Grp}}(G, \Bbbk^\times) \mapsto \chi \circ \pi \in \hom_{\mathsf{Grp}}(G/G', \Bbbk^\times)$$

is also bijective, since $\Bbbk^\times$ is an abelian group. Considering the composition $\pi^* \circ c$ we see that $|S| = |\hom_{\mathsf{Grp}}(G/G', \Bbbk^\times)|$. This proves (*iv*). □

3.3.2. If we make an arithmetical hypothesis on the ground field, the last claim of Proposition 3.3.1 can be made more precise.

Proposition. *If the ground field $\Bbbk$ contains a primitive root of unity of order equal to the exponent of G, the number of isomorphism classes of one-dimensional representations of G is $|G/G'|$.*

Notice that the hypothesis implies in particular that the characteristic of $\Bbbk$ does not divide the order of G.

Proof. In view of part (*iv*) of Proposition 3.3.1, we have to show that $\hom_{\mathsf{Grp}}(G/G', \Bbbk^\times)$ and G/G' have the same number of elements. The quotient G/G' is a finite abelian group, so there exist cyclic groups $C_1, \dots, C_m$ such that $G/G' \cong \prod_{i=1}^m C_i$, and then there is a bijection

$$\hom_{\mathsf{Grp}}(G/G', \Bbbk^\times) \cong \prod_{i=1}^m \hom_{\mathsf{Grp}}(C_i, \Bbbk^\times). \tag{16}$$

A consequence of this is that to prove the proposition it is enough to show that

if C is a cyclic group of order n and $\Bbbk$ contains a primitive root of order n, then $|\hom_{\mathsf{Grp}}(C, \Bbbk^\times)| = n$. (17)

Indeed, the hypothesis that $\Bbbk$ contains a primitive root of unity of order equal to the exponent of G implies that for each $i \in \{1, \dots, m\}$ it contains a primitive root of unity of order $|C_i|$, and then the isomorphism (16) and the claim (17) tell us that

$$|\hom_{\mathsf{Grp}}(G/G', \Bbbk^\times)| = \prod_{i=1}^m |\hom_{\mathsf{Grp}}(C_i, \Bbbk^\times)| = \prod_{i=1}^m |C_i| = |G/G'|.$$

Let us therefore prove (17). Let $x \in C$ be a generator and let $\omega_n \subseteq \Bbbk^\times$ be the subgroup of roots of unity of order n, which has order n by hypothesis. If $f : C \to \Bbbk^\times$ is a morphism of groups, then $1 = f(1_C) = f(x^n) = f(x)^n$, so that $f(x) \in \omega_n$. This implies that there is a function $v : \mathsf{hom}_{\mathsf{Grp}}(C, \Bbbk^\times) \to \omega_n$ such that $v(f) = f(x)$ for each $f \in \mathsf{hom}_{\mathsf{Grp}}(C, \Bbbk^\times)$. This function is injective —as x generates C, two homomorphisms $C \to \Bbbk^\times$ which take the same value on x are in fact equal— and it is asily seen to be also surjective. We can thus conclude that $|\mathsf{hom}_{\mathsf{Grp}}(C, \Bbbk^\times)| = |\omega_n| = n$. $\square$

3.3.3. Proposition. *Let G be a finite group and let S be a simple $\Bbbk G$-module. If $\dim S = 1$, then $\dim \mathsf{End}_{\Bbbk G}(S) = 1$ and the multiplicity of S as a direct summand of $\Bbbk G$ is 1. Moreover, if $\chi_S : G \to \Bbbk^\times$ is the morphism of groups correspinding to S as in Proposition 3.3.1, then the element*

$$u_S = \sum_{h \in G} \chi_S(h^{-1}) h \in \Bbbk G$$

spans a 1-dimensional subspace of $\Bbbk G$ which is a unique $\Bbbk G$-submodule isomorphic to S.

Proof. As $\dim S = 1$, we have that $\dim \mathsf{End}_{\Bbbk}(S) = 1$ and this implies in turn that the algebra $\mathsf{End}_{\Bbbk G}(S)$, being non-zero and contained in $\mathsf{End}_{\Bbbk}(S)$, must be itself one-dimensional. On the other hand, if n be the multiplicity of S as a direct summand of $\Bbbk G$, we know from Proposition 3.2.2 that $n \dim \mathsf{End}_{\Bbbk G}(S) = \dim S$. The proposition follows immediately from these two facts and an easy computation showing that $g \cdot u_S = \chi_S(g) u_S$ for all $g \in G$. $\square$

§3.4. Examples

Abelian groups

3.4.1. If an abelian group has semisimple group algebra, then its representation theory is particularly easy to describe:

Proposition. *Suppose that the ground field $\Bbbk$ is algebraically closed. Let G be a finite abelian group whose order is coprime with the characteristic of $\Bbbk$. Let $\hat{G} = \mathsf{hom}_{\mathsf{Grp}}(G, \Bbbk^\times)$.*

- (*i*) *If $\chi \in \hat{G}$ is a morphisms of groups, then there is a simple $\Bbbk G$-module S_χ which coincides with $\Bbbk$ as a vector space and such that $g \cdot u = \chi(g) u$ for all $g \in G$ and $u \in S_\chi$. If $\chi, \chi' \in \hat{G}$, we have $S_\chi \cong S_{\chi'}$ iff $\chi = \chi'$.*
- (*ii*) *The set $\{S_\chi : \chi \in \hat{G}\}$ is a complete system of representatives of the isomorphism classes of simple $\Bbbk G$-modules. We have $|\hat{G}| = |G|$.*
- (*iii*) *There is an isomorphism of $\Bbbk G$-modules $\Bbbk G \cong \bigoplus_{\chi \in \hat{G}} S_\chi$ and an isomorphism of algebras $\Bbbk G \cong \Bbbk^{|G|}$.*

Proof. The group algebra $\Bbbk G$ is semisimple. Let $\{S_1, \dots, S_r\}$ be a system of representatives of the isomorphism classes of simple $\Bbbk G$-modules, let $n_1, \dots, n_r$ be their multiplicities as direct summands of the regular module $\Bbbk G$ and let $D_i = \mathsf{End}_{\Bbbk G}(S_i)$ for each $i \in \{1, \dots, n\}$. Since D_i is a division algebra and $\Bbbk$ is algebraically closed, we have

$\dim D_i = 1$ for all $i \in \{1, \dots, r\}$. On the other hand, since there is an isomorphism of algebras $\Bbbk G \cong \prod_{i=1}^{r} M_{n_i}(D_i^{\mathsf{op}})$ and $\Bbbk G$ is commutative, we clearly must have that $n_i = 1$ for all $i \in \{1, \dots, r\}$ and then, in view of part (*iv*) of Proposition 3.2.2, that $\dim S_i = 1$ for all $i \in \{1, \dots, r\}$. We thus see that all simple $\Bbbk G$-modules are one-dimensional, and the proposition follows from Proposition 3.3.1 and Proposition 3.3.2. □

Direct products

3.4.2. There is a simple way to construct a representation of a direct product of two groups from representations of the factors:

Proposition. *Let G and H be two finite groups.*

(*i*) *If M and N are representations of G and H, respectively, then the vector space $M \otimes N$ is a representation of $G \times H$ with respect to the unique action such that*

$$(g,h) \cdot m \otimes n = (g \cdot m) \otimes (h \cdot n) \tag{18}$$

for all $(g,h) \in G \times H$, all $m \in M$ and all $n \in N$.

(*ii*) *If M and P are representations of G and N and Q of H, then there is a linear map*

$$\zeta : \mathsf{hom}_G(M,P) \otimes \mathsf{hom}_H(N,Q) \to \mathsf{hom}_{G\times H}(M \otimes N, P \otimes Q)$$

such[2] *that $\zeta(f \otimes g) = f \otimes g$ for all $f \in \mathsf{hom}_G(M,P)$ and all $g \in \mathsf{hom}_G(N,Q)$ is an isomophism.*

(*iii*) *If M and N are representations of G and H, respectively, there is an isomorphism of algebras*

$$\mathsf{End}_G(M) \otimes \mathsf{End}_H(N) \cong \mathsf{End}_{G\times N}(M \otimes N).$$

Proof. That there is a unique action of $G \times H$ on $M \otimes N$ such that the relation (18) holds as claimed in (*i*) is easy to see. To prove (*ii*), let M and P be representations of G and N and Q of H. We view the $G \times H$-module $P \otimes Q$ as a G-module by restriction along the morphism $g \in G \mapsto (g, 1_H) \in G \times H$ so, in particular, we can consider the vector space $\mathsf{hom}_G(M, P \otimes Q)$. This vector space is an H-module with respect to the action such that

$$(h \cdot f)(m) = (1_G, h) \cdot f(m)$$

for all $h \in H$, $g \in \mathsf{hom}_G(M, P \otimes Q)$ and $m \in M$. The isomorphism

$$u_1 : \mathsf{hom}_{\Bbbk}(N, \mathsf{hom}_{\Bbbk}(M, P \otimes Q)) \to \mathsf{hom}_{\Bbbk}(M \otimes N, P \otimes Q)$$

[2] We emphasize that $f \otimes g$ means one thing on the left of this equality and something different on the right!

such that $u_1(f)(m \otimes n) = f(n)(m)$ for all $f \in \mathsf{hom}_{\Bbbk}(N, \mathsf{hom}_{\Bbbk}(M, P \otimes Q))$, $m \in M$ and $n \in N$, is easily seen to restrict to a bijective linear map

$$u_2 : \mathsf{hom}_H(N, \mathsf{hom}_G(M, P \otimes Q)) \to \mathsf{hom}_{G \times H}(M \otimes N, P \otimes Q).$$

On the other hand, the isomorphism

$$v_1 : \mathsf{hom}_{\Bbbk}(M, P) \otimes Q \to \mathsf{hom}_{\Bbbk}(M, P \otimes Q)$$

such that $v_1(f \otimes q)(m) = f(m) \otimes q$ for all $f \in \mathsf{hom}_{\Bbbk}(M, P)$, $q \in Q$ and $m \in M$, restricts to an isomorphism

$$v_2 : \mathsf{hom}_G(M, P) \otimes Q \to \mathsf{hom}_G(M, P \otimes Q).$$

Similarly, for every vector space U the isomorphism

$$\tilde{w}_1 : U \otimes \mathsf{hom}_{\Bbbk}(N, Q) \to \mathsf{hom}_{\Bbbk}(N, U \otimes Q)$$

such that $\tilde{w}_1(u \otimes f)(n) = u \otimes f(n)$ for all $u \in U$, $f \in \mathsf{hom}_{\Bbbk}(N, Q)$ and $n \in N$, restricts to an isomorphism

$$\tilde{w}_1 : U \otimes \mathsf{hom}_H(N, Q) \to \mathsf{hom}_H(N, U \otimes Q),$$

so that in particular we have such an isomorphism

$$w_1 : \mathsf{hom}_G(M, P) \otimes \mathsf{hom}_H(N, Q) \to \mathsf{hom}_H(N, \mathsf{hom}_G(M, P) \otimes Q),$$

The composition

$$u_2 \circ v_2 \circ w_2 : \mathsf{hom}_G(M, P) \otimes \mathsf{hom}_H(N, Q) \to \mathsf{hom}_{G \times H}(M \otimes N, P \otimes Q) \tag{19}$$

is thus an isomorphism, and a calculation shows that this is the map mentioned in (*ii*).

If we specialize the isomorphism (19) to the case where $P = M$ and $Q = N$, we obtain an isomorphism of vector spaces $\mathsf{End}_G(M) \otimes \mathsf{End}_H(N) \cong \mathsf{End}_{G \times N}(M \otimes N)$, and an inmediate verification shows that it is a morphim of algebras: this proves the claim (*iii*) of the proposition. □

3.4.3. Using the construction of Proposition 3.4.2, we are able to decribe the representations of a direct product of groups. For this result, the hypothesis that the ground field be algebraically closed is critical.

Proposition. *Suppose that the ground field $\Bbbk$ is algebraically closed. Let G and H be two finite groups whose orders are coprime with the characteristic of $\Bbbk$, and let $K = G \times H$.*

(*i*) *If M and N are simple $\Bbbk G$- and $\Bbbk H$-modules, respectively, then $M \otimes N$ is a simple $\Bbbk K$-module.*

(*ii*) *Conversely, if S is a simple $\Bbbk K$-module, there exist a simple $\Bbbk G$-module M and a simple $\Bbbk H$-odule N such that $S \cong M \otimes N$ is a simple $\Bbbk K$-module.*

(*iii*) *If $\mathscr{S}_G$ and $\mathscr{S}_H$ are complete systems of representatives for the isomorphism classes of simple $\Bbbk G$- and $\Bbbk H$-modules, respectively, then $\{S \otimes T : S \in \mathscr{S}_G, T \in \mathscr{S}_H\}$ is a complete system of representatives for the isomorphism of simple $\Bbbk K$-modules.*

Proof. (*i*) Let M and N be simple $\Bbbk G$- and $\Bbbk H$-modules. Proposition 3.4.2 gives us an isomorphism of algebras $\mathsf{End}_{\Bbbk K}(M \otimes N) \cong \mathsf{End}_{\Bbbk G}(M) \otimes \mathsf{End}_{\Bbbk H}(N)$ and, since $\Bbbk$ is algebraically closed, both $\mathsf{End}_{\Bbbk G}(M)$ and $\mathsf{End}_{\Bbbk H}(N)$ are isomorphic as algebras to $\Bbbk$, so that $\mathsf{End}_{\Bbbk K}(M \otimes N) \cong \Bbbk \otimes \Bbbk \cong \Bbbk$. We thus see that $\mathsf{End}_{\Bbbk K}(M \otimes N)$ is a local algebra, and Proposition 1.2.5 tells is that $M \otimes N$ is indecomposable, which, in this context, is the same as simple.

(*ii*) There is a linear map $f : \Bbbk G \otimes \Bbbk H \to \Bbbk K$ such that $f(g \otimes h) = (g, h)$ for all $g \in G$ and all $h \in H$, it is clearly bijective and, if we turn $\Bbbk G \otimes \Bbbk H$ into a $\Bbbk K$-module as in Proposition 3.4.2, it is an isomorphism of $\Bbbk K$-modules. If $\{S_1, \dots, S_r\}$ and $\{T_1, \dots, T_s\}$ are complete systems of representatives of the isomorphism classes of the simple $\Bbbk G$- and $\Bbbk H$-modules, respectively, and for each $i \in \{1, \dots, r\}$ we let n_i be the multiplicity of S_i as a direct summand of $\Bbbk G$, and for each $j \in \{1, \dots, s\}$ we let m_j be the multiplicity of T_j as a direct summand of $\Bbbk H$, we have $\Bbbk G \cong \bigoplus_{i=1}^r S_u^{n_i}$ and $\Bbbk H = \bigoplus_{j=1}^s T_j^{m_j}$ as $\Bbbk G$- and $\Bbbk H$-modules, so that

$$\Bbbk G \otimes \Bbbk H \cong \bigoplus_{\substack{1 \leq i \leq r \\ 1 \leq j \leq s}} (S_i \otimes T_j)^{n_i m_j}$$

as $\Bbbk K$-modules. This, in view of the Krull-Remak-Schmidt Theorem 1.4.1, tells us that every simple $\Bbbk K$-module U, which we know is a direct summand of $\Bbbk K$, is in fact a direct summand of a $\Bbbk K$-module of the form $S_i \otimes T_j$ for some $i \in \{1, \dots, r\}$ and some $j \in \{1, \dots, s\}$. As the module $S_i \otimes T_j$ is in fact simple, as we showed in (*i*), this means that it is isomorphic to U. This proves (*ii*).

(*iii*) Given what we have already done, to prove this it is enough to check that if S and S' are simple $\Bbbk G$-modules and T and T' simple $\Bbbk H$-modules, then $S \otimes T \cong S' \otimes T'$ only if $S \cong S'$ and $T \cong T'$. This follows from Proposition 3.4.2: if there is an isomorphism $S \otimes T \cong S' \otimes T'$, we must have $\mathsf{hom}_{\Bbbk K}(S \otimes T, S' \otimes T') \neq 0$ and, since this vector space is isomorphic to $\mathsf{hom}_{\Bbbk G}(S, S') \otimes \mathsf{hom}_{\Bbbk H}(T, T')$, this is only possible if $\mathsf{hom}_{\Bbbk G}(S, S') \neq 0$ and $\mathsf{hom}_{\Bbbk H}(T, T') \neq 0$ which, in turn and according to Proposition 2.1.2, tells us that $S \cong S'$ and $T \cong T'$. □

Dihedral groups

3.4.4. A ***dihedral group*** is a non-cyclic group which is generated by two elements of order 2. It is clear that such a group, if finite, has even order larger than 2.

Lemma. *If G is a finite dihedral group of order $2n$, then G is isomorphic the group*

$$D_{2n} = \langle r, s : r^n,\ s^2,\ (rs)^2 \rangle.$$

Proof. Let G be a finite dihedral group and let g, $h \in G$ be two elements of order 2 which generate G. Since the group is finite, the element $k = gh$ has finite order; let us write that order n. If $n = 2$, then g and h commute, so that G is abelian and, since it is not cyclic, isomorphic to $C_2 \times C_2 \cong D_4$. We suppose hereforth that $n > 2$. There is a morphism $f : D_{2n} \to G$ such that $f(r) = k$ and $f(s) = g$, and it is surjective since g and k generate G.

In D_{2n} we have $(rs)^2 = 1$, so that $sr = r^{-1}s$ and $sr^{-1} = rs$. It follows from this that every element of D_{2n} is of the form $r^i s^j$ with (i, j) an element of the set $I = \{(u, v) : 0 \leq u < n,\ 0 \leq v < 2\}$ and, in particular, that $|D_{2n}| \leq 2n$. Since the map f is surjective, this implies in turn that every element of G is of the form $k^i g^j$ for some $(i, j) \in I$.

If $(i, j) \in I$, we can compute that $k^i g^j \cdot k \cdot (k^i g^j)^{-1}$ is k or k^{-1} according to whether j is 0 or 1 and using this and the fact that $k \neq k^{-1}$ because $n > 2$ we see that if (i, j), $(i', j') \in I$ are such that $k^i g^j = k^{i'} g^{j'}$ in G, then $(i, j) = (i', j')$. This means that G has exactly $2n$ elements, so that D_{2n} has also that order, and that the map f is an isomorphism. □

3.4.5. Proposition. *Let n be a positive integer, let $D_{2n} = \langle r, s : r^n,\ s^2,\ (rs)^2 \rangle$ be the dihedral group of order $2n$ and suppose that $\Bbbk$ is an algebraically closed field whos characteristic does not divide $2n$.*

(*i*) *The following are simple representations of D_{2n}:*
- *for each $\varepsilon \in \{\pm 1\}$, the pair $(V_{1,\varepsilon}, \rho)$ with $V_{1,\varepsilon} = \Bbbk$, $\rho(r) = \mathrm{id}_V$ and $\rho(s) = \varepsilon\,\mathrm{id}_V$;*
- *for each nth root of unity $\lambda \in \Bbbk^\times$ with $\lambda \neq \pm 1$, the pair (V_λ, ρ) with $V_\lambda = \Bbbk^2$ and $\rho(r)$, $\rho(s) \in \mathsf{GL}_\Bbbk(V_\lambda)$ having matrices $\|\rho(r)\| = \left(\begin{smallmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{smallmatrix}\right)$ and $\|\rho(s)\| = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ with respect to the standard basis;*

and, if n is even,
- *for each $\varepsilon \in \{\pm 1\}$, the pair $(V_{-1,\varepsilon}, \rho)$ with $V_{-1,\varepsilon} = \Bbbk$, $\rho(r) = -\mathrm{id}_V$ and $\rho(s) = \varepsilon\,\mathrm{id}_V$.*

(*ii*) *No two of the one-dimensional representations described in (i) are isomorphism. On the other hand, if λ, $\mu \in \Bbbk$ are nth roots of unity such that $\lambda^2 \neq 1 \neq \mu^2$, then we have $V_\lambda \cong V_\mu$ iff $\mu \in \{\lambda, \lambda^{-1}\}$*

(*iii*) *Every simple representation of D_{2n} is isomorphic to one of those listed in (i). The number of isomorphism classes of simple modules is thus $(n+3)/2$ if n is odd and $(n+6)/2$*

if n is even.

Proof. The claim that those listed in (*i*) are representations of D_{2n} and that they are simple is easy to verify, as is the claim of (*ii*).

Let (V, ρ) be a simple representation of D_{2n}. Since $\Bbbk$ is algebraically closed, the linear map $\rho(r) \in \mathsf{End}_{\Bbbk}(V)$ has at least one eigenvector, so that there exist $v \in V \setminus 0$ and $\lambda \in \Bbbk$ such that $rv = \lambda v$. As $r^n = 1$ in D_{2n}, we have $v = r^n v = \lambda^n v$, so that λ is an nth root of unity.

Let $w = sv$. As $rs = sr^{-1}$, we have

$$rw = rsv = sr^{-1}v = \lambda^{-1}sv = \lambda^{-1}w,$$

so that w is an eigenvector for the linear map $\rho(r)$ corresponding to the eigenvalue λ^{-1}.

If $\lambda^2 \neq 1$, then $\lambda \neq \lambda^{-1}$ and the set $\mathscr{B} = \{v, w\}$ is linearly independent since its elements are eigenvalues for the linear map $\rho(r)$ corresponding to distinct eigenvalues. The subspace $\langle v, w\rangle$ is a $\Bbbk D_{2n}$-submodule, as one can check immediatly, so he simplicity of V implies that in fact $\mathscr{B}$ is a basis for V. With respect to that basis, the matrices of $\rho(r)$ and $\rho(s)$ are

$$\|\rho(r)\|_{\mathscr{B}} = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}, \qquad \|\rho(s)\|_{\mathscr{B}} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

It follows that V is isomorphic to V_λ.

Suppose now that $\lambda^2 = 1$; if n is odd, this implies that $n = 1$, and if n is even, then λ is one of 1 or -1. If $v + w \neq 0$, then $\langle v + w\rangle$ is a $\Bbbk D_{2n}$-submodule of V, so that in fact V is one-dimensional, spanned by $v + w$, and $\rho(r) = \lambda\,\mathrm{id}_V$ y $\rho(s) = \mathrm{id}_V$: we see that $V \cong V_{\lambda,1}$. If instead $v + w = 0$, so that $sv = -v$, the subspace $\langle v\rangle$ is a submodule, and then v spans V, $\rho(r) = \lambda\,\mathrm{id}_V$ and $\rho(s) = -\mathrm{id}_V$: in this case we have $V \cong V_{\lambda,-1}$. $\square$

The quaternion group

3.4.6. The ***quaternion group*** is the group

$$Q = \langle i, j, k : i^2 = j^2 = k^2 = ijk\rangle. \tag{20}$$

Let $u = ijk$. Since $ijk = k^2$, we have $ij = k$ and therefore $i^2 = k^2 = ijij$, so that $i = jij$ and $iji^{-1} = j^{-1}$. It follows that

$$u^2 = i^4 = ij^2i = (iji^{-1})(iji^{-1})i^2 = j^{-2}i^2 = 1.$$

Since $u = i^2$, $ui = i^2i = ii^2 = iu$, and similarly u commutes with j and k. This means that u is central, so that the subgroup (u) is normal of order at most 2. The quotient $Q/(u)$ has presentation $\langle i, j, k : i^2, j^2, k^2, ijk\rangle$, which simplifies at once to $\langle i, j : i^2, j^2, (ij)^2\rangle$:

this makes it cleat that $Q/(u)$ is isomorphic to the Klein four-group. We thus see that Q has order either 4 or 8 according to whether the order of u is 1 or 2.

Let us suppose for a moment that u has order 2, so that i and j have order 4. The elements of Q are then

$$1, \quad i, \quad i^2, \quad i^3, \quad j, \quad ij, \quad i^2j, \quad i^3j.$$

If we index them in this order, the permutation given by multiplication from the left by i is $\pi_i = (1\,2\,3\,4)(5\,6\,7\,8)$. Let π_j be the permutation given by multiplication by j on the left. We have $\pi_j(1) = 5$ and $\pi_j(5) = \pi_j^2(1) = \pi_i^2(1) = 3$, because $j^2 = i^2$. Similarly, we have $\pi_j(3) = \pi_j^2(5) = \pi_i^2(5) = 7$ and $\pi_j(7) = \pi_j^2(3) = \pi_i^2(3) = 1$, and we see that $(1\,5\,3\,7)$ is a cycle of π_j. We have $\pi_j^2(2) = \pi_i^2(2) = 4$ and, since $j^3 i = j^{-1} i = ij$, that $\pi_j^3(2) = 6$, so $\pi_j(2) = \pi_j^{-2}\pi_j^3(2) = \pi_i^{-2}(6) = 8$: it follows that $(2\,8\,4\,6)$ is another cycle of π_j. Notice that this means that π_i and π_i are completely determined.

Now, let us drop the assumption that u has order 2. Using the equality $k = ij$, we see that the presentation (20) can be simplified to $Q = \langle i, j : i^2 = j^2 = (ij)^2 \rangle$. Using this, a trivial calculation shows that there exists in fact a morphism $\phi : Q \to S_8$ such that $\phi(i) = (1\,2\,3\,4)(5\,6\,7\,8)$ and $\phi(j) = (1\,5\,3\,7)(2\,8\,4\,6)$. Since $\phi(i^2) = (1\,3)(2\,4)(5\,7)(6\,8)$, and we see that $u = i^2 \neq 1$. We can therefore conclude that Q has order 8.

3.4.7. As $iji^{-1} = j^{-1}$, we have $[i,j] = iji^{-1}j^{-1} = j^{-2} = u$ and, similarly, $[j,k] = [k,i] = u$. As these three commutators generate the derived subgroup Q' as a normal subgroup and u is central, we see that in fact $Q' = (u)$.

3.4.8. Proposition. *Suppose that the characteristic of $\Bbbk$ is not 2. The quaternion group Q has five simple representations, as given in the following table:*

V	$\lVert\rho(i)\rVert_{\mathscr{B}}$	$\lVert\rho(j)\rVert_{\mathscr{B}}$
$\Bbbk$	(1)	(1)
$\Bbbk$	(1)	(-1)
$\Bbbk$	(-1)	(1)
$\Bbbk$	(-1)	(-1)
$\Bbbk^2$	$\begin{pmatrix} \alpha & 0 \\ 0 & -\alpha \end{pmatrix}$	$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$

with $\alpha \in \Bbbk$ such that $\alpha^2 = -1$ and in each case $\mathscr{B}$ a basis of V.

Proof. A direct verification shows that the five representations described in the statement are indeed represeentations of G.

We know from Proposition 3.3.2 that Q has $|Q/Q'| = |Q/(u)| = 4$ isomorphism classes of one-dimensional representations. Since Q/Q' is a Klein four-group, it is easy to see that those one-dimensional representations are precisely the ones listed in the table of the proposition. If $n_1, n_2, \dots,$ are the dimensions of representatives of the other isomorphism classes of simple representations, all of which are at least 2, we must have $8 = |Q| = 4 \cdot 1^2 + n_1^2 + n_2^2 + \cdots$ and this is only possible if there is exactly one isomorphism class of simple modules of dimension larger than 1 and that dimension is actually equal to 2.

It follows that there is, up to isomorphism, a unique simple two-dimensional representation (V, ρ). Since u is central in Q, the linear map $\rho(u) : V \to V$ is map of $\Bbbk Q$-modules and Schur's Leemma tells us that $\rho(u)$ is in fact multiplicatin by a scalar. Since u has order two, the scalar must be either 1 or -1. In the first case, the subgroup (u) acts trivially on V, which can therefore be obtained from a simple representation of $Q/(u)$ by restriction along the projection $Q \to Q/(u)$: this is impossible as the quotient $Q/(u)$ is abelian, so its simple representations are all one-dimensional. We thus conclude that $\rho(u) = -\mathrm{id}_V$.

The map $\rho(j)$ has order 4 so it is diagonalizable. Since $\rho(j)^2 = \rho(u) = -\mathrm{id}_V$, its eigenvalues are square roots of -1. If the two eigenvalues were equal, the $\rho(j)$ would commute with $\rho(i)$ and then, in view of the relation $iji^{-1} = j^{-1}$, we would have that $\rho(j) = \rho(j)^{-1}$ or, equivalently, that $\rho(j)^2 = \mathrm{id}_V$. As this cannot happen, because the characteristic of $\Bbbk$ is not 2 and $V \neq 0$, we see that the two eigenvalues of $\rho(j)$ are distinct. If $\alpha \in \Bbbk$ is such that $\alpha^2 = -1$, there is then a basis $\mathscr{B} = \{v_1, v_2\}$ of V with respect to which $\|\rho(j)\|_{\mathscr{B}} = \left(\begin{smallmatrix} \alpha & 0 \\ 0 & -\alpha \end{smallmatrix}\right)$.

Since $jij = i$, we have $iv_1 = jijv_1 = \alpha jiv_1$, so that $jiv_1 = -\alpha iv_1$: this means that iv_1 is an eigenvector of $\rho(j)$ for the eigenvalue $-\alpha$, and there is then a scalar β_1 such that $iv_1 = \beta_1 v_2$. In a similar way, there is a scalar β_2 such that $iv_2 = \beta_2 v_1$. If we let $v_2' = \beta_1 v_2$, then $\mathscr{B} = \{v_1, v_2'\}$ is also a basis of V, and we have $\|\rho(j)\|_{\mathscr{B}'} = \left(\begin{smallmatrix} \alpha & 0 \\ 0 & -\alpha \end{smallmatrix}\right)$. and $\|\rho(i)\|_{\mathscr{B}'} = \left(\begin{smallmatrix} 0 & \beta \\ 1 & 0 \end{smallmatrix}\right)$, with $\beta = \beta_1\beta_2$. As $\rho(i)^2 = -\mathrm{id}_V$, we must have $\beta = -1$. The representation V is therefore the one appearing in the statement of the proposition. $\square$

The group of the tetrahedron

The group of the cube

3.4.9. Let G be the group of symmetries of a cube. There are 24 ordered pairs of vertices connected by an edge of the cube, and G acts simply transitively on them, so G has 24 elements. On the other hand, the cube has four diagonals and G permutes them faithfully. As the full group of permutations of these four diagonals is a symmetric group of degree 4, which has also 24 elements, we see that $G \cong S_4$.

Let x, y and z be rotations through axes going through the center of the cube and the middle point of a edge, a vertex on that edge, and the center of a face adjacent to that edge, respectively, of angles 180°, 120° and 90°. The orders of these elements are 2,

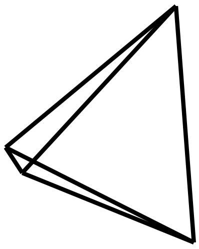


Figure 1. The tetrahedron

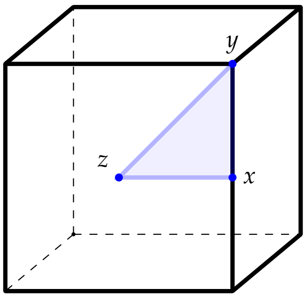


Figure 2. The cube

3 and 4, and it is easy to see that $xyz = 1$, and therefore there is an evident morphism

$$\phi : \langle x, y, z : x^2 = y^3 = z^4 = xyz = 1 \rangle \to G$$

Since x, y and z generate G, this is a surjection.

§3.5. The modular situation

3.5.1. Let G be a finite group, let H be a subgroup of G and for each $\Bbbk G$-module M let $M^P = \{m \in M : hm = m \text{ for all } h \in H\}$, which is clearly a vector subspace of M.

Lemma.

(*i*) *If $\phi : M \to N$ is a morphism of $\Bbbk G$-modules, then we have $\phi(M^P) \subseteq N^P$, so that we can consider the restriction $\phi^P = \phi|_{M^P} : M^P \to N^P$.*

(*ii*) *If M is a $\Bbbk G$-module and we view it as a $\Bbbk H$-module by restriction, and let $\Bbbk$ be the trivial $\Bbbk H$-module. If $f \in \hom_{\Bbbk P}(\Bbbk, M)$, then we have $f(1) \in M^P$. There is therefore a function*

$$\phi_M : f \in \hom_{\Bbbk P}(\Bbbk, M) \mapsto f(1) \in M^P$$

and this function is an isomorphism of vector spaces.

(iii) If $\phi : M \to N$ is a morphism of $\Bbbk G$-modules, then the following diagram commutes:

$$\begin{tikzcd} \hom_{\Bbbk P}(\Bbbk, M) \arrow[r, "\phi_*"] \arrow[d, "\psi_M"'] & \hom_{\Bbbk P}(\Bbbk, N) \arrow[d, "\psi_N"] \\ M^P \arrow[r, "\phi^P"] & N^P \end{tikzcd}$$

Proof. To be done □

3.5.2. Proposition. *Let G be a finite group. If the characteristic of the ground field $\Bbbk$ divides the order of G, then the algebra $\Bbbk G$ is* not *semisimple.*

Proof. In view of Proposition 2.3.8, to show this it is enough to exhibit a $\Bbbk G$-module which is not projective. Let p be the characteristic of $\Bbbk$, which must be positive, and let P be a Sylow p-subgroup of G. We have the trivial $\Bbbk P$-module $\Bbbk$, and therefore we can consider the $\Bbbk G$-module $X = \Bbbk G \otimes_{\Bbbk P} \Bbbk$. A key property of X is that for each $\Bbbk G$-module M there is an isomorphism $\alpha_M : \hom_{\Bbbk G}(X, M) \to \hom_{\Bbbk P}(\Bbbk, M)$ such that $\alpha_M(f)(1_\Bbbk) = f(1_G \otimes 1_\Bbbk)$ for all $f \in \hom_{\Bbbk G}(X, M)$, and that for each morphism $\phi : M \to N$ of $\Bbbk G$-modules we have $\phi_* \circ \alpha_M = \alpha_N \circ f_*$.

Let now $\varepsilon : \Bbbk G \to \Bbbk$ be the linear map such that $\varepsilon(g) = 1$ for all $g \in G$; it is a surjective morphism of $\Bbbk G$-modules. According to Lemma 3.5.1 and the observation we made about X, we have a commutative diagram

$$\begin{tikzcd} \hom_{\Bbbk G}(X, \Bbbk G) \arrow[r, "\varepsilon_*"] \arrow[d, "\alpha_{\Bbbk G}"'] & \hom_{\Bbbk G}(X, \Bbbk) \arrow[d, "\alpha_\Bbbk"] \\ \hom_{\Bbbk P}(\Bbbk, \Bbbk G) \arrow[r, "\varepsilon_*"] \arrow[d, "\psi_{\Bbbk G}"'] & \hom_{\Bbbk P}(\Bbbk, \Bbbk) \arrow[d, "\psi_N"] \\ (\Bbbk G)^P \arrow[r, "\varepsilon^P"] & \Bbbk^P \end{tikzcd}$$

We will show that the map ε^P is the zero map. Since $\Bbbk^P = \Bbbk$ is not zero, this means that ε^P is not surjective and then, since the vertical arrows in the diagram are isomorphisms, the map $\varepsilon_* : \hom_{\Bbbk G}(X, \Bbbk G) \to \hom_{\Bbbk G}(X, \Bbbk)$ is also not surjective: we will then be able to conclude that X is not a projective $\Bbbk G$-module.

Consider an element $z = \sum_{g \in G} a_g g$, with $a_g \in \Bbbk$ for each $g \in G$, of $\Bbbk G$. We have that $z \in (\Bbbk G)^P$ iff for all $h \in P$ we have

$$\sum_{g \in G} a_g g = z = hg = \sum_{g \in G} a_g hg = \sum_{g \in G} a_{h^{-1}g} g$$

and —since G is a basis of $\Bbbk G$— this happens iff $a_{hg} = a_g$ for all $h \in P$ and all $g \in G$. In other words, we have $z \in \Bbbk G$ iff the function $g \in G \mapsto a_g \in \Bbbk$ is constant on the right cosets of P in G.

Suppose now that z is in $(\Bbbk G)^P$, and let $g_1, \dots, g_r$ be a complete system of representatives for the right cosets of P in G, so that $G = \bigsqcup_{i=1}^r Pg_i$. We then have

$$\varepsilon(z) = \sum_{g \in G} a_g = \sum_{i=1}^r \sum_{g \in Pg_i} a_g = |P| \sum_{i=1}^r a_{g_i}aa = 0$$

because p divides $|P|$. This proves what we wanted. □

Cyclic p-groups

3.5.3. Proposition. *Suppose that the characteristic p of $\Bbbk$ is positive, let $r \geq 1$, let $G = C_{p^r}$ be a cyclic p-group of order p^r and let σ bee a generator of G.*

(*i*) *For each $s \in \{1, \dots, p^r\}$, the $\Bbbk G$-module $V_s = \Bbbk G/((\sigma - 1)^s)$ is indecomposable of dimension s. The only one of these modules which is simple is V_1.*

(*ii*) *The set $\{V_s : 1 \leq s \leq p^r\}$ is a complete system of indecomposable $\Bbbk G$-modules.*

(*iii*) *The algebra $\Bbbk G$ has finite representation type.*

Proof. The algebra $\Bbbk[X] \to \Bbbk G$ which maps X to σ has the polynomial $X^{p^r} - 1$ in its kernel and it is surjective, so that it factors through a surjection $\Bbbk[X]/(X^{p^r} - 1) \to \Bbbk G$. Since the domain of this last map has the same dimension as its codomain, it is in fact an isomorphism. This lets us replace the algebra $\Bbbk G$ by $A = \Bbbk[X]/(X^{p^r} - 1)$ in the statement of the proposition. Let $x \in A$ be the class of X.

Let M be an indecomposable A-module and let $\xi : m \in M \mapsto xm \in M$. Since $x^{p^r} - 1 = 0$ in A, the map ξ annihilates the polinomial $X^{p^r} - 1 = (X - 1)^{p^r}$ and therefore the minimal polynomial of ξ is of the form $(X - 1)^s$ for some $s \in \{1, \dots, p^r\}$ and, in particular, the only eigenvalue of ξ is 1. We know that there is a direct sum decomposition $M = \bigoplus_{i=1}^r M_i$ with each M_i a ξ-invariant subspace such that the matrix of $\xi|_{M_i} : M_i \to M_i$ with respect to same basis of M_i, is a Jordan block. Since x generates the algebra A, each such subspace M_i is in fact an A-submodule: we must thus have $r = 1$, for M is indecomposable. This tells us that there is a basis $\mathscr{B} = \{v_1, \dots, v_s\}$ of M such that the matrix $\|\xi\|_{\mathscr{B}}$ is a Jordan block of size $\dim M$ with eigenvalue 1, so that $xv_1 = v_1$ and $xv_i = v_i + v_{i-1}$ if $1 < i \leq s$. We see that v_s generates V as an A-module, its annihilator contains $(x-1)^s$ and, since $\dim A/((x-1)^s) = s$, actually concides with it. We can conclude in this way that in fact $V \cong A/((x-1)^s)$ as an A-module and, in consequence, that every indecomposable A-module appears among the modules mentioned in (*i*).

It is clear that if $s, t \in \{1, \dots, p^r\}$, we have $V_s \cong V_t$ iff $s = t$, as this follows simply by looking at the dimension of the modules involved. To finish the proof of the proposition, then, it is enough that we prove that if $s \in \{1, \dots, p^r\}$ then the module V_s is indecomposable. As $V_s \cong A/((x-1)^s)$ as an A-module, we have an algebra isomorphism

$$\mathsf{End}_A(V_s) \cong \mathsf{End}_A(A/((x-1)^s)$$

and, on the other hand, it is easy to check that the function

$$f \in \mathsf{End}_A(A/((x-1)^s) \mapsto f(1) \in A/((x-1)^s)$$

is an isomorphism of algebras. As $A/((x-1)^s) \cong \Bbbk[X]/((x-1)^s)$, the ideals of A are in bijection with those of $\Bbbk[X]$ which contain $(x-1)^s$, and among this it is clear that the one generated by $(x-1)$ is the unique maximal one. We thu see that the endomorphism algebra of V_s is local, so that the module is indecomposable, as we wanted. □

Elementary p-groups of rank 2

3.5.4. Proposition. *Suppose that the characteristic p of $\Bbbk$ is positivei and let $G = C_p \times C_p$ be a direct product of two cyclic p-group of order p. The group algeebra $\Bbbk G$ has infinite representation type.*

Proof. To be done □

§3.6. Separable extensions of algebras

3.6.1. If B is an algebra and A a subalgebra, we say that B is an ***extension*** of A. In that situation, B is an A-bimodule in a natural way so that in particular we can consider the A-bimodule $B \otimes_A B$ and there is a morphism of A-bimodules

$$\mu_{B/A} : B \otimes_A B \to B$$

such that $\mu_{B/A}(b \otimes b') = bb'$ for all $b, b' \in B$. We say that B is a ***separable extension*** of A if this map $\mu_{B/A}$ is a split surjection of B-bimodules, so that there exists a morphism of B-bimodules $s : B \to B \otimes_A B$ such that $\mu_{B/A} \circ s = \mathrm{id}_B$. In the special case were $A = \Bbbk$, we say simply that B is is a ***separable algebra***.

3.6.2. Separability of an extension can be expressed in terms internal to the B-bimodule $B \otimes_A B$ and this is very useful.

Lemma. *Let B be an algebra and let A be a subalgebra. Then B is a separable extension of A iff there exists an element $e \in B \otimes_A B$ such that $\mu_{B/A}(e) = 1$ and $be = eb$ for all $b \in B$.*

Proof. Suppose first that B is a separable extension of A, so that we have a morphism $s : B \to B \otimes_A B$ of B-bimodules such that $\mu_{B/A} \circ s = \mathrm{id}_B$, and consider the element $e = s(1) \in B \otimes_A B$. We have $\mu_{B/A}(e) = \mu_{B/A}(s(1)) = 1$ and, if $b \in B$,

$$be = bs(1) = s(b1) = s(b) = s(1b) = s(1)b = eb$$

because s is a map of B-bimodules. We thus see that the condition is necessary.

To see the sufficiency, suppose that $e \in B \otimes_A B$ is as in the statemeent of the lemma, and conisder the function $s : b \in B \mapsto be \in B \otimes_A B$. It is clearly a map of left B-modules; since b, $b' \in B$, then $s(bb') = bb'e = beb' = s(b)b'$, and this means that s is also a map of right B-modules. Finally, if $b \in B$ we have

$$\mu_{B/A}(s(b)) = \mu_{B/A}(be) = b\mu_{B/A}(e) = b1 = b,$$

so that s is a right inverse to $\mu_{B/A}$. The map $\mu_{B/A}$ is a split surjection of B-bimodules and, therefore, B a separable extension of A. □

3.6.3. With this lemma, we can exhibit a simple example of a separable algebra:

Proposition. *If $n \geq 1$, then the matrix algebra $M_n(\Bbbk)$ is separable.*

Proof. Let $e = \sum_{i=1}^{n} e_{i,1} \otimes e_{1,i} \in M_n(\Bbbk) \otimes M_n(\Bbbk)$, where for each i, $j \in \{1, \ldots, n\}$ we denote $e_{i,j}$ the usual (i,j)th matrix unit, that is, the matrix whose only non-zero entry is the (i,j)th one, which is equal to 1. We have

$$\mu_{M_b(\Bbbk)/\Bbbk}(e) = \sum_{i=1}^{n} e_{i,1}e_{1,i} = \sum_{i=1}^{n} e_{i,i} = 1.$$

On the other hand, if $1 \leq k, l \leq n$ we have

$$e_{k,l}e = \sum_{i=1} e_{k,l}e_{i,1} \otimes e_{1,i} = e_{k,1} \otimes e_{1,l} = \sum_{i=1} e_{i,1} \otimes e_{1,i}e_{k,l} = ee_{k,l}.$$

We thus see that e satisfies the conditions of Lemma 3.6.2 and that $M_n(\Bbbk)$ is therefore a separable algebra. □

3.6.4. Let B be an algebra and A a subalgebra of B. Given another algebra C and a (B, C)-bimodule N, there is a linear map

$$\mu_{N/A} : B \otimes_A N \to N$$

such that $\mu_{N/A}(b \otimes n) = bn$ for all $b \in B$ and all $n \in N$, and it is in fact a morphism of (B, C)-bimodules. Notice that when C is B and N is B with is usual structure of a B-bimodule, the map $\mu_{N/B}$ is precisely the map $\mu_{B/A}$ of 3.6.1.

3.6.5. Proposition. *Let B be an algebra and let A be a subalgebra of B. The following two statements are equivalent:*

(*a*) *B is a separable extension of A.*

(*b*) *For every algebra C and every (B, C)-bimodule N, the morphism $\mu_{N/A} : B \otimes_A N \to N$ is a split surjection of (B, C)-bimodules.*

Proof. If we take $N = B$ in (*b*) we obtain precisely the condition (*a*), so that the implication (*b*) ⇒ (*a*) is clear. Let us prove the converse.

Let C be an algebra and let N be a (B,C)-bimodule. Since we are assuming that B is a separable extension of A, there is a morphism $s : B \to B \otimes_A B$ of B-bimodules such that $\mu_{B/A} \circ s = \mathrm{id}_B$. We have then construct the horizontal solid arrows in the diagram

$$\begin{tikzcd}
B \otimes_B N \arrow[r, "s\otimes\mathrm{id}_N"] \arrow[d, "f"] & B \otimes_A B \otimes_B N \arrow[r, "\mu_{B/A}\otimes\mathrm{id}_N"] \arrow[d, "g"] & B \otimes_B N \arrow[d, "f"] \\
N \arrow[r, dotted, "s_N"] & B \otimes_A N \arrow[r, "\mu_{N/A}"] & N
\end{tikzcd}$$

There are linear maps $f : B \otimes_B N \to N$ and $g : B \otimes_A \otimes_B N \to B \otimes_A N$ such that $f(b \otimes n) = bn$ and $g(b \otimes b' \otimes n) = b \otimes b'n)$ for all $b, b' \in B$ and all $n \in N$, and both f and g are in fact bijective and make the right square in the diagram commute. All the solid arrows are in fact morphisms of (B,C)-bimodules. If we define $s_N : N \to B \otimes_A N$ so that the left square commutes, then s_N is also a morphism of (B,C)-bimodules and the commutation of the whole diagram implies that $\mu_{N/A} \circ s_N = \mathrm{id}_N$. We thus see that $\mu_{N/A}$ is a split surjection of (B,C)-bimodules. □

3.6.6. If B is an algebra, A a subalgebra of B, C another algebra and M a (A,C)-bimodule, there is a map

$$\nu_{B/M} : M \to B \otimes_A M$$

such that $\nu_{B/M}(m) = 1 \otimes m$ for all $m \in M$, and it is a morphism of (A,C)-bimodules. This construction is, in a way, dual to that of 3.6.4 and therefore the following result can be viewed as dual to Proposition 3.6.5:

3.6.7. Proposition. *Let B be an algebra and let A be a subalgebra of A. The following two statements are equivalent:*

(*a*) *A is a direct summand of B as an A-bimodule.*

(*b*) *For every algebra C and every (A,C)-bimodule M, the morphism $\nu_{B/M} : M \to B \otimes_A M$ is a split injection of (A,C)-bimodules.*

Proof. (*a*) ⇒ (*b*) Let $i : A \to B$ be the inclusion. The hypothesis implies that there is a morphism $p : B \to A$ of A-bimodules such that $p \circ i = \mathrm{id}_A$. Let C be an algebra and let M be a (C,A)-bimodule. If $f : A \otimes_A M \to M$ is the linear map such that $f(a \otimes n) = an$ for all $a \in A$ and all $n \in M$, which is a bijection, the solid arrows in the diagram

$$\begin{tikzcd}
A \otimes_A M \arrow[r, "i\otimes\mathrm{id}_M"] \arrow[d, "f"] & B \otimes_A M \arrow[r, "p\otimes\mathrm{id}_M"] \arrow[d, equal] & A \otimes_A M \arrow[d, "f"] \\
M \arrow[r, "\nu_{B/M}"] & B \otimes_A M \arrow[r, dotted, "s_M"] & M
\end{tikzcd}$$

commute and are all morphisms of (A,C)-bimodules. There is then a unique morphism $s_M : B \otimes_A M \to M$ of (A,C)-bimodules which completes the diagram preserving the commutativity, and we have $s_M \circ \nu_{B/M} = \mathrm{id}_M$. It follows that $\nu_{B/M}$ is a split injection of (A, C)-bimodules, as we were to show.

$(b) \Rightarrow (a)$ If we let the algebra C be A and M be A with its usual structure of A-bimodule, the hypothesis (b) tells us that there exists a morphism $s : B \otimes_A A \to A$ such that $s \circ \nu_A = \mathrm{id}_A$. If $f : B \otimes_A A \to A$ is the linear map such that $f(b \otimes a) = ba$ for all $b \in B$ and all $a \in A$, the solid arrows in the diagram

$$\begin{tikzcd} A \arrow[r, "\nu_{B/A}"] \arrow[d, equal] & B \otimes_A A \arrow[r, "s"] \arrow[d, "f"'] & A \arrow[d, equal] \\ A \arrow[r, "i"] & B \arrow[r, dotted, "p"] & A \end{tikzcd}$$

commute and, since they are all morphisms of A-bimodules, there exists a unique morphism $p : B \to A$ of A-bimodules which completes it preserving the commutativy. As $p \circ i = \mathrm{id}_A$, we see that A is a direct summand of B as an A-bimodule. □

3.6.8. Proposition. *Let B be an algebra, let A be subalgebra of B.*

(i) *If for every B-module N the map $\mu_{N/A} : B \otimes_A N \to N$ is a split surjection of B-modules and A has finite representation type, then so does B.*

(ii) *If for every A-module M the map $\nu_{B/M} : M \to B \otimes_A M$ is a split injection of A-modules and B has finite representation type, then so does A.*

Proof. (i) Let $M_1, \dots, M_r$ be representatives for the finitely many isomorphism classes of indecomposable A-modules. Let N be an indecomposable B-module. From the Krull-Remak-Schmidt Theorem 1.4.1 we know there exist non-negative integers $m_1, \dots, m_r$ such that $N \cong \bigoplus_{i=1}^r M_i^{m_i}$ as an A-module, and it follows from this that

$$B \otimes_A N \cong \bigoplus_{i=1}^{r} (B \otimes_A M_i)^{m_i}$$

as a B-module. As the map $\mu_{N/A} : B \otimes_A N \to N$ is a split surjection of B-modules, so that N is isomorphic to an indecomposable summand of $B \otimes_A N$. Using the uniqueness claim of Theorem 1.4.1, we see at once that there exists a $j \in \{1, \dots, r\}$ such that in fact N is isomorphic to an indecomposable direct summand the B-module $B \otimes_A M_j$.

In this way, we conclude that every indecomposable B-module is a direct summand of one of the B-modules $B \otimes_A M_1, \dots, B \otimes_A M_r$. As Theorem 1.4.1 implies that there is a finite number of isomorphism classes of indecomposable summands of this finite set of B-modules, this implies that thre are finitely many isomorphism classes of indecomposable B-modules in all, that is, that B is of finite representation type.

(ii) To be done □

§3.7. Group algebras of finite representation type

3.7.1. Proposition. *Suppose that the characteristic p of $\Bbbk$ is positive and let G be a finite group. If P is a Sylow p-subgroup of G, then the algebra $\Bbbk G$ is a separable extension of $\Bbbk P$.*

Proof. Let $r = [G : P]$ be the index of P in G and let $\{g_1, \dots, g_r\}$ be a complete system of representatives for the left cosets of P in G. As P is a Sylow p-subgroup, r is not divisible by p and we can consider the element $e = \frac{1}{r}\sum_{i=1}^{r} g_i \otimes g_i^{-1}$ of $\Bbbk G \otimes_{\Bbbk P} \Bbbk G$. It is immediate that $\mu_{\Bbbk G/\Bbbk P}(e) = 1$. On the other hand, if $g \in G$ then there exists a permutation π of $\{1, \dots, r\}$ and elements $u_1, \dots, u_r \in P$ such that $gg_i = g_{\pi(i)}u_i$, and then

$$
\begin{aligned}
ge &= \frac{1}{r}\sum_{i=1}^{r} gg_i \otimes g_i^{-1} = \frac{1}{r}\sum_{i=1}^{r} g_{\pi(i)}u_i \otimes g_i^{-1} = \frac{1}{r}\sum_{i=1}^{r} g_{\pi(i)} \otimes u_i g_i^{-1} \\
&= \frac{1}{r}\sum_{i=1}^{r} g_{\pi(i)} \otimes g_{\pi(i)}^{-1} g = eg
\end{aligned}
$$

Since G spans $\Bbbk G$, it follows from this that in fact $be = eb$ for all $b \in \Bbbk G$, and then Lemma 3.6.2 allows us to conclude that $\Bbbk G$ is a separable extension of $\Bbbk P$. □

3.7.2. Proposition. *Let G be a finite group and let H be a subgroup of G. The subalgebra $\Bbbk H$ of $\Bbbk G$ is a direct summand of $\Bbbk G$ as a $\Bbbk G$-bimodule.*

Proof. The set $G \setminus H$ clearly spans a subspace I of $\Bbbk G$ such that $\Bbbk G = \Bbbk H \oplus I$ as vector spaces. If $h \in H$ and $x \in G \setminus H$, we have $hx, xh \in G \setminus H$, and from this it follows that that in fact I is a $\Bbbk H$-subbimodule of $\Bbbk G$. This proves the proposition. □

3.7.3. Lemma. *Let p be a prime number.*

(*i*) *The number of elements of order p in a finite p-group is congruent to -1 modulo p.*

(*ii*) *If G is a non-cyclic p-group, then there exists a normal subgroup N in G such that G/N is isomorphic to $C_p \times C_p$.*

Proof. (*i*) Let $X = \{(g_1, \dots, g_o) \in G^p : g_1 \cdots g_p = 1\}$. It is clear that there are $|X| = |G|^{p-1}$, for the last component of an element of X is determined by the others and the latter can be arbitrary. Let C be a cyclic group of order p and let σ be a generator of C and let us consider the action of C on the set X such that $\sigma \cdot (g_1, \dots, g_p) = (g_2, \cdots, g_p, g_1)$ for all $(g_1, \dots, g_p) \in X$.

The stabilizer of an element $x \in X$ is a subgroup of C, so it is either the trivial subgroup or C itself, and the orbit of x has therefore either p or 1 elements. Moreover, the orbit of x has 1 element iff x is of the form $(g, \dots, g)$ for some $g \in G$ such that $g^p = 1$, and then g is either the identity element or an element of order p in G. We thus see that if n is the number of one-element orbits in X and α the number of elements of order p in G, we have $n = \alpha + 1$.

Let now m be the number of orbits of order p. As the orbits partition X, we have $n + mp = |X| = |G|^{p-1}$ and then we see that $\alpha + 1 = n = |G|^{p-1} - mp$ is divisible by p

or, equivalently, that $\alpha \equiv -1 \mod p$, as we wanted.

(*ii*) If G is abelian, then there exist positive integers n and $r_1, \dots, r_n$ such that $r_1 \leq \cdots \leq r_n$ and cyclic subgroups $C_1, \dots, C_n$ of orders $p^{r_1}, \dots, p^{r_n}$ such that $G = \prod_{i=1}^{n} C_{p^{r_i}}$. Since G is not cyclic, we have $n \geq 2$. If g_1 and g_2 are generators of C_1 and C_2, then the subgroup $N = (g_1^p) \times (g_2^p) \times \prod_{i=3}^{r} C_i$ is certainly normal in G and $G/N \cong C_1/(g_1^p) \times C_2/(g_2^p)$ is a direct product of two cyclic groups of order p.

We may therefore suppose that G is not abelian. Let P be the set of elements of G of order p, on which the group G acts by conjugation. If $x \in P$ and $G_x = \{g \in G : gx = x\}$ is the stabilizer subgroup of x, then the orbit of x has cardinal equal to the index in $[G : G_x]$ which, as it divides $|G|$, is a power of p. If there were no orbits with one element, then all orbits would therefore have a number of elements divisible by p and, as they partition P, we would have that p divides $|P|$: this is impossible inview of what we proved in (*i*). There exists then a $z \in P$ whose orbit is simply $\{z\}$ and this means precisely that z is central in G. Let $Z = (z)$ be the subgroup generated by z, which is a normal subgroup which is both non-trivial and proper.

The quotient G/Z is a p-group, of course, and it is not cyclic. Indeed, let us suppose that there exists a $g_0 \in G$ whose class g_0Z in G/Z is a generator. If $g \in G$ is an arbitrary element, then the hypothesis implies that there exists an integer r such that $gZ = (g_0Z)^r = g_0^rZ$ in G/Z, and this equality implies in turn that there exists an integer s such that $g = g_p^r z^s$. We see in this way that G is generated by its subset $\{g_0, z\}$: as g_0 and z commute, this is absurd, for G is not abelian.

As $|G/Z| < |G|$, we may assume by induction that there is a normal subgroup N' of G/Z such that $(G/Z)/N' \cong C_p \times C_p$. If now $\pi : G \to G/Z$ is the canonical projection and we put $N = \pi^{-1}(N')$, then $G/N \cong (G/Z)/N' \cong C_p \times C_p$ and we obtain the result we wanted. $\square$

3.7.4. The following beautiful theorem is due to Donald Higman [Hig1954].

Theorem. *Let the characteristic p of the ground field $\Bbbk$ be positive. The group algebra $\Bbbk G$ is of a finite group has finite representation type iff the Sylow p-subgroup of G is cyclic.*

Proof. To be done $\square$

§3.8. An application to Hecke algebras of type A_n

3.8.1. If $\mathcal{O}$ is a commutative ring and $q \in \mathcal{O}^\times$ a unit in $\mathcal{O}$, the ***Hecke algebra of type A_n with coefficients in $\mathcal{O}$ and parameter q*** is the $\mathcal{O}$ algebra $\mathscr{H}(\mathsf{A}_n, \mathcal{O}, q)$ freely generated by letters $s_1, \dots, s_n$ subject to the relations

$$\begin{aligned}
&(s_i - q)(s_i + q^{-1}) = 0, && \text{if } 1 \leq i \leq n;\\
&s_i s_j = s_j s_i, && \text{if } 1 \leq i, j \leq n \text{ and } |i-j| \geq 2;\\
&s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1} && \text{if } 1 \leq i < n.
\end{aligned}$$

3.8.2. This Hecke algebra is closely related to the symmetric group S_{n+1} of degree $n+1$. This becomes clear if we compare its defining presentation with the presentation of S_{n+1} given in the following propositon.

Proposition. *Let $n \geq 1$ and for each $i \in \{1, \dots, n\}$ let $\sigma_i = (i, i+1) \in S_{n+1}$. Then the permutations $\sigma_1, \dots, \sigma_n$ satisfy the relations*

$$\begin{aligned}
&\sigma_i^2 = 1, && \text{if } 1 \leq i \leq n;\\
&\sigma_i \sigma_j = \sigma_j \sigma_i, && \text{if } 1 \leq i, j \leq n \text{ and } |i-j| \geq 2;\\
&\sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1} && \text{if } 1 \leq i < n.
\end{aligned}$$

and this is in fact a presentation for S_{n+1}.

Proof. Let us write G_n the group freely generated by symbols $\sigma_1, \dots, \sigma_n$ subject to the relations given in the statement. There is a morphism of groups $f : G_n \to S_{n+1}$ such that $f(\sigma_i) = (i, i+1)$ for each $i \in \{1, \dots, n\}$, as one can see by a straightforward computation, and this morphism is surjective because the set $\{(i, i+1) : 1 \leq i \leq n\}$ generates S_{n+1}. To prove the proposition, then, it will be enough that we show that G_n has at most $(n+1)!$ elements, for this will imply that f is also injective.

There is a morphism of groups $g : G_{n-1} \to G_n$ such that $g(\sigma_i) = \sigma_i$ for each $i \in \{1, \dots, n-1\}$, whose image K is the subgroup of G_n generated by $\{\sigma_1, \dots, \sigma_{n-1}\}$. If $1 \leq i \leq j \leq n$, we write $\sigma_{i,j} = \sigma_i \sigma_{i+1} \cdots \sigma_j$; we make the convention that if $i > j$ then $\sigma_{i,j}$ denotes the identity element of G_n. Consider the left cosets

$$C_1 = \sigma_{1,n} K, \quad C_2 = \sigma_{2,n} K, \quad \dots, \quad C_n = \sigma_n K, \quad C_{n+1} = K$$

of K in G_n. If $i \in \{1, \dots, n\}$ and $j \in \{1, \dots, n+1\}$, we have

- $\sigma_i C_j = \sigma_i \sigma_{j,n} K = \sigma_{j,n} \sigma_i K = \sigma_{j,n} K = C_j$ if $j > i+1$;
- $\sigma_i C_j = \sigma_i \sigma_{i+1,n} K = \sigma_{i,n} K = C_i$ if $j = i+1$;
- $\sigma_i C_j = \sigma_i \sigma_{i,n} K = \sigma_{i+1,n} K = C_{i+1}$ if $j = i$,
- and, finally, if $i > j$,

$$\begin{aligned}
\sigma_i C_j &= \sigma_i \sigma_{j,n} K = \sigma_i \sigma_{j,i-2} \sigma_{i-1} \sigma_i \sigma_{i+1,n} K = \sigma_{j,i-2} \sigma_i \sigma_{i-1} \sigma_i \sigma_{i+1,n} K\\
&= \sigma_{j,i-2} \sigma_{i-1} \sigma_i \sigma_{i-1} \sigma_{i+1,n} K = \sigma_{j,i-2} \sigma_{i-1} \sigma_i \sigma_{i+1,n} \sigma_{i-1} K = \sigma_{j,n} K = C_j.
\end{aligned}$$

We thus see that $\sigma_i C_j = C_{f(\sigma_i)(j)}$ and that the set $\mathscr{C} = \{C_1, \dots, C_{n+1}\}$ is closed under left multiplication by elements of G_n. This implies that $\mathscr{C}$ is in fact the set of *all* cosets of K in G_n, so that in particular we have $[G_n : K] \leq n + 1$.

If we assume now inductively that $G_{n-1} \cong S_n$, then $|K| \leq |S_n| = n!$ and therefore

$$|G_n| = [G_n : K]\,|K| \leq (n+1)n! = (n+1)!,$$

which is what we set out to prove. □

3.8.3. It follows from the proof of this proposition that that

$$\text{every element } w \text{ of } S_{n+1} \text{ is equal to one of the form } \sigma_{i,n}w' \text{ with } 1 \leq i \leq n+1 \text{ and } w' \in S_n. \tag{21}$$

We say that a word w in the generators of S_{n+1} is a ***standard word*** if it is of the form $\sigma_{i,n}w'$ with $i \in \{1, \dots, n+1\}$ and w' a standard word in S_n. The observation (21) used recursively implies that every element of S_{n+1} is equal to a standard word. Since there are $(n+1)!$ standard words in the generators of S_{n+1}, the obvious function from standard words to elements of S_{n+1} is in fact a bijection.

3.8.4. We extend this definition of standard words to words in the generators $s_1, \dots, s_n$ of the algebra $\mathscr{H}(\mathsf{A}_n, \mathcal{O}, q)$.

Proposition. *Let $\Bbbk$ be a field and q a variable, so that we can consider the ring of Laurent polynomials $\Bbbk[q^{\pm 1}]$. The set of standard words of $\mathscr{H}(\mathsf{A}_n, \Bbbk[q^{\pm 1}], q)$ is a $\Bbbk[q^{\pm 1}]$-basis.*

Proof. Let us write $\mathscr{H}_n$ instead of $\mathscr{H}(\mathsf{A}_n, \Bbbk[q^{\pm 1}], q)$. There is a morphism of $\Bbbk[q^{\pm 1}]$-algebras $f : \mathscr{H}_{n-1} \to \mathscr{H}_n$ such that $f(s_i) = s_i$ for each $i \in \{1, \dots, n-1\}$ and whose image is the subalgebra of $\mathscr{H}_n$ generated by $\{s_1, \dots, s_{n-1}\}$.

We start with the observation that

$$\mathscr{H}_n \text{ is spanned as a } \Bbbk[q^{\pm 1}]\text{-module by words in the generators containing at most once instance of } s_n. \tag{22}$$

To prove it, it is enough that we show that every word of the form $s_n w s_n$, with w a word in the generators $s_1, \dots, s_{n-1}$, is equal in $\mathscr{H}_n$ to a $\Bbbk[q^{\pm 1}]$-linear combination of words containg s_n a most once. If in that situation the generator s_{n-1} does not appear in w, we have that $s_n w s_n = w s_n^2 = (q - q^{-1}) w s_n + w$, and s_n appears at most once in each word in the last member of this equality.

Suppose now that s_{n-1} does appear in w. Proceeding by induction and since w is in the image of the morphism f, we may assume that s_{n-1} appears exactly once in w, so that $w = w' s_{n-1} w''$ with w' and w'' words in the generators $s_1, \dots, s_{n-2}$. Then we have

$$s_n w s_n = s_n w' s_{n-1} w'' s_m = w' s_n s_{n-1} s_m w'' = w' s_{n-1} s_n s_{n-1} w''$$

and this last word has exactly one occurrence of s_n. This completes the proof of (22)

Let now Σ_n be the $\Bbbk[q^{\pm 1}]$-linear span of the set of standard words in $\mathscr{H}_n$; since the morphism f maps standard words to standard words, we have $f(\Sigma_{n-1}) \subseteq \Sigma_n$. We want to show that Σ_n is in fact equal to $\mathscr{H}_n$ and, in view of (22), for this it is enough to show that every word in $\mathscr{H}_n$ involving at most one occurrence of s_n is in Σ_n.

Consider first a word u in $\mathscr{H}_n$ which does not involve s_n. It is then in the image of the morphism f which, by induction, is equal to $f(\Sigma_{n-1})$, and since this is contained in Σ_n, we see that $u \in \Sigma_n$.

Suppose next that u is a word in $\mathscr{H}_n$ in which s_n occurs once, so that $u = w' s_n w''$ with w' and w'' words in the generators $s_1, \ldots, s_{n-1}$. As w' is in the image of the morphism f, we can assume inductively that it is a standard word in the generators $s_1, \ldots, s_{n-1}$, that is, that $u = s_{i,n-1} v$ for some $i \in \{1, \ldots, n\}$ and some standard word v in the generators $s_1, \ldots, s_{n-2}$, and then

$$u = w' s_n w'' = s_{i,n-1} v s_n w'' = s_{i,n} v w''.$$

Now vw'' is in the image of f, so it is equal to a $\Bbbk[q^{\pm 1}]$-linear combination of standard words in the generators $s_1, \ldots, s_{n-1}$. This shows that $u \in \Sigma_n$, as we wanted.

Finally, we have to how that the standard words are linearly independent over $\Bbbk[q^{\pm}]$ in $\mathscr{H}_n$. First, notice that if σ is an element of the symmetric group S_{n+1}, there is a unique standard word in the generators $\sigma_1, \ldots, \sigma_n$ which is equal to σ, and then we can consider the corresponding standard word w_σ in $\mathscr{H}_n$. All standard words of $\mathscr{H}_n$ are obtained in this way and exactly for one σ. To show the linear independence of the standard words, let us suppose that there exists a relation of linear dependence

$$\sum_{\sigma \in S_{n+1}} c_\sigma w_\sigma = 0 \tag{23}$$

in which $c_\sigma \in \Bbbk[q^{\pm 1}]$ for each $\sigma \in S_{n+1}$ and show that all the c_σ are necessarily zero. Let us suppose that this is not the case and, as we may without losing generality, that the coefficients c_σ have no non-trivial common divisor in $\Bbbk[q^{\pm 1}]$.

There is a morphism of $\Bbbk$-algebras $\varepsilon : \Bbbk[q^{\pm 1}] \to \Bbbk$ such that $\varepsilon(q) = 1$; if $c \in \Bbbk[q^{\pm 1}]$ is a Laurent polynomial, then $\varepsilon(c) = c(1)$, the evaluation of c at 1. This morphism ε allows us to view the $\Bbbk$-algebra $\Bbbk S_{n+1}$ as a $\Bbbk[q^{\pm 1}]$-algebra, and using this structure we can see that there is a morphism $\bar{\varepsilon} : \mathscr{H}_n \to \Bbbk S_{n+1}$ of $\Bbbk[q^{\pm 1}]$-algebras such that $\bar{\varepsilon}(s_i) = \sigma_i$ for each $i \in \{1, \ldots, n\}$: this follows immediately from Proposition 3.8.2 and the defining presentation of $\mathscr{H}_n$. In particular, applying the map $\bar{\varepsilon}$ to both sides of the equality (23) we find that

$$\sum_{\sigma \in S_{n+1}} c_\sigma(1) \sigma = 0$$

and since S_{n+1} is a $\Bbbk$-basis for $\Bbbk S_{n+1}$, this tells us that $c_\sigma(1) = 0$ for all $\sigma \in S_{n+1}$. This is absurd since it implies that $q - 1$ is a divisor of all the coefficients c_σ, contradicting our assumption. This completes the proof of the proposition. □

3.8.5. Theorem. *Let $\Bbbk$ be a field of characteristic zero.*

(*i*) *For all $q \in \Bbbk$ except a finite number of exceptions, all of which are algebraic over the prime field of $\Bbbk$, the $\Bbbk$-algebra $\mathscr{H}(\mathsf{A}_n, \Bbbk, q)$ is a semisimple.*

(*ii*) *If q is a variable and $\Bbbk(q)$ is the field of rational functions in q with coefficients in $\Bbbk$, then the $\Bbbk(q)$-algebra $\mathscr{H}(\mathsf{A}_n, \Bbbk(q), q)$ is semisimple.*

Proof. To be done □

§3.9. Exercises

3.9.1. Let $\Bbbk$ be a field of characteristic zero and let us write $\mathscr{H}_n$ for the $\Bbbk(q)$-algebra $\mathscr{H}(\mathsf{A}_n, \Bbbk(q), q)$. It follows from the proof of Proposition 3.8.4 that the we can view $\mathscr{H}_{n-1}$ as a subalgebra of $\mathscr{H}_n$.

(*i*) Find all the one-dimensional $\mathscr{H}_n$-modules.

(*ii*) Let S be a one-dimensional $\mathscr{H}_{n-1}$-module. Viewing $\mathscr{H}_n$ as an $(\mathscr{H}_n, \mathscr{H}_{n-1})$-bimodule in the natural way, we may consider the $\mathscr{H}_n$-module $V_n = \mathscr{H}_n \otimes_{\mathscr{H}_{n-1}} S$. For each $i \in \{1, \dots, n+1\}$ let $v_i = s_{i,n} \otimes 1 \in V$. Show that the set $\mathscr{B} = \{v_1, \dots, v_{n+1}\}$ is an ordered basis for V_n, find the matrices describing the action of the generators of $\mathscr{H}_n$ on V_n with respect to this basis, and decompose V_n as a direct sum of simple submodules.

3.9.2. Let $\mathcal{O}$ be a commutative ring and $q \in \mathcal{O}$ is an invertible element. If p is a positive integer, then ***Hecke algebra of type $\mathsf{I}_2(p)$ with coefficients in $\mathcal{O}$ and parameter q*** is the $\mathcal{O}$-algebra $\mathscr{H}(\mathsf{I}_2(p), \mathcal{O}, q)$ freely generated by letters s_1 and s_2 subject to the relations

$$(s_i - q)(s_i + q^{-1}) = 0, \qquad \text{for each } i \in \{1, 2\}$$

and

$$\underbrace{s_1 s_2 s_1 \cdots}_{p \text{ factors}} = \underbrace{s_2 s_1 s_2 \cdots}_{p \text{ factors}}.$$

Show that if $\Bbbk$ is a field of characteristic zero, then the $\Bbbk$-algebra $\mathscr{H}(\mathsf{I}_2(p), \Bbbk, \varepsilon)$ is semisimple for almost all $\varepsilon \in \Bbbk$ and if q is a variable the $\Bbbk(q)$-algebra $\mathscr{H}(\mathsf{I}_2(p), \Bbbk(q), q)$ is semisimple. Describe the simple $\mathscr{H}(\mathsf{I}_2(3), \Bbbk(q), q)$-modules and find their multiplicities as direct summands of the regular module.

3.9.3. Characters en semisimple

CHAPTER 4

The radical of algebras and modules

§4.1. The socle and the radical of a module

4.1.1. If M is a module, the ***socle*** of M is the sum $\operatorname{soc} M$ of all simple submodules of M.

4.1.2. Proposition. *Let M be a module.*

(*i*) *The socle of M is the unique maximal semisimple submodule of M.*

(*ii*) *The module M is semisimple iff $M = \operatorname{soc} M$.*

(*iii*) *We have $\operatorname{soc}(\operatorname{soc} M) = \operatorname{soc} M$.*

(*iv*) *If $f : M \to N$ is a morphism of modules, then $f(\operatorname{soc} M) \subseteq \operatorname{soc} N$.*

Proof. It is clear that $\operatorname{soc} M$ is a semisimple submodule of M. On the other hand, if N is a semisimple submodule of M, it is a sum of simple submodules of M and we then have $N \subseteq \operatorname{soc} M$, since $\operatorname{soc} M$ is the sum of *all* simple submodules of M. This proves (*i*).

The claim of (*ii*) is actually a restatement of the definition of semisimplicity, and that of (*iii*) follows at once from (*i*) and (*ii*). Finally, if $f : M \to N$ is a morphism of modules, the submodule $f(\operatorname{soc} M)$ of N is semisimple —because it the sum of the images of the simple submodules of M under f, which are either zero or simple submodules of N— so that it is contained in $\operatorname{soc} M$ by (*i*). □

4.1.3. The socle is always non-trivial:

Proposition. *If M is a non-zero module, then $\operatorname{soc} M \neq 0$.*

Proof. Indeed, if a module M is non-zero, then it contains non-zero submodules and any one of these of minimal dimension is simple, so contained in $\operatorname{soc} M$. □

4.1.4. This non-triviality has a very useful corollary:

Corollary. *A morphism $f : M \to N$ of modules is injective iff its restriction $f|_{\operatorname{soc} M}$ is injective.*

Proof. The necessity of the condition is obvious. On the other hand, if f is not injective, then $\ker f$ is a non-zero submodule of M and Proposition 4.1.3 tells us that $\operatorname{soc}(\ker f) \neq 0$. Since $\operatorname{soc}(\ker f)$ is a semisimple submodule of M, it is contained in $\operatorname{soc} M$ and, therefore, equal to the kernel of the restriction $f|_{\operatorname{soc} M}$, which is then also not injective. □

4.1.5. If M is a module, the ***radical*** of M is the intersection $\operatorname{rad} M$ of all maximal submodules of M, if there are any, and M in any other case. Since our modules are all finite-dimensional, this second case occurs only when $M = 0$.

4.1.6. Proposition. *Let M be a module.*

(*i*) *If M is a simple module, then* $\operatorname{rad} M = 0$.

(*ii*) *If $N \subseteq M$ is a submodule and* $\operatorname{rad} M/N = 0$, *then* $\operatorname{rad} M \subseteq N$.

(*iii*) *We have* $\operatorname{rad}(M/\operatorname{rad} M) = 0$.

Proof. (*i*) If M is simple, the zero submodule is the unique maximal submodule.

(*ii*) Let $m \in M \setminus N$. As $m + N \notin \operatorname{rad} M/N$, there exists a maximal submodule P of M/N such that $m + N \notin P$. If $p : M \to M/N$ is the canonical projection, then $p^{-1}(P)$ is a maximal submodule of M and clearly $m \notin p^{-1}(P)$. It follows that $m \notin \operatorname{rad} M$.

(*iii*) Let $x \in M/\operatorname{rad} M$ be a non-zero element, so that there exists an $m \in M \setminus \operatorname{rad} M$ with $x = m + \operatorname{rad} M$. As m is not in $\operatorname{rad} M$, there exists a maximal submodule $N \subseteq M$ such that $m \notin N$. Since N is maximal in M, the quotient M/N is simple and, according to (*i*), we have $\operatorname{rad} M/N = 0$, so that $\operatorname{rad} M \subseteq N$ by (*ii*). Now $N/\operatorname{rad} M$ is a maximal submodule of M/N and $x \notin N/\operatorname{rad} M$, so we see that $x \notin \operatorname{rad}(M/\operatorname{rad} M)$. □

4.1.7. Proposition. *A module M is semisimple iff* $\operatorname{rad} M = 0$.

Proof. Suppose first that M is semisimple, so that there is a family $(S_i)_{i \in I}$ of submodules of M such that $M = \bigoplus_{i \in I} S_i$. If $j \in I$, then the submodule $N_j = \bigoplus_{i \in I \setminus \{j\}} S_i$ is maximal in M, since M/N_j is clearly isomorphic to S_j. As we have $\operatorname{rad} M \subseteq \bigcap_{j \in I} N_j = 0$, we see that the condition is necessary.

To prove the converse, suppose that $\operatorname{rad} M = 0$. If $M = 0$, then M is trivially semisimple, so we may assume that that is not the case. The set $\mathscr{N}$ of all maximal submodules of M is therefore not empty. Since M is finite-dimensional, there exist $N_1, \dots, N_r \in \mathscr{N}$ such that $N = \bigcap_{i=1}^r N_i$ has minimal dimension among all the intersections of finite subsets of $\mathscr{N}$. We must have $N = 0$. Indeed, if we had $n \in N \setminus 0$ then, as $n \notin \operatorname{rad} M$, there would be a maximal submodule $N' \in \mathscr{N}$ such that $n \notin N'$ and, consequently, $N' \cap N \subsetneq N$: this is absurd since $N' \cap N$ is the intersection of the finite subset $\{N_1, \dots, N_r, N'\}$ of $\mathscr{N}$.

The fact that $\bigcap_{i=1}^r N_i = 0$ implies at once that the morphism $p : M \to \bigoplus_{i=1}^r M/N_i$ such that $p(m) = (m + N_1, \dots, m + N_r)$ for all $m \in M$ is injective. It follows from this that M is isomorphic to a submodule of the semisimple module $\bigoplus_{i=1}^r M/N_i$ and, in view of Corollary 2.2.5, that it is semisimple itself. □

4.1.8. Corollary. *The radical of a module M is the smallest submodule N of M such that the quotient M/N is semisimple.*

Proof. Since we know that $\operatorname{rad}(M/\operatorname{rad} M) = 0$ from part (*iii*) of Proposition 4.1.6, it follows from Proposition 4.1.7 that the quotient $M/\operatorname{rad} M$ is semisimple. On the other hand, if $N \subseteq M$ is a submodule such that M/N is semisimple, Proposition 4.1.7

tells us that $\mathsf{rad}(M/N) = 0$, so that $\mathsf{rad}\, M \subseteq N$ by part (*ii*) of Proposition 4.1.6. $\square$

4.1.9. Proposition. *If $f : M \to N$ is a morphism of modules, then $f(\mathsf{rad}\, M) \subseteq \mathsf{rad}\, N$.*

Proof. Let P be a maximal ideal of N. The map f induces an injective morphism $M/f^{-1}(P) \to N/P$ of modules. As N/P is simple, this means that the quotient $M/f^{-1}(P)$ is either zero or simple, so that $f^{-1}(P)$ is either equal to M or a maximal submodule of M. In any case, we see that $\mathsf{rad}\, M \subseteq f^{-1}(P)$ and, therefore, that $f(\mathsf{rad}\, M) \subseteq P$. Since $\mathsf{rad}\, N$ is the intersection of all maximal submodules of N and since $f(\mathsf{rad}\, M)$ is contained in each of them, we can conclude that $f(\mathsf{rad}\, M) \subseteq \mathsf{rad}\, N$, as we want. $\square$

§4.2. The radical of an algebra

4.2.1. It is an immediate consequence of Proposition 4.1.7 that a necessary and sufficient condition for an algebra A to be semisimple is that its left ideal $\mathsf{rad}\, A$, the radical of the regular module, be zero. That ideal, then, measures in a way the non-semisimplicity of the algebra.

4.2.2. Proposition. *The radical of an algebra is a proper bilateral ideal*

Proof. Let A be an algebra. It is clear that $\mathsf{rad}\, A$ is a left ideal of A and it is a proper one because A does have maximal left ideals. If $b \in A$, the function $f : a \in A \mapsto ab \in A$ is a morphism of left A-modules, so Proposition 4.1.9 tells us that

$$(\mathsf{rad}\, A)b = f(\mathsf{rad}\, A) \subseteq \mathsf{rad}\, A.$$

This means that $\mathsf{rad}\, A$ is also a right ideal. $\square$

4.2.3. Proposition. *If A is an algebra, then $A/\mathsf{rad}\, A$ is a semisimple algebra.*

Notice that the statement of this proposition makes sense precisely because $\mathsf{rad}\, A$ is a bilateral ideal of A.

Proof. We know that the radical of the left A-module $A/\mathsf{rad}\, A$ is zero from part (*iii*) of Proposition 4.1.6. As the $A/\mathsf{rad}\, A$-submodules of $A/\mathsf{rad}\, A$ coincide with its A-submodules, the radical of $A/\mathsf{rad}\, A$ as a module over itself is also zero, so that $A/\mathsf{rad}\, A$ is a semisimple $A/\mathsf{rad}\, A$-module, by Proposition 4.1.7, and therefore $A/\mathsf{rad}\, A$ a semisimple algebra. $\square$

4.2.4. Proposition. *If A is an algebra and M an A-module, then $\mathsf{rad}\, M = (\mathsf{rad}\, A)M$.*

Proof. If $m \in \mathsf{rad}\, M$, the function $f : a \in A \mapsto am \in M$ is a morphism of A-modules, so Proposition 4.1.9 tells us that $(\mathsf{rad}\, A)m = f(\mathsf{rad}\, A) \subseteq \mathsf{rad}\, M$. It follows from this that $(\mathsf{rad}\, A)M \subseteq M$. Conversely, the quotient $M/(\mathsf{rad}\, A)M$ is an $A/\mathsf{rad}\, A$-module in an obvious way and —since $A/\operatorname{rad} A$ is a semisimple algebra— a semisimple one. The A-submodules of $M/(\operatorname{rad} A)M$ coincide with the $A/\operatorname{rad} A$-submodules, so $M/(\operatorname{rad} A)M$ is also a semisimple A-module. Corollary 4.1.8 then tells us that $(\operatorname{rad} A)M \subseteq \operatorname{rad} M$. $\square$

4.2.5. The following result is usually known as Nakayama's Lemma.

Proposition. *Let M be a module and let $P \subsetneq M$ be a proper submodule. The following two statements are equivalent:*

(*a*) *If N is a submodule of M such that $P + N = M$, then $N = M$.*

(*b*) *The submodule P is contained in* $\operatorname{rad} M$.

Proof. Notice that since P is a proper submodule of M we have $M \neq 0$.

(*a*) $\Rightarrow$ (*b*) If N is a maximal submodule of M and $P \not\subseteq N$, then $N + P = M$ so that the hypothesis tells is that $N = M$, which is absurd. It follows that P is contained in every maximal submodule of M and, then, in $\operatorname{rad} M$.

(*b*) $\Rightarrow$ (*a*) Let us start by proving that

$$\text{if } r \in \operatorname{rad} A \text{ and } N \text{ is a submodule of } M \text{ such that } Ar + N = M, \text{ then } N = M. \tag{24}$$

Suppose there are $r \in \operatorname{rad} M$ and a proper submodule N of M such that $Ar + N = M$. Since N is properly contained in M, there exists a maximal submodule N' of M such that $N' \supseteq N$ and, since $r \in \operatorname{rad} M \subseteq N'$, we have $M = Ar + N \subseteq N'$: this is absurd.

Let us now prove the desired implication. Let P be submodule of M contained in $\operatorname{rad} M$ and let N be another submodule such that $P + N = M$. Since M is finite-dimensional, there exist a non-negative integer n and $r_1, \ldots, r_n \in P$ such that $P = \sum_{i=1}^{n} Ar_i$, and since $P \subseteq \operatorname{rad} M$ we have $r_i \in \operatorname{rad} M$ for all $i \in \{1, \ldots, r\}$. We may proceed by induction on the number r, assuming that what we want to prove is true when P can be generated by less that r elements, after noting that when $r = 0$ there is nothing to prove. Now, we have $P + N = Ar_1 + \sum_{i=2}^{r} Ar_i + N = M$ and r_1 is in $\operatorname{rad} M$, so we have that $\sum_{i=2}^{r} Ar_i + N = M$ in view of (24). Using the induction hypothesis, then, we conclude at once that $N = M$. $\square$

4.2.6. An immediate corollary of this result is the following special case, which is the most often used form of Nakayama's Lemma.

Corollary. *If M is a module such that $(\operatorname{rad} A)M = M$, then $M = 0$.*

Proof. This is the implication (*b*) $\Rightarrow$ (*a*) of Proposition 4.2.5 in the case where $N = 0$ and $P = (\operatorname{rad} A)M$. $\square$

4.2.7. The radical of an algebra is in fact the largest ideal with the property stated in Proposition 4.2.5: this follows from the equivalence of the first two statements in the following proposition.

Proposition. *If I is a left ideal in the algebra A, then the following statements are equivalent:*

(*a*) *I is contained in* $\operatorname{rad} A$.

(*b*) *If N is a submodule of M such that $N + IM = M$, then $N = M$.*
(*c*) *If $x \in I$, then $1 + x$ is a unit of A.*

Proof. The implication (*a*) $\Rightarrow$ (*b*) follows from Propositions 4.2.4 and 4.2.5.

To prove that (*b*) $\Rightarrow$ (*c*), let us fix $x \in I$. Since $A(1+x) + I = A$, the hypothesis implies that $A(1+x) = A$ and, then, that there exists a $y \in A$ such that $1 = y(1+x)$. Notice that $y = 1 - yx$, so $Ay + I = A(1 - yx) + I = A$ and the hypothesis again tells us that $Ay = A$, so there is a $z \in A$ such that $zy = 1$. It follows that $1 + x$ has a left-inverse who has itself a left-inverse, so that $1 + x$ is in fact invertible.

Finally, suppose that (*c*) holds, let $x \in I$ and, to reach a contradiction, assume that $x \notin \operatorname{rad} A$, so that there is a maximal left ideal J in A such that $x \notin J$. Then $Ax + J = A$ and there exist $a \in A$ and $y \in J$ such that $ax + y = 1$. As $y = 1 + (-ax)$ and $-ax \in I$, the hypothesis tells us that y is a unit of A, and this is impossible because the ideal J, which contains it, is proper. This proves (*i*). □

4.2.8. Using Proposition 4.2.7 we can easily show that the asymmetry incurred in defining the radical of an algebra as the intersection of its maximal left ideals is only apparent.

Corollary. *The radical of an algebra A is equal to the intersection of the maximal* right *ideals of A.*

Proof. We know from Proposition 4.2.2 that $\operatorname{rad} A$ is a right ideal and from Proposition 4.2.7 that $1 + x$ is a unit of A for all $x \in \operatorname{rad} A$. It follows the from the right version of Proposition 4.2.7 that $\operatorname{rad} A$ is contained in the radical of A viewed as a *right* module over itself. Symmetry then implies that the two radicals are in fact equal and this is what the corollary asserts. □

4.2.9. Corollary. *We have* $\operatorname{rad} A = \{x \in A : 1 + yx \text{ is a unit for all } y \in A\}$.

Proof. That $\operatorname{rad} A$ is contained in the set described in the statement follows from the implication (*a*) $\Rightarrow$ (*c*) of Proposition 4.2.7. Conversely, if $x \in A$ is such that $1 + yx$ is a unit for all $y \in A$, then $1 + z$ is a unit for all z in the left ideal Ax, and the implication (*c*) $\Rightarrow$ (*a*) of that proposition tells us that $x \in Ax \subseteq \operatorname{rad} A$. □

4.2.10. A left, right or bilateral ideal in an algebra is ***nil*** if all its elements are nilpotent

Corollary. *The radical of an algebra contains every nil left ideal.*

Proof. Let A be an algebra, let I be a nil left ideal of A and let $x \in I$. There exists a positive integer k such that $x^{k+1} = 0$, so that $1 + x$ is a invertible in A with inverse $\sum_{i=0}^{k} x^i$. It follows from Corollary 4.2.9 that $x \in \operatorname{rad} A$. □

4.2.11. We are in position to prove a very useful criterion to recognize the radical of an algebra:

Proposition. *The radical of an algebra A is a nilpotent ideal. It is in fact the unique nil ideal I of A such that A/I is semisimple.*

This tells us that every element of the radical of A is nilpotent. In general, it is not true, though, that every nilpotent element of A is in the radical.

Proof. Since we have a decreasing chain of ideals

$$\operatorname{rad} A \supseteq (\operatorname{rad} A)^2 \supseteq (\operatorname{rad} A)^3 \supseteq \cdots$$

and A has finite dimension, there exists a positive integer k such that the left ideal $P = (\operatorname{rad} A)^k$ is such that $P = (\operatorname{rad} A)P$. According to Corollary 4.2.6, then, we have $P = 0$, so that $\operatorname{rad} A$ is nilpotent. On the other hand, we know from Proposition 4.2.3 that the quotient algebra $A/\operatorname{rad} A$ is semisimple.

Suppose now that I is a nil ideal of A such that A/I is a semisimple algebra. This means that the radical of A/I as an A/I-module vanishes, and since that radical coincides with it radical viewed as an A-module, we have $\operatorname{rad}(A/I) = 0$, so that $\operatorname{rad} I \subseteq A$. On the other hand, since I is nil Corollary 4.2.10 tells us that $I \subseteq \operatorname{rad} A$. □

4.2.12. Corollary.

(*i*) *If $f : A \to B$ is a surjective morphism of algebras, then $f(\operatorname{rad} A) \subseteq \operatorname{rad} B$.*

(*ii*) *If A and B are algebras, then $\operatorname{rad}(A \times B) = \operatorname{rad} A \times \operatorname{rad} B$.*

Proof. (*i*) Since f is surjective, $f(\operatorname{rad} A)$ is an ideal of B. It is nilpotent, since $\operatorname{rad} A$ is nilpotent, and the quotient $B/f(\operatorname{rad} B)$, being isomorphic to $A/\operatorname{rad} A$, is semisimple. It follows from Proposition 4.2.11 that $f(\operatorname{rad} A) = \operatorname{rad} B$.

(*ii*) The ideal $\operatorname{rad} A \times \operatorname{rad} B$ of the direct product $A \times B$ is nilpotent and, since there is an obvious isomophism of algebras

$$\frac{A \times B}{\operatorname{rad} A \times \operatorname{rad} B} \cong \frac{A}{\operatorname{rad} A} \times \frac{B}{\operatorname{rad} B},$$

the quotient $(A \times B)/(\operatorname{rad} A \times \operatorname{rad} B)$ is semisimple. The result follows then from Proposition 4.2.11 □

§4.3. Examples

Group algebras

4.3.1. The following result is due to Wallace [Wal1961].

Proposition. *Suppose that the characteristic p of the ground field $\Bbbk$ is positive and let G be a finite group. If G has a* normal *Sylow p-subggroup P, then the radical of the group algebra $\Bbbk G$ is*

$$\operatorname{rad} \Bbbk G = \sum_{x \in P \setminus \{1\}} \Bbbk G(x-1)$$

and we have $\Bbbk G/\operatorname{rad} \Bbbk G \cong \Bbbk(G/P)$.

In the general case, the determination of the radical of the group algebra is a notoriously difficult problem and it remains open. The monograph by Gregory Karpilovsky [Kar] is a systematic yet not exhaustive exposition on the subject.

Proof. To be done □

4.3.2. In the situation of the proposition, if X is a subset of P which generates it as a group, then $\operatorname{rad} G = \sum_{x \in X} \Bbbk G(x-1)$.

4.3.3. Corollary. *Suppose that the characteristic p of the ground field $\Bbbk$ is positive. If G is a finite p-group and $\varepsilon : \Bbbk G \to \Bbbk$ is the unique morphism of algebras such that $\varepsilon(g) = 1$ for all $g \in G$, then $\operatorname{rad} \Bbbk G = \ker \varepsilon$.*

Proof. To be done □

Incidence algebras

4.3.4. Let P be a finite poset with order relation $\preceq$, and let $R = \{(i, j) \in P \times P : i \preceq j\}$. For each $(i, j) \in R$ we consider a symbol $x_{i,j}$ and assume that $x_{i,j} = x_{i',j'}$ iff $(i, j) = (i', j')$. The ***incidence algebra*** of the poset P is the algebra $\Bbbk P$ which has the set $\{x_{i,j} : (i, j) \in R\}$ as basis and whose multiplication is such that whenever $(i, j), (k, l) \in R$ we have

$$x_{i,j} \cdot x_{k,l} = \begin{cases} x_{i,l}, & \text{if } j = k, \\ 0, & \text{in any other case.} \end{cases}$$

It is easy to verify that this is indeed a unitary algebra, whose unit element is $\sum_{i \in P} x_{i,i}$.

4.3.5. If n is a positive integer, let T_n be the subalgebra of $M_n(\Bbbk)$ of upper triangular matrices.

Proposition. *Every subalgebra of T_n which is spanneed as a vector space by unit matrices is isomorphic to the incidence algebra of a poset. Conversely, the incidence algebra of a finite poset is isomorphic to such a subalgebra, with $n = |P|$.*

Proof. Let A be subalgebra of T_n spanned by unit matrices, let $P = \{1, \dots, n\}$ and consider the set $R = \{(i, j) \in I \times I : e_{i,j} \in A\}$. The hypothesis implies at once that the set $S = \{e_{i,j} : (i, j) \in R\}$ spans A as a vector space and, since this set is linearly independent, it is in fact a basis of A. The only way of writing the identity matrix as a sum of unit matrices is $\sum_{i \in P} e_{i,i}$, and since it belongs to A we must have $(i, i) \in R$ for all $i \in P$. This means that P, viewed as a relation on the set P, is reflexive. Since $A \subseteq T_n$ we have that $i \leq j$ for all $(i, j) \in R$, and this implies at once that R is an anti-symmetric relation. Finally, if $i, j, k \in P$ are such that (i, j) and (j, k) are in R, so that $e_{i,j}, e_{j,k} \in A$, then $e_{i,k} = e_{i,j} e_{j,k} \in A$ and $(i, j) \in R$: this tells us that P is transitive. We thus see that R is an order relation on P and we can consider the corresponding incidence algebra $\Bbbk P$.

As the set S is a basis for A, there exists a linear function $f : A \to \Bbbk P$ such that $f(e_{i,j}) = x_{i,j}$ for all $(i, j) \in R$. This function maps the basis S of A bijectively only a basis of $\Bbbk P$, so it is an isomorphism, and a immediate verification shows that it is multiplicative: it is therefore an isomorphism of algebras.

To prove the converse, let now P be a finite poset with order $\preceq$. Let $n = |P|$ and put $I = \{1, \dots, n\}$. We claim that

$$\text{\textit{there is a bijection } } \phi : I \to P \text{ \textit{such that for all} } i, j \in I \text{ \textit{we have} } i \leq j \text{ \textit{if} } \phi(i) \preceq \phi(j). \tag{25}$$

We prove this by induction on n. If $n = 1$, then the unique function $\phi : \{1\} \to P$ satisfies the condition. Suppose then that $n > 1$. Since P is finite, there exists a maximal element p in P. If we consider the set $P \setminus \{p\}$ as a poset with the order induced from that of P, we know inductively that there is a bijection $\phi' : \{1, \dots, n-1\} \to P \setminus \{p\}$ such that for all $i, j \in \{1, \dots, n-1\}$ we have $i \leq j$ if $\phi'(i) \preceq \phi'(j)$. We define a function $\phi : I \to P$ so that $\phi(i) = \phi'(i)$ if $i \in \{1, \dots, n-1\}$ and $\phi(n) = p$. A simple verification shows that ϕ has the desired property.

Let now $S = \{e_{i,j} \in M_n(\Bbbk) : i, j \in I, \phi(i) \preceq \phi(j)\}$, a linearly independent set. It follows immediately from (25) that S is contained in the triangular matrix algebra T_n, so the same is true of the subspace A spanned by S. Suppose that i, j, k, $l \in I$ are such that $e_{i,j}$, $e_{k,l} \in S$, so that $\phi(i) \preceq \phi(j)$ and $\phi(k) \preceq \phi(l)$. If $j = k$, transitivity implies that $\phi(i) \preceq \phi(l)$ and then $e_{i,k} = e_{i,j}e_{k,l}$ is in A; if instead $j \neq k$ we have that $e_{i,j}e_{k,l} = 0$, which is again in A. We thus see that A is closed under multiplication in T_n. Finally, as $\phi(i) \preceq \phi(i)$ for all $i \in I$, we have $1 = \sum_{i=1}^{n} e_{i,i} \in A$, and A is therefore a subalgebra of T_n —and it is spanned by unit matrices by construction. As the map $f : \Bbbk P \to A$ such that $f(x_{i,j}) = e_{i,j}$ is, just as in the first part, an isomorphism of algebras, this completes the proof of the proposition. $\square$

4.3.6. If the poset P is the set $\{1, \dots, n\}$ with its usual order, then we can take as bijection ϕ in (25) the identity function and the subalgebra A constructed in the proof of this proposition is the full algebra T_n of upper triangular matrices. If instead P is the poset whose Hasse diagram is the one appearing here on the left

$$\begin{tikzcd}
& 6 \arrow[d, dash] & \\
& 5 \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
2 \arrow[dr, dash] & 3 \arrow[d, dash] & 4 \arrow[dl, dash] \\
& 1 &
\end{tikzcd}
\qquad\qquad
\begin{pmatrix}
* & * & * & * & * & * \\
0 & * & 0 & 0 & * & * \\
0 & 0 & * & 0 & * & * \\
0 & 0 & 0 & * & * & * \\
0 & 0 & 0 & 0 & * & * \\
0 & 0 & 0 & 0 & 0 & *
\end{pmatrix}$$

is the set of matrice in $M_6(\Bbbk)$ which have zeroes in the marked positions in tthe matrix on the right.

4.3.7. Proposition. *If P is a finite poset, the radical of the incidence algebra $\Bbbk P$ is spanned as a vector space by the set $\{x_{i,j} : i, j \in P, i \precneq j\}$.*

Proof. Let $n = |P|$. If $(i, j) \in R$, we let $d(i, j)$ be the maximal integer non-negative k such that there exist a sequence $i_0, \dots, i_k \in I$ such that $i_0 = i$, $i_k = j$ and for all $t \in \{1, \dots, k-1\}$ we have $i_t \lneq i_{t+1}$; in such a sequence we have $i_s \neq i_t$ if $s, t \in \{0, \dots, k\}$ and $s \neq t$, and it follows from this that $d(i, j) < n$. Clearly, given $(i, j) \in R$ we have $d(i, j) = 0$ iff $i = j$, so that $d(i, j) \geq 1$ iff $i \lneq j$. On the other hand, if i, j, $k \in P$ are such that (i, j), $(j, k) \in R$, then $d(i, k) \geq d(i, j) + d(j, k)$.

If k is a non-negative integer, we let I_k be the subspace of the incidence algebra $\Bbbk P$ spanned by the set $R_k = \{x_{i,j} : i, j \in P, d(i, j) \geq k\}$. We claim that I_1 is an ideal of $\Bbbk P$ and that for all non-negative integers r we have $I_1^r \subseteq I_r$. This implies at once that I_1 is a nilpotent ideal, for $I_1^n \subseteq I_n = 0$ since $R_n = \emptyset$.

Let $(i, j) \in R_1$ and $(k, l) \in R$. If $j = k$, then $x_{i,j}x_{k,l} = x_{i,l}$ and this is in I_1 because $i \lneq j \leq l$, so that $i \lneq l$; if $i \neq k$, then $x_{i,j}x_{k,l} = 0$. In any case, we see that $x_{i,j}x_{k,l}$ is in I_1. A similar arguments shows that $x_{k,l}x_{i,j} \in I_1$, and these two facts are enough to conclude that I_1 is an ideal of $\Bbbk P$, for R_0 spans the whole algebra. This verifies our first claim.

To establish the second one, we proceed by induction: we suppose that $r \geq 1$ and $I_1^r \subseteq I_r$, and show that $I_1 I_r \subseteq I_{r+1}$, which is enough for our purpose since then $I_1^{r+1} = I_1 I_1^r \subseteq I_1 I_r \subseteq I_{r+1}$. To prove that $I_1 I_r \subseteq I_{r+1}$, in turn, we need only show that if (i, j), $(k, l) \in R$ are such that $d(i, j) \geq 1$ and $d(k, l) \geq r$, then $x_{i,j}x_{k,l}$ is in I_{r+1}. If $j \neq k$, the product is zero and this is clear; if not, then the product is $x_{i,l}$, and this is in R_{r+1} because in that case $d(i, l) \geq d(i, j) + d(k, l) \geq r + 1$.

If $i \in P$, let e_i be the image of $x_{i,i}$ under the canonical projection $\Bbbk P \to \Bbbk P/I_1$. It is immediate that $e_i = e_j$ iff $i = j$, that the set $\{e_i : i \in P\}$ is a basis of the algebra $\Bbbk P/I_1$, and that $e_i e_j = \delta_{i,j} e_i$ for all i, $j \in P$. It follows from this there is an evident algebra isomorphism $\Bbbk P \cong \Bbbk \times \cdots \times \Bbbk$, with n factors on the right, and, in particular, that the quotient algebra $\Bbbk P/I_1$ is semisimple. According to Proposition **4.2.11**, we have then that $I_1 = \operatorname{rad} \Bbbk P$. This is precisely the content of the proposition. □

Path algebras and their admissible quotients

4.3.8. A ***quiver*** is a 4-tuple $Q = (Q_0, Q_1, s, t)$ in which Q_0 and Q_1 are finite sets and s, $t : Q_1 \to Q_0$ are functions. We will always assume that Q_0 is non-empty. The elements of Q_0 and of Q_1 are the ***vertices*** and ***arrows*** of the quiver, respectively. If $\alpha \in Q_1$ is an arrow, the vertices $s(\alpha)$ and $t(\alpha)$ are the ***source*** and the ***target*** of α; we will write $\alpha : x \to y$ to mean that α is an arrow, that x and y are vertices, and that $x = s(\alpha)$ and $y = t(\alpha)$.

We will often visualize a quiver as an oriented graph: each vertex of Q will be drawn as a vertex of the graph and each arrow $\alpha : x \to y$ as an actual arrow. For example, the quiver $Q = (Q_0, Q_1, s, t)$ with $Q_0 = \{1, 2, 3, 4\}$, $Q_1 = \{\alpha, \beta, \gamma, \delta, \varepsilon, \zeta, \eta, \theta, \kappa\}$ and s and t given by in the table appearing in Figure 3 on the following page will be drawn as in the accompanying graph.

	s	t
α	1	2
β	2	3
γ	2	1
δ	2	3
ε	1	4
ζ	1	1
η	4	2
θ	3	3
κ	3	3

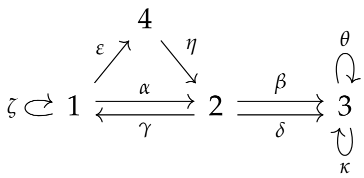


Figure 3. A quiver

4.3.9. Let us fix a quiver $Q = (Q_0, Q_1, s, t)$. A ***path*** in Q is a sequence $u = (\alpha_n, \dots, \alpha_1, x)$ with n a non-negative integer, $x \in Q_0$, and $\alpha_1, \dots, \alpha_n \in Q_1$ such that

- for each $i \in \{1, \dots, n-1\}$ we have $t(\alpha_i) = s(\alpha_{i+1})$;
- if $n \geq 1$, then $x = s(\alpha_1)$.

The ***length*** of such a path is the number n and we denote it $|u|$. We say that u is a ***cycle*** if its length n is positive and $t(\alpha_n) = x$.

We denote Q_* the set of all paths in Q and we define functions $s, t : Q_* \to Q_0$ so that for each path $u = (\alpha_n, \dots, \alpha_1, x)$ we have $s(u) = x$ and $t(u) = x$ or $t(u) = t(\alpha_n)$ according to whether $n = 0$ or not.

4.3.10. If $u = (\alpha_n, \dots, \alpha_1, x)$ and $v = (\beta_m, \dots, \beta_1, y)$ are two paths in Q and $t(v) = s(u)$, we say that u and v are ***concatenable*** and we define the ***concatenation*** of u and v to be the path

$$uv = (\alpha_n, \dots, \alpha_1, \beta_m, \dots, \beta_1, y).$$

This is an associative operation, in the following sense: if u, v and w are paths in Q with $t(w) = s(v)$ and $t(v) = s(u)$, so that the concatenations vw, uv, $u(vw)$ and $(uv)w$ are all defined, we have $u(vw) = (uv)w$. It follows from this that if $n \geq 1$ and $u_n, \dots, u_1$ is a finite sequence of paths such that for each $i \in \{1, \dots, n-1\}$ the paths u_{i+1} and u_i are concatenable, we can unambiguously consider the concatenation $u_n \cdots u_1$.

4.3.11. If $x \in Q_0$, we will denote e_i the path (x) of length 0 and say that it is a ***trivial*** or a ***stationary*** path. On the other hand, we will henceforth identify an arrow α of Q with the corresponding path $(\alpha, s(\alpha))$ of length 1. If $u = (\alpha_n, \dots, \alpha_1, x)$ is a path of positive length, then for all $i \in \{1, \dots, n-1\}$ the paths α_{i+1} and α_i are concatenable and we in fact have that u is equal to the concatenation $\alpha_n \cdots \alpha_1$. We will always write it in this way, dropping the notation $(\alpha_x, \dots, \alpha_1, x)$ from now on.

4.3.12. The ***path algebra*** of the quiver Q is the algebra $\Bbbk Q$ which as a vector space has the set Q_* of all paths of Q as a basis and in which the product is such that for all paths $u, v \in Q_*$ we have

$$u \cdot v = \begin{cases} uv, & \text{if } u \text{ and } v \text{ are concatenable;} \\ 0, & \text{if not.} \end{cases}$$

That this is an associative algebra follows at once from the corresponding property of the concatenation operation of paths and the element $\sum_{i \in Q_0} e_i$ is easily seen to be an identity element.

4.3.13. In general, the path algebra of a quiver is not finite-dimesional, but it is easy to decide when it is:

Proposition. *The set Q_* of paths in Q is finite and the algebra $\Bbbk Q$ finite-dimesional iff Q does not have any cycles.*

When that condition holds, we say that Q is ***acyclic***.

Proof. Clearly Q_* is an infinite set iff $\Bbbk Q$ is a finite-dimensional vector space, so we need only worry about the cardinality of Q_*.

Suppose first that the set Q_* is infinite. Since the number of paths of each length is finite, there is no bound on the length of the paths of Q and, in particular, there exists in Q_* a path $u = \alpha_n \cdots \alpha_1$ of length n strictly larger than $|Q_0|$. It follows then that the vertices $s(\alpha_1)$, $s(\alpha_2)$, …, $s(\alpha_n)$ are not all distinct, so that there exist $i, j \in \{1 \dots, n\}$ with $i < j$ and $s(\alpha_i) = s(\alpha_j)$. This implies at once that the path $\alpha_{j-1} \cdots \alpha_1$ is a cycle.

Conversely, suppose that Q has a cycle u. Since u is concatenable wiith itself, we can recursively define paths $u_1 = u$ and $u_{k+1} = uu_k$ for all positive integers k. A trivial induction shows that $|u_k| = k|u|$ for all positive integers k, so that $u_k = u_l$ iff $k = l$, and thn it is clear that the set $\{u_k : k \in \mathbb{N}\}$, which is contained in Q_*, is infinite. □

4.3.14. If Q is a quiver, we denote FQ the ideal of $\Bbbk Q$ generated by the arrows. As a subspace of $\Bbbk Q$ it has as a basis the set $Q_{\geq 1}$ of all paths of positive length. It follows easily from this that if k is a positive integer, then the kth power FQ^k of F has as a vector space basis the set $Q_{\geq k}$ of paths of length at least k.

4.3.15. We say that an ideal I in the path algebra $\Bbbk Q$ of a quiver is ***admissible*** if

- I is contained in FQ^2, and
- there exists an integer $k \geq 2$ such that I contains FQ^k.

The first condition is that every element of I be a linear combination of paths of length at least 2 and the second one is that there exist a positive integer k such that all paths of length at least k are in I —and in fact it is enough that those of length exactly k be in I.

If Q is an acyclic quiver, then the second condition is automatic, as $FQ^k = 0$ for k larger than the number of vertices in Q. In particular, the zero ideal of $\Bbbk Q$ is in that case admisssible.

4.3.16. Proposition. *If Q is a quiver and I is an admissible ideal of $\Bbbk Q$, then the quotient algebra $\Bbbk Q/I$ is finite-dimensional.*

Proof. Let $p : \Bbbk Q \to \Bbbk Q/I$ be the canonical projection. Since the set Q_* spans the path algebra $\Bbbk Q$, the set $p(Q_*)$ spans the quotient $\Bbbk Q/I$. The second condition imposed by admissibility implies that there exists an integer $k \geq 2$ such that $Q_{\geq k} \subseteq I$ and then $p(Q_*) = p(Q_{<k}) \cup \{0\}$ is a finite set. Of course, this tells us that $\Bbbk Q/I$ is finite-dimensional. □

4.3.17. As we see in the proof of Proposition 4.3.16, the finite-dimensionality of the algebra $\Bbbk Q/I$ depends only on the second condition imposed on the ideal I. We will see later what is the role payed by the first condition.

It should be remarked that not all ideals of a path algebra satisfy that second condition. An example is given by the quiver Q

$$\begin{tikzcd} \circ \arrow[loop right, "\alpha"] \end{tikzcd}$$

and the ideal $I = (\alpha^2 - \alpha^3)$: it is easy to see that this ideal does not contain any path at all. As the quotient $\Bbbk Q/I$ is finite-dimensional in this case, we see that the second condition imposed by admissibility is not necessary for this.

4.3.18. If I is an admissible ideal of the path algebra and $\Bbbk Q_{\leq 1}$ is the subspace of $\Bbbk Q$ spanned by the paths of length at most 1, then we have $I \cap \Bbbk Q_{\leq 2} = 0$. This implies that the restriction of the canonical projection $p : \Bbbk Q \to \Bbbk Q/I$ to $\Bbbk Q_{\leq 1}$ is injective. Abusing language a bit, if $u \in Q_*$ is a trivial path or an arrow, we will say that the image $p(u)$ is also a trivial path or an arrow.

4.3.19. Proposition. *Let Q be a quiver and let I be an admissible ideal of the path algebra $\Bbbk Q$ of Q. If FQ is the ideal of $\Bbbk Q$ generated by the arrows, as before, then the radical of the algebra $\Bbbk Q/I$ is the ideal FQ/I.*

In other words, the radical of $\Bbbk Q/I$ is «generated by the arrows».

Proof. To be done □

§4.4. Exercises

4.4.1. Let A be an algebra.

(*i*) If M is a left A-module, we write $D(M) = \mathsf{hom}(M, \Bbbk)$. This is a *right* A-module with action $\cdot : D(M) \times A \to D(M)$ such that $(\phi \cdot a)(m) = \phi(am)$ for all $\phi \in D(M)$, $a \in A$ and $m \in M$. If $f : M \to N$ is a morphism of left A-modules, then the map $D(f) : \phi \in D(N) \mapsto \phi \circ f \in D(M)$ is a morphism of right A-modules. In this way we find a kk-linear functor $D : {}_A\mathsf{mod} \to \mathsf{mod}_A^{\mathsf{op}}$ with values in the opposite category of the category of finite-dimensional right A-modules which is an equivalence of categories.

(*ii*) Let M be a left A-module. We let $\mathscr{L}(M)$ be the set of submodules of M, which is a complete lattice with respect to the ordering given by inclusion; we use the same notation for right A-modules. If N is an submodule of M, then the set $\lambda(N) = \{\phi \in D(M) : \phi|_N = 0\}$ is a submodule of the right A-module $D(M)$. We obtain in this way a function $\lambda : \mathscr{L}(M) \to \mathscr{L}(D(M))$ which is an order-reversing bijection, and we have $\lambda(\operatorname{soc} M) = \operatorname{rad} D(M)$ and $\lambda(\operatorname{rad} M) = \operatorname{soc} D(M)$.

4.4.2. (*i*) A set of nilpotent matrices does not span the vector space $M_n(\Bbbk)$.

(*ii*) If $\Bbbk$ is algebraically closed, then a semisimple algebra has no non-zero ideals spanned by nilpotent elements.

(*iii*) If $\Bbbk$ is algebraically closed, then an ideal I in an algebra A which is spanned by nilpotent elements is in fact nilpotent.
Hint. To see this, consider the ideal $(I + \operatorname{rad} A)/\operatorname{rad} A$ of $A/\operatorname{rad} A$.

(*iv*) The conclusion of (*iii*) holds even without the hypothesis made on the field.
Hint. If $\overline{\Bbbk}$ is an algebraic closure of $\Bbbk$, this can be seen by considering the $\overline{\Bbbk}$-algebra $\overline{\Bbbk} \otimes A$.

CHAPTER 5

Projective modules

§5.1. Idempotents

5.1.1. If an algebra A is semisimple, all its modules are projective and, moreover, every indecomposable projective is a direct summand of A itself. This suggests that the direct summands of the regular module may be relevant in the general case and it is easy to describe them:

Proposition. *Let A be an algebra. An A-submodule P of A is a direct summand iff there exists an idempotent element $e \in A$ such that $P = Ae$.*

Proof. Suppose first that P is a direct summand of A, so that there is another submodule Q of A such that $A = P \oplus Q$ and, in particular, there exist $e \in P$ and $f \in Q$ such that $1 = e + f$. If $p \in P$, multiplying this equality on the left by p, we find that $p = pe + pf$, so that $P \ni p - pe = pf \in Q$. Since $P \cap Q = 0$, this tells us that $p = pe$. On one hand, we see from this that $P \subseteq Pe \subseteq Ae \subseteq P$, so that in fact $P = Ae$. On the other, taking $p = e$ shows that e is an idempotent in A.

Conversely, let $e \in A$ be an idempotent element and consider the submodules Ae and $A(1-e)$. If $x \in Ae \cap A(1-e)$, then there are $a, b \in A$ such that $ae = x = b(1-e)$, and therefore $xe = aee = ae = x$ and $xe = b(1-e)e = b(e-e^2) = 0$, so $x = 0$; this tells us that $Ax \cap A(1-e) = 0$. Since clearly $Ae + A(1-e) = A$, we have $A = Ae \oplus A(1-e)$ and Ae is therefore a direct summand of A, as we wanted to show. $\square$

5.1.2. It should be noted that in the situation of Proposition 5.1.1 there exist in general many idempotent elements $e \in A$ such that $P = Ae$. For example, if $A = M_2(\Bbbk)$, then for all $\lambda \in \Bbbk$ the matrix $e_\lambda = \left(\begin{smallmatrix} 1 & 0 \\ \lambda & 0 \end{smallmatrix}\right) \in A$ is idempotent and we have $Ae_0 = Ae_\lambda$ for all $\lambda \in \Bbbk$.

5.1.3. Having identified the direct summands of A, we want to decide when they are indecomposable. We know that this can be done by studying their endomorphism algebras, and the following proposition describes them:

Proposition. *Let A be an algebra, let P be a direct summand of A and let $e \in A$ be an idempotent such that $P = Ae$.*

(*i*) *If N is an A-module, for every morphism $f : P \to N$ we have $f(e) \in eN$ and the function $\phi_N : f \in \mathsf{hom}_A(P, N) \mapsto f(e) \in eN$ is an isomorphism of vector spaces.*

(*ii*) *The function $\phi_P : \mathsf{End}_A(P)^{\mathsf{op}} \to eP = eAe$ is an isomorphism of algebras.*

In the second statement, we are viewing eAe as a subalgebra of A. It is a unital algebra —its unit element is e, as one can immediately check— but its unit is not in general that of A.

Proof. (*i*) If $f : P \to N$ is a morphism of A-modules, then $f(e) = f(ee) = ef(e) \in eN$; this means that there is in fact a function ϕ_N as decribed in the proposition. It is injective: if $f \in \mathsf{hom}_A(P, N)$ is such that $\phi_N(f) = f(e) = 0$, then for all $a \in A$ w have $f(ae) = af(e) = 0$, and then $f = 0$ since $P = Ae$.

Let $n \in N$. The function $g : a \in A \mapsto au \in N$ is a morphism of A-modules, and so is the inclusion $\iota : Ae \to A$, so that $g \circ \iota \in \mathsf{hom}_A(P, N)$. As $\phi_N(g \circ \iota) = en$, this shows that the function ϕ_N es surjective.

(*ii*) We know from (*i*) that the function ϕ_P is an isomorphism of vector spaces. If $f, g \in \mathsf{End}_A(P)$, then we have $\phi_P(f \circ g) = (f \circ g)(e) = f(g(e))$ and, as $g(e) \in P = Ae$, this is equal to $f(g(e)e) = g(e)f(e) = \phi_P(g)\phi_P(f)$. This shows that ϕ_P is multiplicative when it is viewed as defined on $\mathsf{End}_A(P)^{\mathsf{op}}$. □

5.1.4. Proposition. *Let A be an algebra, let $e \in A$ be an idempotent and let $P = Ae$ be the corresponding direct summand of A. The module P is indecomposable iff e is not zero and whenever $e = e_1 + e_2$ with e_1, $e_2 \in A$ two idempotent elements such that $e_1e_2 = e_2e_1 = 0$ we have $e_1 = 0$ or $e_2 = 0$.*

An idempotent e with this property is said to be ***primitive***.

Proof. From part (*ii*) of Proposition 5.1.3 we know that $\mathsf{End}_A(P)$ is isomorphic to the algebra eAe, and we know from Proposition 1.2.2 that P is indecomposable iff the only idempotents in $\mathsf{End}_A(P)$ or, equivalently, in eAe, are trivial.

If $e_1 \in eAe$ is an idempotent, then $e_2 = e - e_1$ is also idempotent and we have $e = e_1 + e_2$ and $e_1e_2 = e_2e_1 = 0$. Since obviously e_1 is a trivial idempotent of eAe iff we have $e_1 = 0$ or $e_2 = 0$, the result of the proposition follows. □

5.1.5. Proposition 5.1.4 describes the indecomposable summands of the regular module of an algebra in terms of its idempotents. From that descriptin we can extract one of the direct sum decompositions of the regular module in the same spirit:

Proposition. *Let A be an algebra.*

(*i*) *There exists an integer n and a set $\{e_1, \dots, e_n\}$ of idempotent elements of A with $\sum_{1=1}^{n} e_1 = 1$ and $e_ie_j = 0$ when i, $j \in \{1, \dots, n\}$ are different such that $A = \bigoplus_{i=1}^{n} Ae_i$ as a left A-module.*

(*ii*) *Every indecomposable projective A-module is isomorphic to Ae_i for some $i \in \{1, \dots, n\}$.*

Proof. We know from the Krull-Remak-Schmidt Theorem 1.4.1 that there exist a positive integer n and indecomposable submodules $P_1, \dots, P_n$ of the regular A-module A such that $A = \bigoplus_{i=1}^n P_i$ and Proposition 5.1.4 tells us there exist primitive idempotent elements $e'_1, \dots, e'_n \in A$ such that $P_i = Ae'_i$ for each $i \in \{1, \dots, n\}$.

In view of the direct sum decomposition of A, there exist $a_1, \dots, a_n \in A$ such that $\sum_{i=1}^n a_i e'_i = 1$. If $j \in \{1, \dots, n\}$ and we multiply this equality on the right by e'_j, we find that $e'_j = \sum_{i=1}^n e'_j a_i e'_i$: since the sum is direct, this implies that $e'_j a_i e'_j = 0$ if $i, j \in \{1, \dots, n\}$ are different, and that $e'_i = e'_i a_i e'_i$ for all $i \in \{1, \dots, n\}$.

It follows from this that if we put $e_i = a_i e'_i$ for each $i \in \{1, \dots, n\}$, then the elements $e_1, \dots, e_n$ are idempotent, $\sum_{i=1}^n e_i = 1$ and $e_i e_j = 0$ if $i, j \in \{1, \dots, n\}$ are different. Finally, since $P_i = Ae'_i = Ae'_i a_i e'_i \subseteq Ae_i \subseteq Ae'_i = P_i$ we have $P_i = Ae_i$ and, as P_i is indecomposable, Proposition 5.1.4 tells us that e_i is primitive. This proves (i).

Every indecomposable projective module is isomorphic to an indecomposable summand of a free module A^r of some positive rank r. Since every indecomposable summand of A is isomorphic to one of $Ae_1, \dots, Ae_n$, the claim of (ii) follows now immediately from the Krull-Remak-Schmidt Theorem. □

5.1.6. A ***system of idempotents*** in an algebra A is a set $E = \{e_1, \dots, e_n\}$ of non-zero idempotent elements; when we write such a system in this way, we will always assume implicitly that $e_i \neq e_j$ whenever $i, j \in \{1, \dots, n\}$ are different. The system E is ***complete*** if $\sum_{i=1}^n e_i = 1$ and it is ***orthogonal*** if $e_i e_j = 0$ whenever $i, j \in \{1, \dots, n\}$ are different.

5.1.7. Proposition. *Let A be an algebra and let $E = \{e_1, \dots, e_n\}$ be a system of orthogonal idempotents in A.*

(i) *The set E is linearly independent.*

(ii) *There exist a system of orthogonal* primitive *idempotents $\{f_1, \dots, f_m\}$ in A and a surjective function $\phi : \{1, \dots, m\} \to \{1, \dots, n\}$ such that for all $i \in \{1, \dots, n\}$ we have $e_i = \sum_{j \in \phi^{-1}(i)} f_j$.*

Proof. (i) Suppose that $a_1, \dots, a_n \in \Bbbk$ are such that $\sum_{i=1}^n a_i e_i = 0$. If $j \in \{1, \dots, n\}$, multiplying this equality on the right by e_j and using the orthogonality of E and the idempotence of e_j we find at once that $a_j e_j = 0$ and, since $e_j \neq 0$, that $a_j = 0$.

(ii) In the set $\mathscr{S}$ of all pairs $(\{f_1, \dots, f_m\}, \phi)$ with $\{f_1, \dots, f_m\}$ a system of orthogonal idempotents in A and $\phi : \{1, \dots, m\} \to \{1, \dots, n\}$ a surjective function such that for all $i \in \{1, \dots, n\}$ we have $e_i = \sum_{j \in \phi^{-1}(i)} f_j$ we may consider one with m maximal; this makes sense since such pairs do exist: $(\{e_1, \dots, e_n\}, \mathrm{id}_{\{1,\dots,n\}})$ is one. The desired result will be proven if we show that the idempotents $f_1, \dots, f_m$ are primitive.

Assume this is not the case, so that there exists $j_0 \in \{1, \dots, m\}$ and non-zero idempotents g_1, g_2 such that $f_{j_0} = g_1 + g_2$ and $g_1 g_2 = g_2 g_1 = 0$.

If there existed $j \in \{1, \dots, m\} \setminus \{j_0\}$ and $k \in \{1, 2\}$ such that $f_j = g_k$, then we would have that $g_k = g_k(g_1 + g_1) = f_j f_{j_0} = 0$, which is absurd. It follows then that the $m + 1$

elements $f_1, \ldots, f_{j_0-1}, g_1, g_2, f_{j_0+1}, \ldots, f_m$ are pairwise different; let us denote them, in order, $h_1, \ldots, h_{m+1}$. If $\psi : \{1, \ldots, m\} \to \{1, \ldots, m+1\}$ is the function such that $\psi(i) = i$ for each $i \in \{1, \ldots, J_0\}$ and $\psi(j) = j - 1$ if $i \in \{j_0 + 1, \ldots, m+1\}$, then one can immediately check that the pair $(\{h_1, \ldots, h_{m+1}\}, \psi \circ \phi)$ belongs to the set $\mathscr{S}$. This contradicts the choice of m, so our assumption does not hold. $\square$

5.1.8. The first part of Proposition 5.1.5 tells us that every algebra contains a complete orthogonal system of primitive idempotents and, as seen in its proof, this is essentially a consequence of the existence claim of the Krull-Remak-Schmidt Theorem 1.4.1. The uniqueness part of this theorem, in turn, allows us to prove that all complete orthogonal systems of primitive idempotents are closely related:

Proposition. *Let A be an algebra. If $\{e_1, \ldots, e_n\}$ and $\{e'_1, \ldots, e'_m\}$ are two complete orthogonal systems of primitive idempotents in A, then $n = m$ and there exist a unit $u \in A^\times$ and a permutation π of $\{1, \ldots, n\}$ such that for all $i \in \{1, \ldots, n\}$ we have $e'_{\pi(i)} = u^{-1} e_i u$.*

Proof. We know that $A = \bigoplus_{i=1}^n Ae_i = \bigoplus_{j=1}^m Ae'_j$ and that the Ae_i for $i \in \{1, \ldots, n\}$ and the Ae'_j for $j \in \{1, \ldots, m\}$ are indecomposable. It follows from the Krull-Remak-Schmidt Theorem 1.4.1 that $n = m$ and that there exists a permutation π of $\{1, \ldots, n\}$ such that $Ae_i \cong Ae'_{\pi(i)}$ for all $i \in \{1, \ldots, n\}$.

For each $i \in \{1, \ldots, n\}$ let $f_i : Ae_i \to Ae_{\pi(i)}$ be an isomorphism. There is a unique morphism $f : A \to A$ such that $f(x) = f_i(x)$ for each $i \in \{1, \ldots, n\}$ and all $x \in Ae_i$ and it is an isomorphism, and there exists then an invertible element u in A such that $f(x) = xu$ for all $x \in A$. If $i \in \{1, \ldots, n\}$ and we consider the maps $p_i : x \in A \mapsto xe_i \in A$ and $p'_{\pi(i)} : x \in A \mapsto xe'_j \in A$, then the square

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "p_i"'] & A \arrow[d, "p'_{\pi(i)}"] \\ A \arrow[r, "f"] & A \end{tikzcd}$$

commutes and, therefore, $ue'_{\pi(i)} = p'_{\pi(i)}(f(1)) = f(p_i(1)) = e_i u$. As this shows that u satisfies the condition required by the proposition, the proof is complete. $\square$

§5.2. Isomorphisms

5.2.1. If A is an algebra, then there is a functor $\theta : {}_A\mathsf{mod} \to {}_{A/\operatorname{rad} A}\mathsf{mod}$ such that for each A-module M we have $\theta(M) = M/\operatorname{rad} M$ and for each morphism $f : M \to N$ of A-modules the morphism $\theta(f) : M/\operatorname{rad} M \to N/\operatorname{rad} N$ is the one induced by f; this makes sense since, according to Proposition 4.1.9, we have $f(\operatorname{rad} P) \subseteq \operatorname{rad} Q$. If M and N are A-modules, we will denote $\theta_{M,N}$ the function

$$f \in \hom_A(M, N) \mapsto \theta(f) \in \hom_{A/\operatorname{rad} A}(M/\operatorname{rad} M, N/\operatorname{rad} N).$$

induced by this functor.

5.2.2. Proposition. *Let A be an algebra and P a projective A-module.*

(*i*) *If Q is an A-module, then the natural map described above*

$$\theta_{P,Q} : \hom_A(P, Q) \to \hom_{A/\operatorname{rad} A}(P/\operatorname{rad} P, Q/\operatorname{rad} Q)$$

is surjective.

(*ii*) *The map $\theta_{P,P}$ is a morphism of algebras, its kernel is $\operatorname{rad}\operatorname{End}_A(P)$ and it induces an isomorphism of algebras*

$$\bar\theta_{P,P} : \frac{\operatorname{End}_A(P)}{\operatorname{rad}\operatorname{End}_A(P)} \to \operatorname{End}_{A/\operatorname{rad} A}(P/\operatorname{rad} P).$$

Proof. (*i*) Let $f : P/\operatorname{rad} P \to Q/\operatorname{rad} Q$ be a morphism of $A/\operatorname{rad} A$-modules, which is also a morphism of A-modules. If $\pi_P : P \to P/\operatorname{rad} P$ and $\pi_Q : Q \to Q/\operatorname{rad} Q$ are the canonical surjections, the diagram of solid arrows

$$\begin{tikzcd}
P \arrow[r, dotted, "\bar f"] \arrow[d, two heads, "\pi_P"'] & Q \arrow[d, two heads, "\pi_Q"] \\
P/\operatorname{rad} P \arrow[r, "f"] & Q/\operatorname{rad} Q
\end{tikzcd}$$

can be completed with a morphism $\bar f : P \to Q$ of A-modules so that it commutes, since π_Q is surjective and P is projective. It is clear that $\theta_{P,Q}(\bar f) = f$.

(*ii*) That the function $\theta_{P,P}$ is a morphism of algebras is immediate and it is surjective by the first part of the proposition. To prove (*ii*) it is then enough that we show that the kernel of $\theta_{P,P}$ is precisely the radical of $\operatorname{End}_A(P)$. On the other hand, the codomain of $\theta_{P,P}$ is a semisimple algebra —because it is the endomorphism algebra of the semisimple module $P/\operatorname{rad} P$— so Proposition 4.2.11 implies that to show that $\ker\theta_{P,P}$ is the radical of $\operatorname{End}_A(P)$ we need only prove that it is a nil ideal.

Let then $f : P \to P$ be an element of $\ker\theta_{P,P}$. If $\pi_P : P \to P/\operatorname{rad} P$ is the canonical projection, this tells us that $\pi_P \circ f = \theta_{P,P}(f) \circ \pi_P = 0$, so that

$$f(P) \subseteq \ker \pi_P = \operatorname{rad} P = (\operatorname{rad} A)P.$$

It follows at once from this that $f^k(P) \subseteq (\operatorname{rad} A)^k P$ for all positive integers k. In particular, if k is an integer large enough so that $(\operatorname{rad} A)^k = 0$ —and such an integer exists by Proposition 4.2.11— then we see that $f^k(P) = 0$, that is, that $f^k = 0$. This proves that the ideal $\ker \theta_{P,P}$ is nil and, therefore, the proposition. □

5.2.3. Corollary. *Two projective modules P and Q are isomorphic iff $P/\operatorname{rad} P$ and $Q/\operatorname{rad} Q$ are isomorphic. In fact, the map $\theta_{P,Q}$ of Proposition 5.2.2 restricts to a bijection from the set of isomorphisms $P \to A$ to the set of isomorphisms $P/\operatorname{rad} P \to Q/\operatorname{rad} Q$.*

Proof. We need only prove the second claim, as the first one clearly follows from it.

If $f : P \to Q$ is an isomorphism of A-modules, then $\theta_{P,Q}(f) : P/\operatorname{rad} P \to Q/\operatorname{rad} Q$ is an isomorphism because the map is obtained from the functor θ that we described in 5.2.1. Conversely, suppose that $f : P \to Q$ is a morphism of A-modules such that $\theta_{P,Q}(f)$ is an isomorphism. Since the function $\theta_{Q,P}$ is surjective, there exists then a morphism $g : Q \to P$ of A-modules such that $\theta_{Q,P}(g)$ is an inverse for $\theta_{P,Q}(f)$ and, since θ is a functor, this implies that $\theta_{P,P}(\mathrm{id}_P - gf) = 0$ and $\theta_{Q,Q}(\mathrm{id}_Q - fg) = 0$. According to part (*ii*) of Proposition 5.2.2, this means that $\mathrm{id}_P - gf \in \operatorname{rad} \operatorname{End}_A(P)$ and $\mathrm{id}_Q - fg \in \operatorname{rad} \operatorname{End}_A(Q)$. It follows then from Corollary 4.2.9 that $gf = \mathrm{id}_P - (gf - \mathrm{id}_P)$ and $fg = \mathrm{id}_Q - (\mathrm{id}_Q - fg)$ are invertible in the algebras $\operatorname{End}_A(P)$ and in $\operatorname{End}_A(Q)$, respectively, and then that both f and g are isomorphisms, as one can see at once. □

5.2.4. Lemma. *An algebra A is local iff $A/\operatorname{rad} A$ is a division algebra.*

Proof. If A is local, then A has a unique maximal left ideal, which is then equal to $\operatorname{rad} A$, and it coincides with the set of non-invertible elements. It follows that $A/\operatorname{rad} A$ is a division algebra. Conversely, suppose that $A/\operatorname{rad} A$ is a division algebra and let $x \in A \setminus \operatorname{rad} A$. Since the class of x in $A/\operatorname{rad} A$ is invertible the exists a $y \in A$ such that $1 - xy$ and $1 - yx$ are in $\operatorname{rad} A$ and, in particular, are nilpotent. It follows that $xy = 1 - (1 - xy)$ and $yx = 1 - (1 - yx)$ are invertible in A, so that there exist $u, v \in A$ such that, among other things, $xyu = vyx = 1$. The element x then has both a left and a right inverse, so is invertible. This shows that every element in $A \setminus \operatorname{rad} A$ is invertible, and we can conclude that A is local using Proposition 1.1.2. □

5.2.5. Proposition.

(*i*) *A projective module P is indecomposable iff $P/\operatorname{rad} P$ is simple.*

(*ii*) *The rule which assigns to each indecomposable projective module P the simple module $P/\operatorname{rad} P$ induces a bijection between the set of isomorphism classes of indecomposable projectives modules and the set of isomorphism classes of simple modules.*

Proof. (*i*) The projective module P is indecomposable iff its endomorphism algebra is local, which according to the lemma and to part (*ii*) of Proposition 5.2.2 happens iff the endomorphism algebra of the semisimple module $P/\operatorname{rad} P$ is a division algebra. it follow easily from Schur's Lemma 2.1.2 that the endomorphism algebra of a semisimple module is a division algebra iff the module is actually simple. This proves the claim.

(*ii*) Let P and Q be two indecomposable projective modules. If $P/\operatorname{rad} P \cong Q/\operatorname{rad} Q$, then Corollary 5.2.3 tells us that $P \cong Q$, and the converse implication is evident. It follows that the rule mentioned in the statement indeed induces a function on isomorphism classes and that that function is injective.

On the other hand, if $A = \bigoplus_{i=1} P_i$ is a decomposition of the regular module as a direct sum of indecomposable summands then we have $A/\operatorname{rad} A = \bigoplus_{i=1}^{n} P_i/\operatorname{rad} P_i$. If S is a simple module, we know that S is isomorphic to a direct summand of $A/\operatorname{rad} A$, and then it follows from the Krull-Remak-Schmidt Theorem 1.4.1 that there exists an $i \in \{1, \dots, n\}$ such that $S \cong P_i/\operatorname{rad} P_i$. This tells us that the function of the statement is surjective. $\square$

§5.3. Blocks

5.3.1. If A is an algebra and $E = \{e_1, \dots, e_n\}$ a complete orthogonal system of primitive idempotents of A, we construct a quiver $\Gamma_E(A)$ with E as set of vertices and, if $e, f \in E$, an arrow $e \to f$ iff $\hom_A(Af, Ae) \neq 0$, which happens iff $fAe \neq 0$, according to the first part of Proposition 5.1.3. This quiver is clearly never empty, as E must contain at least one element.

5.3.2. Proposition. *If A is an algebra and E and E' two complete orthogonal systems of primitive idempotents, then the quivers $\Gamma_E(A)$ and $\Gamma_{E'}(A)$ are isomorphic.*

Proof. We know from Proposition 5.1.8 that E and E' have the same number of elements and, if $E = \{e_1, \dots, e_n\}$ and $E' = \{e'_1, \dots, e'_n\}$, that there exist a unit $u \in A^\times$ and a permutation π of $\{1, \dots, n\}$ such that $e'_{\pi(i)} = u^{-1}e_iu$ for all $i \in \{1, \dots, n\}$. It follows then that we have a function $\phi : e \in E \mapsto u^{-1}eu \in E'$ and that it is bijective. Moreover, if $e, f \in$, there is an arrow $e \to f$ in $\Gamma_E(A)$ iff $fAe \neq 0$, and clearly this occurs iff $\phi(f)A\phi(e) = u^{-1}fuAu^{-1}eu = u^{-1}fAeu \neq 0$, that is, iff there is an arrow $\phi(f) \to \phi(e)$ in $\Gamma_{E'}(A)$. This means, precisely, that the function $\phi : \Gamma_E(A) \to \Gamma_{E'}(A)$ is an isomorphism of quivers. $\square$

5.3.3. If $Q = (Q_0, Q_1, s, t)$ and $Q' = (Q'_0, Q'_1, s', t')$ are quivers, the ***disjoint union*** of Q and Q' is the quiver $Q \sqcup Q' = (Q_0 \sqcup Q'_0, Q_1 \sqcup Q'_1, S, T)$ with $S, T : Q_1 \sqcup Q'_1 \to Q_0 \sqcup Q'_0$ the functions such that $S|_{Q_0} = s$, $S|_{Q'_0} = s'$. $T|_{Q_0} = t$ and $T|_{Q'_0} = t'$.

Proposition. *If A and B are algebras and E and E' are complete orthogonal systems of primitive idempotents in A and in B, respectively, then $F = \{(e, 0) : e \in E\} \cup \{(0, e) : e \in E'\}$ is a complete orthogonal system of primitive idempotents in $A \times B$ and we have an isomorphism of quivers $\Gamma_F(A \times B) \cong \Gamma_E(A) \sqcup \Gamma_{E'}(B)$.*

Proof. If $e \in E$, then $(e, 0)$ is clearly a non-zero idempotent in $A \times B$. Let (g_1, g_2) and (h_2, h_2) be orthogonal idempotents in $A \times B$ such that $(e, 0) = (g_1, g_2) + (h_1, h_2)$. We have that g_1 and h_1 are orthogonal idempotents of A such that $e = g_1 + h_1$, so that one of the two must be zero. On the other hand, g_2 and h_2 are orthogonal idempotents of B and $g_2 + h_2 = 0$, so that in fact they are both zero. This means that one of (g_1, g_2) or (h_1, h_2) is zero, and proves that the idempotent $(e, 0)$ is primitive.

Of course, the same argument shows that $(0, e)$ is a non-zero primitive idempotent of $A \times B$ for each $e \in E'$. Since the functions $i_1 : e \in E \mapsto (e, 0) \in F$ and $i_2 : e \in E' \mapsto (0, e) \in F$ are injective and their images are disjoint, the set F of the statement is a system of primitive idempotents in $A \times B$. It is orthogonal and complete, as one can see at once, so we can consider the quiver $\Gamma_F(A \times B)$.

Consider the function $i : E \sqcup E' \to F$ such that $i|_E = i_1$ and $i|_{E'} = i_2$, which is bijective. If $e, f \in E$, we have a bijective function $a \in fAe \mapsto (a, 0) \in (f, 0)(A \times B)(e, 0)$, and this means that there is an arrow $e \to f$ in $\Gamma_E(A)$ iff there is an arrow $i(e) \to i(f)$ in $\Gamma_F(A \times B)$. Similarly, if $e, f \in E'$, there is an arrow $e' \to f'$ in $\Gamma_{E'}(B)$ iff there is an arrow $i(e) \to i(f)$ in $\Gamma_G(A \times B)$. Finally, if $e \in E$ and $f \in E'$, then there are no arrows $e \to f$ or $f \to e$ in $\Gamma_E(A) \sqcup \Gamma_{E'}(B)$ and there are no arrows $i(e) \to i(f)$ or $i(f) \to i(e)$ in $\Gamma_F(A \times B)$, because $(0, f)(A \times B)(e, 0) = (0, e)(A \times B)(0, f) = 0$. These observations prove that the function i is an isomorphism of quivers $\Gamma_E(A) \sqcup \Gamma_{E'}(B) \to \Gamma_F(A \times B)$. □

5.3.4. An algebra A is ***connected*** if for all complete orthogonal systems of primitive idempotents E of A the quiver $\Gamma_E(A)$ is connected. In view of Proposition 5.3.2, it is enough that the quiver be connected for one such E.

5.3.5. Local algebras are connected. Indeed, a local algebra A has no non-trivial idempotents so the only complete orthogonal system of primitive idempotents is $E = \{1\}$ and the corresponding quiver $\Gamma_E(A)$ is trivially connected. It is not true, on the other hand, that connected algebras are local —we will see lots of examples of this later— but we do have the following result:

Proposition. *The center of a connected algebra is local.*

Proof. Let A be an algebra and let us suppose that its center $\mathsf{Z}(A)$ is not local, so that there exists a complete orthogonal system of idempotents $\{e, f\}$ in $\mathsf{Z}(A)$. Since e and f are central in A, it follows at once that we have a direct product decomposition $A = eAe \times fAf$ of algebras and, if E and E' are complete orthogonal systems of primitive idempotents for eAe and of fAf, according to Proposition 5.3.3, a decomposition of quivers $\Gamma_{E \cup E'}(A) = \Gamma_E(eAe) \sqcup \Gamma_{E'}(fAf)$. This shows that A is not connected. □

5.3.6. Proposition. *An algebra is, in a unique way, a direct product of connected subalgebras.*

Those direct factors are the ***blocks*** of the algebra.

Proof. Let A be an algebra and let us fix a complete orthogonal system of primitive idempotents E in A. Let $\{E_1, \dots, E_r\}$ be the partition of E into connected components of the quiver $\Gamma_E(A)$ and for each $i \in \{1, \dots, r\}$ let $f_i = \sum_{e \in E_i} e$. There is a direct sum decomposition $A = \bigoplus_{i,j=1}^{r} f_i A f_j$ of A as a vector space and if i, $j \in \{1, \dots, r\}$ are different then

$$f_i A f_j = \bigoplus_{\substack{e \in E_i \\ e' \in E_j}} eAe' \cong \bigoplus_{\substack{e \in E_i \\ e' \in E_j}} \mathsf{hom}_A(Ae_i, Ae_j) = 0$$

since there are no arrows from a vertex in E_j to one in E_i in the quiver $\Gamma_E(A)$. We thus see that $A = \bigoplus_{i=1}^{r} f_i A f_i$ a vector space and, in fact, also as an algebra.

If $i \in \{1, \dots, r\}$, then E_i is a complete orthogonal system of primitive idempotents of the algebra $f_i A f_i$, and it is clear that $\Gamma_{E_i}(f_i A f_i)$ is isomorphic to the graph induced by $\Gamma_E(A)$ on the set E_i. It follows form this that $f_i A f_i$ is a connected algebra. This proves the existence of a decomposition as in the statement of the proposition.

Suppose now that $A = \prod_{i=1}^{s} A_i = \prod_{j=1}^{t} A'_i$ are two decompositions of A as a direct product of connected subalgebras. For each $i \in \{1, \dots, s\}$ we denote e_i the unit element of A_i and for each $j \in \{1, \dots, t\}$ we denote e'_j that of A'_j. The sets $\{e_1, \dots, e_s\}$ and $\{e'_1, \dots, e'_t\}$ are complete orthogonal system of central idempotents of A. If $i \in \{1, \dots, s\}$, then $\{e_i e'_j : 1 \leq j \leq t, e_i e'_j \neq 0\}$ is a complete orthogonal system of central idempotents of A_i, whose center is a local algebra: it follows from this that there exists a unique $\sigma(i) \in \{1, \dots, t\}$ such that $e_i e'_{\sigma(i)} = e_i$ and $e_i e'_j = 0$ for all $j \in \{1, \dots, t\} \setminus \{\sigma(i)\}$, and in this way we find a function $\sigma : \{1, \dots, s\} \to \{1, \dots, t\}$. Similarly, there is a unique function $\tau : \{1, \dots, t\} \to \{1, \dots, s\}$ such that $e'_j e_{\tau(j)} = e'_j$ and $e'_j e_i = 0$ for all $j \in \{1, \dots, t\}$ and all $i \in \{1, \dots, s\} \setminus \{\tau(j)\}$.

If now $i \in \{1, \dots, s\}$, we have $0 \neq e_i = e_i e'_{\sigma(i)} = e_i e'_{\sigma(i)} e_{\tau(\sigma(i))}$, so that $e_i e_{\tau(\sigma(i))} \neq 0$, which is possible only if $\tau(\sigma(i)) = i$. This implies that the function σ is injective. Proceeding symmetrically, we find that τ is also injective, and then we conclude that $s = t$ and that σ and τ are inverse permutations of $\{1, \dots, s\}$. In particular, for each $i \in \{1, \dots, s\}$ we have that

$$e'_{\sigma(i)} = e'_{\sigma(i)} e_{\tau(\sigma(i))} = e'_{\sigma(i)} e_i = e_i$$

From this we see at once that $A_i = A_{\sigma(i)}$, and then the two direct product decompositions that we started with have the same factors. $\square$

§5.4. An equivalence of categories

5.4.1. Let A be an algebra and let P be a A-module. We put $B = \mathsf{End}_A(P)^{\mathsf{op}}$, then there is a right B-module structure on P, which we will denote $\triangleleft$ when we need to emphasize it, such that $p \triangleleft f = f(p)$ for all $p \in P$ and all $f \in B$, and in fact in this way P becomes an (A, B)-bimodule. Similarly, if N is another A-module, then $\mathsf{hom}_A(P, N)$ has a left B-module structure, which we will write $\triangleright$ when needed, such that $(b \triangleright f)(p) = f(b(p))$ for all $b \in B$, $f \in \mathsf{hom}_A(P, N)$ and $p \in P$.

As a consequence of this, we have linear functors

$$F_P = P \otimes_B (-) : {}_B\mathsf{mod} \to {}_A\mathsf{mod}$$

and

$$G_P = \mathsf{hom}_A(P, -) : {}_A\mathsf{mod} \to {}_B\mathsf{mod},$$

and F_P is left adjoint to G_P, since for every $M \in {}_B\mathsf{mod}$ and $N \in {}_A\mathsf{mod}$ we have an isomorphism of vector spaces

$$\alpha_{M,N} : \mathsf{hom}_A(F_P M, N) \to \mathsf{hom}_B(M, G_P N)$$

such $\alpha_{M,N}(f)(m)(p) = f(p \otimes m)$ for all $f \in \mathsf{hom}_A(F_P M, N)$, $m \in M$ and $p \in P$, which is natural both in M and in N.

We have natural transformations $\varepsilon : F_P G_P \to \mathrm{id}_{{}_A\mathsf{mod}}$ and $\eta : \mathrm{id}_{{}_B\mathsf{mod}} \to G_P F_P$, the counit and the unit of the adjuntion, which can be described as follows. For each $N \in {}_A\mathsf{mod}$, the morphism of A-modules $\varepsilon_N : P \otimes_B \mathsf{hom}_A(P, N) \to N$ is the unique one such that $\varepsilon_N(p \otimes f) = f(p)$ for each $p \in P$ and each $f \in \mathsf{hom}_A(P, N)$, and for each $M \in \mathsf{mod}_A$ the morphism $\eta_M : M \to \mathsf{hom}(P, P \otimes M)$ is given by $\eta_M(m)(p) = m \otimes p$ for each $m \in M$ and $p \in P$.

5.4.2. If P is an A-module, then the vector space $\mathsf{hom}_A(P, A)$ has a natural structure of right A-module, whose action $\leftharpoondown$ is such that $(\phi \leftharpoondown a)(p) = \phi(p)a$ for all $\phi \in \mathsf{hom}_A(P, A)$ and all $p \in P$. We use this structure in the following statement.

5.4.3. Proposition. *Let P be a projective A-module. If C is an algebra and N an (A, C)-bimodule N, then there is an isomorphism $\theta_{P,N} : \mathsf{hom}_A(P, A) \otimes_A N \to \mathsf{hom}_A(P, N)$ of (B, C)-bimodules such that $\theta_{P,N}(\lambda \otimes n)(p) = \lambda(p)n$ for all $\lambda \in \mathsf{hom}_A(P, A)$, $n \in N$ and $p \in P$.*

Proof. Since P is a finitely generated, there exist a non-negative integer n and a surjective morphism of A-modules $\phi : A^n \to P$ and, as P is projective, this map has an A-linear section $s : P \to A^n$, so that $\phi \circ s = \mathrm{id}_P$. For each $i \in \{1, \dots, n\}$ we let $p_i = \phi(e_i)$, with $e_i \in A^i$ the ith element of the standard basis, and let $\phi_i : P \to A$ be the composition of s with the ith projection $A^n \to A$. We then have $\phi(a_1, \dots, a_n) = \sum_{i=1}^n a_i p_i$ for all $(a_1, \dots, a_n) \in A^n$, and $s(p) = (\phi_1(p), \dots, \phi_n(p))$ for all $p \in P$. The relation $\phi \circ s = \mathrm{id}_P$ then tells us that $\sum_{i=1}^n \phi_i(p) p_i = p$ for all $p \in P$.

Let C and N be as in the statement of the proposition and let us consider the function $\mu : \mathrm{hom}_A(P, N) \to \mathrm{hom}_A(P, A) \otimes_A N$ such that for all $f \in \mathrm{hom}_A(P, N)$ we have $\mu(f) = \sum_{i=1}^n \phi_i \otimes f(p_i)$. If $f \in \mathrm{hom}_A(P, N)$, then for all $p \in P$ we have

$$\theta_{P,N}(\mu(f))(p) = \theta_{P,N}\Big(\sum_{i=1}^n \phi_i \otimes f(p_i)\Big)(p) = \sum_{i=1}^n \phi_i(p) f(p_i) = f\Big(\sum_{i=1}^n \phi_i(p) p_i\Big) = f(p),$$

so that $\theta_{P,M}(\mu(f)) = f$ and, therefore, $\theta_{P,N} \circ \mu = \mathrm{id}_{\mathrm{hom}_A(P,N)}$. On the other hand, if $\phi \in \mathrm{hom}_A(P, A)$ and $n \in N$, we have that for all $p \in P$

$$\Big(\sum_{i=1}^n \phi_i \leftharpoonup \phi(p_i)\Big)(p) = \sum_{i=1}^n \phi_i(p)\phi(p_i) = \phi\Big(\sum_{i=1}^n \phi_i(p) p_i\Big) = \phi(p),$$

so that in fact $\sum_{i=1}^n \phi_i \leftharpoonup \phi(p_i) = \phi$, and then

$$\mu(\theta_{P,N}(\phi \otimes n)) = \sum_{i=1}^n \phi_i \otimes \phi(p_i) n = \Big(\sum_{i=1}^n \phi_i \leftharpoonup \phi(p_i)\Big) \otimes n = \phi \otimes n.$$

This means that $\mu \circ \theta_{P,N}$ is the identity map of $\mathrm{hom}_A(P, A) \otimes_A N$ and, in conclusion, that μ and $\theta_{P,N}$ are inverse bijections. □

5.4.4. Let P be an A-module. We say that P ***generates*** an A-module M if there exist a positive integer n and a surjective morphism of A-modules $P^n \to M$, and this happens iff there exist A-linear maps $\phi_1, \ldots, \phi_n : P \to M$ such that for all $m \in M$ there are $p_1, \ldots, p_n \in P$ with $m = \sum_{i=1}^n \phi_i(p_i)$.

If P generates all A-modules, then we say that it is a ***generator*** for the category ${}_A\mathrm{mod}$. For example, the regular module A is a generator. It is easy to see that an A-module which generates a generator of ${}_A\mathrm{mod}$ is itself a generator of that category.

5.4.5. Proposition. *Let P be an A-module.*

(*i*) *If P is a generator for ${}_A\mathrm{mod}$, then the counit morphism $\varepsilon_N : P \otimes_B \mathrm{hom}_A(P, N) \to N$ is an isomorphism of A-modules for every A-module N.*

(*ii*) *If P is projective, then the unit morphism $\eta_M : M \to \mathrm{hom}_A(P, P \otimes_B M)$ is an isomorphism of B-modules for every B-module M.*

Proof. (*i*) Since P is a generator of ${}_A\mathrm{mod}$, it generates the regular module A and there are a positive integer n, elements $p_1, \ldots, p_n \in P$ and morphisms $\phi_1, \ldots, \phi_n \in \mathrm{hom}_A(P, A)$ such that $\sum_{i=1}^n \phi_i(p_i) = 1$. There is then a function $\lambda_N : N \to P \otimes_B \mathrm{hom}_A(P, N)$ such that for each $n \in N$ we have

$$\lambda_N(n) = \sum_{i=1}^n p_i \otimes \theta_{P,N}(\phi_i \otimes n),$$

with $\theta_{P,N}$ as in Proposition 5.4.3. If $n \in N$, then $\varepsilon_N(\lambda_N(n)) = \sum_{i=1}^n \phi_i(p_i) n = n$ simply because of the way we chose the p_i and the ϕ_i. On the other hand, if $p \in P$ and

$\phi \in \mathsf{hom}_A(P, N)$, we have for all $i \in \{1, \dots, n\}$ that

$$\begin{aligned}\theta_{P,N}(\phi_i \otimes \phi(p))(q) = \phi_i(q)\phi(p) = \phi(\phi_i(q)p) = \phi(\theta_{P,P}(\phi_i \otimes p)(q))\\ = (\theta_{P,P}(\phi_i \otimes p) \triangleleft \phi)(q)\end{aligned}$$

for all $q \in P$, so that $\theta_{P,N}(\phi_i \otimes \phi(p)) = \theta_{P,P}(\phi_i \otimes p)$ and therefore

$$\begin{aligned}\lambda_N(\varepsilon_N(p \otimes \phi)) = \lambda_N(\phi(p)) &= \sum_{i=1}^{n} p_i \otimes \theta_{P,N}(\phi_i \otimes \phi(p))\\ &= \sum_{i=1}^{n} p_i \otimes \theta_{P,P}(\phi_i \otimes p) \triangleright \phi = \sum_{i=1}^{n} p_i \triangleleft \theta_{P,P}(\phi_i \otimes p) \otimes \phi\\ &= \sum_{i=1}^{n} \theta_{P,P}(\phi_i \otimes p)(p_i) \otimes \phi = \sum_{i=1}^{n} \phi_i(p_i)p \otimes \phi = p \otimes \phi.\end{aligned}$$

We thus see that λ_N and ε_N are inverse isomorphisms, and this proves the first claim of the proposition.

(*ii*) If M is a B-module, we have a commutative diagram

$$\begin{tikzcd} \mathsf{hom}_A(P, P \otimes_B M) \arrow[r, "\eta_M"] & M \\ \mathsf{hom}_A(P, A) \otimes_A P \otimes_B M \arrow[u, "\theta_{P,P\otimes_B M}"] \arrow[r, "\theta_{P,P}\otimes \mathrm{id}_M"] & B \otimes_B M \arrow[u] \end{tikzcd}$$

in which the unnamed arrow is the canonical isomorphism $b \in B \otimes_B M \to bm \in M$. Since P is projective, we know that all the arrows except possibly η_M are isomorphisms, so that so is the counit η_M. □

5.4.6. Corollary. *If P is a projective A-module which generates ${}_A\mathsf{mod}$ and $B = \mathsf{End}_A(P)^{\mathsf{op}}$, the functors $F_P = P \otimes_B (-) : {}_B\mathsf{mod} \to {}_A\mathsf{mod}$ and $G_P = \mathsf{hom}_A(P, -) : {}_A\mathsf{mod} \to \mathsf{mod}_B$ are quasi-inverse equivalences and, in particular, the categories ${}_A\mathsf{mod}$ and ${}_B\mathsf{mod}$ are equivalent.*

When two algebras have equivalent categories of modules, as A and B do in this corollary, we say that they are ***Morita equivalent***.

Proof. If P is a projective generator of ${}_A\mathsf{mod}$, then Proposition 5.4.5 tells us that the unit and the counit of the adjuntion between the functors F_P and G_P described in 5.4.1 are isomorphisms, and this implies that they are quasi-inverse equivalences. □

§5.5. Basic algebras

5.5.1. Proposition. *Let A be an algebra and let $\{P_1, \dots, P_n\}$ be a complete system of representatives of the isomorphism classes of indecomposable projective A-modules.*

(*i*) *The module $P = \bigoplus_{i=1}^n P_i$ is a projective generator of ${}_A\mathsf{mod}$ so that if $B = \mathsf{End}_A(P)^{\mathsf{op}}$, we have an equivalence of categories $G_P = \mathsf{hom}_A(P, -) : {}_A\mathsf{mod} \to {}_B\mathsf{mod}$.*

(*ii*) *If for each $i \in \{1, \dots, n\}$ we put $Q_i = G_P(P_i)$, then Q_i is an indecomposable projective B-module. Moreover, we have $Q_i \cong Q_j$ iff $i = i$, and $B \cong \bigoplus_{i=1}^n Q_i$. In particular, $\{Q_1, \dots, Q_n\}$ is a complete system of representatives of the isomorphism classes of the indecomposable projective B-modules.*

Proof. To be done □

5.5.2. We say that an algebra A is ***basic*** if whenever $A = \bigoplus_{i=1}^n P_i$ is a decomposition of the regular A-module as a direct sum of indecomposable projective modules we have for each $i, j \in \{1, \dots, n\}$ we have $P_i \cong P_j$ iff $i = j$. As a consequence of the Krull-Remak-Schmidt Theorem 1.4.1, it is enough for this that the condition hold for one such decomposition .

Proposition. *If A is an algebra, there exists a basic algebra B such that the categories ${}_A\mathsf{mod}$ and ${}_B\mathsf{mod}$ are equivalent, and any two algebras satisfying these conditions are isomorphic.*

Proof. The existence claim follows from Proposition 5.5.1, so we need only prove the uniqueness up to isomorphism of the algebra B. For this it is clearly sufficient that we show that if A and B are two basic algebras such that that there exists an equivalence of categories $F : {}_A\mathsf{mod} \to {}_B\mathsf{mod}$, then A and B are in fact isomorphic.

Let us put ourselves in that situation and let $\{P_1, \dots, P_n\}$ be a complete system of representatives of the isomorphism classes of indecomposable projective A-modules. Since an equivalence preserves projectivity, indecomposability and isomorphism, the set $\{FP_1, \dots, FP_n\}$ is complete system of representatives of the isomorphism classes of the indecomposable projective B-modules. Now, the algebra A is basic, and this implies that $A \cong \bigoplus_{i=1}^n P_i$ in ${}_A\mathsf{mod}$, so that in particular there is an isomorphism of algebras $A^{\mathsf{op}} \cong \mathsf{End}_A(\bigoplus_{i=1}^n P_i)$; similarly, we have an isomorphism of algebras $B^{\mathsf{op}} \cong \mathsf{End}_B(\bigoplus_{i=1}^n FP_i)$. Finally since $F(\bigoplus_{i=1}^n P_i) \cong \bigoplus_{i=1}^n FP_i$ and F is an equivalence, we have that the map

$$f \in \mathsf{End}_A\left(\bigoplus_{i=1}^n P_i\right) \mapsto F(f) \in \mathsf{End}_B\left(\bigoplus_{i=1}^n FP_i\right)$$

is an isomorphism of algebras. Putting everything together, we find that $A \cong B$, as we wanted. □

5.5.3. Proposition. *Let A be an algebra. The following statements are equivalent:*

(*a*) *The algebra A is basic.*

(*b*) *The algebra $A/\operatorname{rad} A$ is basic.*
(*c*) *The algebra $A/\operatorname{rad} A$ is a direct product of division algebras.*

If they hold and the ground field is algebraically closed, then every simple A-module is one-dimensional.

Proof. To be done □

§5.6. The Gabriel quiver of an algebra

5.6.1. Proposition. *Let A be an algebra and let P and Q be two indecomposable projective A-modules.*

(*i*) *A morphism $f : P \to Q$ of A-modules is not an isomorphism iff $f(P) \subseteq \operatorname{rad} Q$.*
(*ii*) *If a morphism $f : P \to Q$ factors as the composition of two non-isomorphisms $g : P \to R$ and $h : R \to Q$ with R an indecomposable projective A-module, then $f(P) \subseteq \operatorname{rad}^2 Q$.*

Proof. (*i*) Corollary 5.2.3 tells us that $f : P \to Q$ is an isomorphism iff the induced map $\bar{f} : P/\operatorname{rad} P \to Q/\operatorname{rad} Q$ is an isomorphism. Both the domain and codomain of $\bar{f}$ are simple modules in view of the first part of Proposition 5.2.5, so this happens iff the map $\bar{f}$ is non-zero, which occurs precisely when $f(P) \not\subseteq \operatorname{rad} Q$.

(*ii*) Suppose that $f : P \to Q$ factors as the composition of two non-isomorphisms $g : P \to R$ and $h : R \to Q$. By the first part, we know that $g(P) \subseteq \operatorname{rad} R = (\operatorname{rad} A)R$ and $h(R) \subseteq \operatorname{rad} Q = (\operatorname{rad} A)Q$, and it follows from this that $f(P) \subseteq (\operatorname{rad}^2 A)P = \operatorname{rad}^2 P$. □

5.6.2. Proposition. *Let A be an algebra. If e, $f \in A$ are primitive idempotents, then there are vector space isomorphisms*

$$\frac{\hom_A(Ae, \operatorname{rad} Af)}{\hom_A(Ae, \operatorname{rad}^2 Af} \cong \frac{e(\operatorname{rad} A)f}{e(\operatorname{rad}^2 A(f} \cong e\left(\frac{\operatorname{rad} A}{\operatorname{rad}^2 A}\right)f.$$

Proof. To be done □

5.6.3. Let A be a basic algebra and $E = \{e_1, \dots, e_n\}$ a complete orthogonal system of primitive idempotents in A. The ***Gabriel quiver*** $Q_{A,E}$ of A with respect to E has E as set of vertices and for each pair e, $f \in E$ of vertices exactly $\dim e(\operatorname{rad} A/\operatorname{rad}^2 A)f$ arrows $e \to f$. According to Propositions 5.6.1 and 5.6.2, the number of arrows from a vertex to another in this quiver is a measure of the number of non-isomorphisms between the corresponding indecomposable morphisms which do not factor as a product of two non-isomorphisms through a third indecomposable projective.

5.6.4. Proposition. *If A is a basic algebra and E and E' two complete orthogonal systems of primitive idempotents, then the quivers $Q_{A,E}$ and $Q_{A,E'}$ are isomorphic.*

It follows from this that the isomorphism type of the quiver $Q_{A,E}$ does not depend on the complete orthogonal system of primitive idempotents E used to construct it but only on the algebra A. We will henceforth write Q_A to denote any quiver in this isomorphism class.

Proof. According to Proposition 5.1.8, the sets E and E' have the same number of elements and if $E = \{e_1, \dots, e_n\}$ and $E' = \{e'_1, \dots, e'_n\}$ there exist a unit $u \in A^\times$ and a permutation π of $\{1, \dots, n\}$ such that $e'_{\pi(i)} = u^{-1}e_i u$ for all $i \in \{1, \dots, n\}$. We may then consider the function $\phi : e \in E \mapsto u^{-1}eu \in E'$. Let us show that ϕ is an isomorphism of quivers $Q_{A,E} \to Q_{A,E'}$ and to do this, that whenever $e, f \in E$ the number of arrows $e \to f$ in $Q_{A,E}$ is the same as the number of arrows $\phi(e) \to \phi(f)$ in $Q_{A,E'}$. In view of the construction of these quivers, this amounts to showing that $e(\operatorname{rad} A/\operatorname{rad}^2 A)f$ and $\phi(e)(\operatorname{rad} A/\operatorname{rad}^2 A)\phi(f) = u^{-1}ea(\operatorname{rad} A/\operatorname{rad}^2 A)u^{-1}eu$ are vector spaces of the same dimension and this is clearly true since u is a unit. □

5.6.5. Theorem. *Let A be a basic algebra, let E be a complete orthogonal system of primitive idempotents in A, and let $Q_{A,E}$ be the Gabriel quiver of A with respect to E. There is then a surjective algebra map $g : \Bbbk Q_{A,E} \to A$ whose kernel is an admissible ideal of the path algebra $\Bbbk Q_{A,E}$.*

Proof. To be done □

5.6.6. Corollary. *Every algebra is Morita equivalent to the quotient of a path algebra by an admissible ideal.*

Proof. To be done □

§5.7. Examples

Path algebras and their admissible quotients

5.7.1. Proposition. *Let Q be a quiver, let I be an admissible ideal of the path algebra $\Bbbk Q$ and let $A = \Bbbk Q/I$. The algebra A is then basic and it is connecte iff the quiver Q is connected. The set $E = \{e_i : i \in Q_0\}$ of trivial paths in Q is a complete orthogonal system of primitive idempotents in A and the function $i \in Q_0 \mapsto e_i \in E$ is an isomorphism of quivers $Q \to Q_{A,E}$. The kernel*

Proof. To be done □

Incidence algebras

5.7.2. Let P be a poset with order relation $\preceq$. If i and j are two elements of P, we say that j ***covers*** i, and in that case we $i \prec j$, if the set $\{k \in P : i \preceq k \preceq j\}$ has exactly two elements. The ***Hasse diagram*** of P is the quiver $Q_P = (Q_0, Q_1, s, t)$ with $Q_0 = P$, $Q_1 = \{(i,j) \in P \times P : i \prec j\}$, and s, $t : Q_1 \to Q_0$ the restriction to Q_1 of the two projection maps $P \times P \to P$.

5.7.3. Proposition. *Let P be a poset. The set $E = \{x_{i,i} : i \in P\}$ is a complete orthogonal system of primitive idempotents in the incidence algebra $\Bbbk P$ and the function $i \in P \mapsto x_{i,i} \in E$ is an isomorphism of quivers $Q_P \to Q_{\Bbbk P,E}$. There is a surjective morphism of algebras $\pi : \Bbbk Q_P \to \Bbbk P$ such that $\pi(e_i) = x_{i,i}$ for each vertices i of Q_P and $\pi(\alpha) = x_{s(\alpha),t(\alpha)}$ for all arrows α of Q_P. The kernel of π is generated as a vector space by the set of all elements of the form $u - v$ with u and v paths in Q_P such that $s(u) = s(v)$ and $s(u) = t(v)$.*

Proof. To be done □

The two non-abelian groups of order 8

The non-abelian groups of order pq

5.7.4. Proposition. *Let p and q be two prime numbers with $p > q$. There exists a non-abelian group of order pq iff q divides $p-1$. In that case all groups of that order are isomorphic and if $a \in \{2, \dots, p-1\}$ has order q in $(\mathbb{Z}/p\mathbb{Z})^\times$, the group $G_a = \langle r, s : r^p, s^q, srs^{-1}r^{-a}\rangle$ is non-abelian of order pq.* □

Notice that q divides $p-1$ iff there are elements of order q in $(\mathbb{Z}/p\mathbb{Z})^\times$.

Proof. Suppose that G is a non-abelian group of order pq. If n_p is the number of Sylow p-subgroups in G, we know that n_p divides q, so that it is either 1 or q, and that $n_p \equiv 1 \mod p$. Since $p > q \geq 2$, we have $q \not\equiv 1 \mod p$ and we see that $n_p = 1$, that is, that there is a unique Sylow p-subgroup P in G, which is therefore normal.

Let r be a generator of P and let s be a non-identity element of a Sylow q-subgroup of G, which has then order q. As P is normal, we have a function $x \in P \mapsto sxs^{-1} \in P$ which is an automorphism and it maps r to another generator of P. It follows that there is an $a \in \{1, \dots, p-1\}$ such that

$$srs^{-1} = r^a. \tag{26}$$

Since G is not abelian and r and s clearly generate it, we must have $a \neq 1$. On the other hand, since s has order q, we have $r = s^q r s^{-q} = r^{a^q}$, so that $a^q \equiv 1 \mod p$. We thus see that a is an element of order exactly q on the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$ and, in particular, that q divides $p-1$. Moreover, using only the relation (28) and the equalities $r^p = s^q = 1$ it follows easily that $G = \{r^i s^j : 0 \leq i < p, 0 \leq j < q\}$ and that the pq

elements listed on the right hand side of this equality are in fact pairwise different. This proves that the group G can in fact be presented as $\langle r, s : r^p, s^q, srs^{-1}r^{-a}\rangle$.

The group $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic, for it is the group of units of a finite field, so all of its subgroups are also cyclic. In particular, the subgroup of its elements of order dividing q is cyclic of order q and, therefore, it is generated by a. If $b \in \{2, \dots, p-1\}$ is another element of order exactly q in $(\mathbb{Z}/p\mathbb{Z})^\times$, a consequence of this is that there exists an integer n such that $b \equiv a^n \mod p$, and then it is easy to see that there is an isomorphism $\phi : G_b \to G_a$ mapping r and s to r and s^n.

Conversely, if q divides $p-1$ and $a \in \{2, \dots, p-1\}$ is such that its order in $(\mathbb{Z}/p\mathbb{Z})^\times$ is exactly q, then there is an injective morphism $\phi : \mathbb{Z}/q\mathbb{Z} \to \mathsf{Aut}_{\mathsf{Grp}}(\mathbb{Z}/p\mathbb{Z})$ such that $\phi(1)(x) = ax$ for all $x \in \mathbb{Z}/p\mathbb{Z}$, and we may consider the semidirect product $\mathbb{Z}/q\mathbb{Z} \ltimes_\phi \mathbb{Z}/p\mathbb{Z}$, which is non-abelian of order pq. This means that the condition on p and q is sufficient for the existence of such groups. $\square$

5.7.5. Let us put ourselves in the situation of Proposition 5.7.4, so that p and q are prime numbers with $p > q$ and q a divisor of $p-1$, a an element of $(\mathbb{Z}/p\mathbb{Z})^\times$ of order q and $G = G_a$ the non-abelian group of order pq described there. Let us assume, moreover, that p is the characteristic of our ground field.

The Sylow p-subgroup is the cyclic group P generated by r, it is normal and the quotient group $C = G/P$ is cyclic of order q, generated by $\bar{s} = sP$. We know from Proposition 4.3.1 that the kernel of the surjective algebra map $\pi : \Bbbk G \to \Bbbk C$ induced by the canonical projection $G \to C$ is the radical of $\Bbbk P$ and that it is generated by $r-1$ as a left or right ideal. The projection $G \to C$ has a section $C \to G$ which is a morphism of groups and which maps $\bar{s}$ to s, and this section induces a morphism of algebras $\sigma : \Bbbk C \to \Bbbk G$ which is a section to π.

Since the group C is abelian and the field algebraically closed, the group algebra $\Bbbk C$ is basic. Since it is isomorphic to $\Bbbk G/\operatorname{rad}\Bbbk G$, this implies that $\Bbbk G$ itself is basic. The choice of a means that we can view it as a primitive qth root of unity in $\Bbbk$. If we set $\bar{e}_i = q^{-1}\sum_{j=0}^{q-1} a^{-ij}\bar{s}^j$ for each $i \in \{0, \dots, q-1\}$, then we know from EXAMPLE:CYCLIC that $\bar{E} = \{\bar{e}_0, \dots, \bar{e}_{q-1}\}$ is a complete ortogonal system of primitive idempotents in $\Bbbk C$, and it follows that $E = \sigma(\bar{E})$ is a complete ortogonal system of primitive idempotents in $\Bbbk G$. We have $E = \{e_0, \dots, e_{q-1}\}$ with $e_i = q^{-1}\sum_{j=0}^{q-1} a^{-ij}s^j$ for each $i \in \{0, \dots, q-1\}$; we will consider the index of the e_i to be in $\mathbb{Z}/p\mathbb{Z}$.

5.7.6. The radical $\operatorname{rad}\Bbbk G$, as we observed above, is generated as a right ideal by $r-1$, so it is spanned as a vector space by the elements $(r-1)r^is^j = (r^{i+1}-r^i)s^j$ with $0 \le i < p$ and $0 \le j < q$. It is easy to see from this that the set with elements

$$(r-1)^is^j, \qquad 1 \le i < p, \quad 0 \le j < q$$

is a basis of $\operatorname{rad}\Bbbk G$. It follows that the ideal $I = ((r-1)^is^j : 2 \le i < p, 0 \le j \le q)$ is contained in $\operatorname{rad}^2\Bbbk G$. We claim that in fact $I = \operatorname{rad}^2\Bbbk G$. To see this it is enough to show that whenever $1 \leq i, k < p$ and $0 \leq j, l < q$ we have

$$(r-1)^i s^j \cdot (r-1)^k s^l \equiv a^{jk}(r-1)^{i+k} s^{j+l} \mod I$$

and, since I is an ideal, for this it is in turn enough to check that

$$s(r-1) \equiv a(r-1)s \mod I,$$

which we can do by straightforward computation:

$$\begin{aligned} s(r-1) &= (r^a - 1)s = \sum_{i=1}^{a} \binom{a}{i} (r-1)^i s = a(r-1)s + \sum_{i=2}^{a} \binom{a}{i} (r-1)^i s \\ &\equiv a(r-1)s \mod I. \end{aligned}$$

In this way we can conclude that the set of classes of the q elements

$$(r-1)s^j, \qquad 0 \leq j < q$$

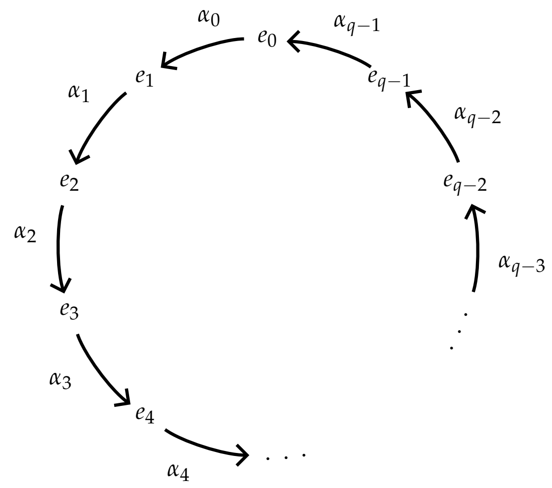
is a basis for $\operatorname{rad} \Bbbk G / \operatorname{rad}^2 \Bbbk G$, and it follows at once from this that so is the set of classes of the q elements

$$(r-1)e_j, \qquad 0 \leq j < q.$$

If now $i, j \in \{0, \ldots, q-1\}$, we have

$$\begin{aligned} e_i(r-1)e_j &= q^{-2} \sum_{k,l=0}^{q-1} a^{-ik-jl} s^k (r-1) s^l \\ &\equiv q^{-2} \sum_{k,l=0}^{q-1} a^{-ik-jl+k} (r-1) s^{k+l} \mod \operatorname{rad}^2 \Bbbk G \\ &= q^{-2} \sum_{m=0}^{q-1} \sum_{k=0}^{q-1} a^{-ik-jm+jk+k} (r-1) s^m \\ &= \left(q^{-1} \sum_{k=0}^{q-1} a^{(j+1-i)k} \right) (r-1) e_j \\ &= \delta_{i,j+1} (r-1) e_j. \end{aligned}$$

This tells us that $e_i(\operatorname{rad} \Bbbk G / \operatorname{rad}^2 \Bbbk G)e_j$ is the zero vector space if $i \neq j+1$, and that it is one-dimensional and spanned by $(r-1)e_j$ if $i = j+1$, and therefore we find that in the Gabriel quiver $Q_{\Bbbk G, E}$ there is an arrow $e_j \to e_i$ iff $i = j+1$, and in that case there is exactly one, which we name α_j. The quiver is therefore of the form



We know there is a surjective morphism of algebras $\phi : \Bbbk Q_{\Bbbk G,E} \to \Bbbk G$ such that $\phi(e_i) = e_i$ and $\phi(\alpha_i) = (r-1)e_i$ for all $i \in \{0,\dots,q-1\}$. We claim that

$$\text{if } i \in \{0,\dots,q-1\} \text{ and } j \geq 1 \text{ we have } \phi(\alpha_{i+j-1}\cdots\alpha_i) \in (r-1)^j \Bbbk G. \tag{27}$$

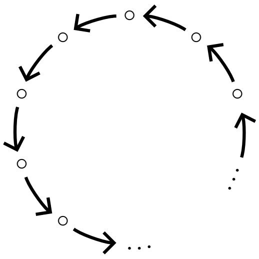
To prove it, we proceed by induction on j, noting that the claim is obvious when $j = 1$. Let then $i \in \{0,\dots,q-1\}$ and $j \geq 1$, and assume inductively that there is a $u \in \Bbbk G$ such that $\phi(\alpha_{i+j-1}\cdots\alpha_i) = (r-1)^j u$. Then

$$\begin{aligned}
\phi(\alpha_j \cdots \alpha_i) &= (r-1)e_j(r-1)^j u = q^{-1}(r-1)\sum_{k=0}^{q-1} a^{-jk}s^k(r-1)^j u \\
&= q^{-1}(r-1)\sum_{k=0}^{q-1} a^{-jk}(r^{a^k}-1)^j s^k u.
\end{aligned} \tag{28}$$

Now for all $k \in \{0,\dots,q-1\}$ we have $r^{a^k} - 1 \in (r-1)\Bbbk P$ and since $\Bbbk P$ is a commutative ring, this implies that $(r^{a^k}-1)^j \in (r-1)^j \Bbbk P$. Using this in (28) we see that $\phi(\alpha_j \cdots \alpha_i) \in (r-1)^{j+1}\Bbbk G$, completing the induction.

It follows in particular from our claim (27) that for all $i \in \{0,\dots,q-1\}$ the path $\alpha_{i+p-1}\cdots\alpha_i$ is in the kernel of the morphism ϕ. If I is the ideal of $\Bbbk Q_{A,E}$ generated by these q paths, then I is in fact spanned as a vector space by the paths of length at least p in the quiver. From this wee see at once that the dimension of the quotient $\Bbbk Q/I$ is pq. As I is contanined in the kernel of ϕ, this map induces a surjective morphism of algebras $\bar{\pi} : \Bbbk Q_{A,E}/I \to \Bbbk G$. Since its domain and codomain have the same dimension, the map $\bar{\pi}$ has to be an isomophism. A consequence of this is, of course, that I is actually equal to the kernel of π. We have proved the following:

5.7.7. Proposition. *Let p and q be two prime numbers such that $p > q$ and q divides $p-1$, so that there exists a non-abelian group G of order pq. If $\Bbbk$ is a field of characteristic p, then the group algebra $\Bbbk G$ is isomorphic to the quotient of the quiver*



with q vertices by the ideal generated by all paths of length p. $\square$

5.7.8. Let us now assume we have p, q, a and G just as in 5.7.5 but that our ground field $\Bbbk$ has characteristic q. In this situation the group algebra $\Bbbk P$ of the Sylow p-subgroup of G is semisimple and, since P is abelian, basic. If $\zeta \in \Bbbk$ is a primitive pth root of unity and for each $i \in \{0, \dots, p-1\}$ we put $e_i = p^{-1} \sum_{j=0}^{p-1} \zeta^{-ij} r^j$, then the set $E = \{e_0, \dots, e_{p-1}\}$ is a complete orthogonal system of primitive idempotents in $\Bbbk P$ and therefore a complete orthogonal system of idempotents in $\Bbbk G$, which may not be primitive in the bigger larger algebra. In any case, we have a direct sum decomposition $\Bbbk G = \bigoplus_{i=0}^{p-1} \Bbbk G e_i$ as $\Bbbk G$-modules.

Let $i \in \{1, \dots, p-1\}$. We have $re_i = \zeta^i e_i$ and, since $G = \{s^j r^i : 0 \leq j < q, 0 \leq i < p\}$, this implies at once that $\Bbbk G e_i$ is spanned by the set $\mathscr{B}_i = \{s^j e_i : 0 \leq j < p\}$. If $0 \leq j < p$ we have $rs^j = s^j r^{a^j}$, so $rs^j e_i = \zeta^{ia^{-j}} s^j e_i$. The q scalars $\zeta^{ia^0}, \zeta^{ia^{-1}}, \dots, \zeta^{ia^{-(q-1)}}$ are pairwise distinct, because the order of a in $(\mathbb{Z}/p\mathbb{Z})^\times$ is q and ζ is a primitive pth root of unity. Since the elements $s^0 e_i$, $s^1 e_i$, …, $s^{q-1} e_i$ are eigenvectors for r with those scalars as corresponding eigenvalues, they are linearly independent. It follows from this that $\mathscr{B}_i$ is a basis for $\Bbbk G e_i$ and that it has dimension q.

Suppose now that $f : \Bbbk G e_i \to \Bbbk G e_i$ is an endomorphism of the $\Bbbk G$-module $\Bbbk G e_j$. As $f(e_i)$ must be an eigenvector of r corresponding to the eigenvalue ζ^i and the eigenspace for that eigenvalue is spanned by e_i, we see that there exists a scalar $\lambda \in \Bbbk$ such that $f(e_i) = \lambda e_i$. This implies at once that we in fact have $f = \lambda \operatorname{id}_{\Bbbk G e_i}$, since e_i generates $\Bbbk G e_i$ as a module. We can then conclude that $\dim \operatorname{End}_{\Bbbk G}(\Bbbk G e_i) = 1$, so that $\Bbbk G e_i$ is indecomposable and the idempotent e_i primitive.

The submodule $\Bbbk G e_0$ is a complement to $\bigoplus_{i=1}^{p-1} \Bbbk G e_i$, and this last subspace has dimension $(p-1)q$. It follows form this that $\Bbbk G e_0$ has dimension q and, since it is spanned by the set $\mathscr{B}_0 = \{s^j e_0 : 0 \leq j < q\}$, that $\mathscr{B}_0$ is a basis. If $0 \leq j < q$, we have $rs^j e_0 = s^j r^{a^{-j}} e_0 = s^j e_0$, the element r acts as the identity on $\Bbbk G e_0$, and this means that $\Bbbk G e_0$ is naturally a G/P-module and it is clearly the regular G/P-module, which is indecomposable. In this way, we see that e_0 is also a primitive idempotent in $\Bbbk G$.

We thus see that $\Bbbk G = \bigoplus_{i=0}^{p-1} \Bbbk G e_i$ is a decomposition of $\Bbbk G$ as a direct sum of indecomposable submodules and that $E = \{e_0, \dots, e_{p-1}\}$ is a complete orthogonal system of primitive idempotents in $\Bbbk G$. If $0 \leq i, i' < p$, we claim that

> *$\Bbbk G e_i$ and $\Bbbk G e_{i'}$ are isomorphic iff there exists an $l \in \{0, \dots, q-1\}$ such that $i' = i a^{-l}$, and if that is not the case, then there is in fact no homomorphism $\Bbbk G e_i \to \Bbbk G e_{i'}$.*

§5.8. Exercises

5.8.1. If n is a positive integer and A is an algebra, then the matrix algebra $M_n(A)$ is Morita equivalent to A.

CHAPTER 6

Auslander-Reiten theory

§6.1. The category of modules modulo its radical

§6.2. Irreducible morphisms

6.2.1. Proposition. *If M is a module, then* $\operatorname{rad}(M, M) = \operatorname{rad}\operatorname{End}_A(M)$.

Proof. This follows immediately from Proposition 1.3.5 and Corollary 4.2.9. □

6.2.2. Proposition. *Let M and N be indecomposable modules. A morphism $f : M \to N$ is in $\operatorname{rad}(M, N) \setminus \operatorname{rad}^2(M, N)$ iff it is not an isomorphism and whenever Z is a module and $g : Z \to Y$ and $h : X \to Z$ morphisms such that $f = gh$, then either g is a retraction or h is a section.*

Proof. Suppose first that $f : M \to N$ is in $\operatorname{rad}(M, N) \setminus \operatorname{rad}^2(M, N)$. Since M and N are indecomposable, we know from Proposition 1.3.4 that f is not an isomorphism.

Suppose now that Z is a module, that $g : Z \to N$ and $h : M \to Z$ are morphisms and that $f = gh$. Let $Z_1, \dots, Z_n$ be indecomposable submodules of Z such that $Z = \bigoplus_{i=1}^n Z_i$, and for each $i \in \{1, \dots, n\}$ let $q_i : Z_i \to Z$ be the inclusion and $q_i : Z \to Z_i$ be the projection corresponding to that direct sum decomposition. As $\mathrm{id}_Z = \sum_{i=1}^n q_i p_i$, we have $f = \sum_{i=1}^n g q_i p_i h$ and since $f \notin \operatorname{rad}^2(M, N)$, there exists an $i_0 \in \{1, \dots, n\}$ such that either $g q_{i_0} \notin \operatorname{rad}(Z_{i_0}, N)$ or $p_{i_0} h \notin \operatorname{rad}(M, Z_{i_0})$. In the first case, we have that $g q_{i_0} : Z_{i_0} \to N$ is an isomorphism and, consequently, that $g \circ q_{i_0}(g q_{i_0})^{-1} = \mathrm{id}_N$, so that g is a retraction of the map $q_{i_0}(g q_{i_0})^{-1} : N \to Z$. The other case, in which $p_{i_0} h$ is not in $\operatorname{rad}(M, Z_{i_0})$ can be handled in the same way to show that then h is a section.

Let us now prove the converse. Let $f : M \to N$ be a morphism which is not an isomorphism and which satisfies the condition of the statement. Proposition 1.3.4 tells us that $f \in \operatorname{rad}(M, N)$ and we have to show that it is not in $\operatorname{rad}^2(M, N)$. To do this, we suppose otherwise, so that there exist a module Z and morphisms $g \in \operatorname{rad}(Z, N)$ and $h \in \operatorname{rad}(M, Z)$ such that $f = gh$. The hypothesis made on f implies that either g is a retraction or h a section. If the first possibility occurs, there is a morphism $k : N \to Z$ such that $\mathrm{id}_N = gk \in \operatorname{rad}(N, N) = \operatorname{rad}\operatorname{End}_A(N)$, and this is impossible. If instead we have that h is a section, there exists a $l : Z \to M$ such that $\mathrm{id}_M = lm \in \operatorname{rad}(M, M) = \operatorname{rad}\operatorname{End}_A(M)$, which is also impossible. This completes the proof. $\square$

6.2.3. A morphism $f : M \to N$ is ***irreducible*** if it is neither a section nor a retraction and whenever we have a factorization $f = gh$ with $h : M \to Z$ and $g : Z \to N$ through an arbitrary module Z, either g is a retraction or h is a section.

6.2.4. Corollary. *A morphism $f : M \to N$ with M and N indecomposable modules is irreducible iff it belongs to $\mathsf{rad}(M, N) \setminus \mathsf{rad}^2(M, N)$.*

Proof. This is a consequence from Proposition 6.2.2, since a morphism between indecomposable modules is not an isomorphism iff it is neither a section nor a retraction. $\square$

6.2.5. Proposition. *An irreducible morphism in ${}_A\mathsf{mod}$ is either injective or surjective.*

Proof. Suppose that $f : M \to N$ is an irreducible morphism in ${}_A\mathsf{mod}$. There exists a unique factorization

$$M \xrightarrow{f_1} \mathsf{im}\, f \xrightarrow{f_2} N$$

as the composition of the correstriction $f_1 : M \to \mathsf{im}\, f$ of f to $\mathsf{im}\, f$ and the inclusion $f_2 : \mathsf{im}\, f \to N$, and then either f_1 is a section or f_2 a retraction, and then either f_1 is injective or f_2 surjective. This implies, that f is injective or surjective, respectively. $\square$

6.2.6. Proposition. *Let $f : M \to N$ be an irreducible morphism.*

(*i*) *If $N_1 \subsetneq N$ is a proper submodule such that $f(M) \subseteq N_1$, then the correstriction $f|^{N_1} : M \to N_1$ is a section.*

(*ii*) *If $M_1 \subseteq \mathsf{ker}\, f$ is a non-zero submodule, then the induced map $\bar{f} : M/M_1 \to N$ is a retraction.*

Proof. (*i*) If $i : N_1 \to N$ is the inclusion, we have $f = if|^{N_1}$. As N_1 is a proper submodule of N, the map i is not a retraction so $f|^{N_1}$ must be a section because f is irreducible.

(*ii*) If $p : M \to M/M_1$ is the canonical projection, we have $f = \bar{f}p$ and p is not a section because M_1 is a non-zero submodule of M. It follows from the irreducibility of f that $\bar{f}$ is a retraction. $\square$

6.2.7. Proposition. *If $f : M \to N$ is an irreducible morphism and at least one of M or N is indecomposable, then $f \in \mathsf{rad}(M, N)$.*

Proof. Suppose, for example, that M is indecomposable. Let $N_1, \dots, N_n$ be indecomposable submodules of N such that $N = \bigoplus_{i=1}^n N_n$ and for each $i \in \{1, \dots, n\}$ let $q_i : N_i \to N$ be the inclusion and $p_i : N \to N_i$ the projection corresponding to that direct sum decomposition. If $i \in \{1, \dots, n\}$ then the morphism $p_i f$ is not an isomorphism —it if were, then we would have $(p_i f)^{-1} p_i \circ f = \mathrm{id}_N$, yet f is not section— so it belongs to $\mathsf{rad}(M, N_i)$. As rad is an ideal in ${}_A\mathsf{mod}$, this implies that $f = \sum_{i=1}^n q_i p_i f$ is in $\mathsf{rad}(M, N)$. $\square$

6.2.8. Proposition. *Let $f : M \to N$ be an irreducible morphism.*

(*i*) *If M is an indecomposable module and N_1 and N_2 are submodules of N such that $N = N_1 \oplus N_2$, and we let $p_1 : N \to N_1$ be the projection corresponding to this direct sum decomposition, then $p_1 f : M \to N_1$ is also an irreducible morphism.*

(*ii*) *versión dual*

Proof. Let $p_2 : N \to N_2$ be the other canonical projection and let $i_1 : N_1 \to N$ and $i_2 : N_2 \to N$ be the inclusions. As f is not a section, neither is $p_1 f$; on the other hand, since M is indecomposable, $p_1 f$ is not a retraction.

Suppose now that Z is a module and that $h : M \to Z$ and $g : Z \to N_1$ are morphisms such that $p_1 f = gh$.

$$\begin{tikzcd} & X \arrow[dr, "g"] & \\ M \arrow[ur, "h"] \arrow[rr, "p_1 f"'] & & N_1 \end{tikzcd} \qquad \begin{tikzcd} & X \oplus N_2 \arrow[dr, "\begin{pmatrix} i_1 g & i_2 \end{pmatrix}"] & \\ M \arrow[ur, "\begin{pmatrix} h \\ p_2 f \end{pmatrix}"] \arrow[rr, "f"'] & & N \end{tikzcd}$$

The triangle on the right in this diagram then commutes and, since f is irreducible, either $\begin{pmatrix} h \\ p_2 f \end{pmatrix}$ is a section or $\begin{pmatrix} i_1 g & i_2 \end{pmatrix}$ a retraction.

We deal first with the second case, in which there is a morphism $\begin{pmatrix} \delta_1 \\ \delta_2 \end{pmatrix} : N \to X \oplus N_2$ such that $i_1 g \delta_1 + i_2 \delta_2 = \mathrm{id}_N$. It follows that $i_1 g \delta_1 i_1 + i_2 \delta_2 i_1 = i_1$ and, since i_1 and i_2 have images N_1 and N_2, which intersect trivially, this implies that $i_1 g \delta_1 i_1 = i_1$. As i_1 injective, we see that $g \delta_1 = \mathrm{id}_{N_1}$ and, therefore, that g is a retraction.

Suppose now that there is instead a morphism $\begin{pmatrix} \gamma_1 & \gamma_2 \end{pmatrix} : X \oplus N_2 \to M$ such that $\gamma_1 h + \gamma_2 p_2 f = \mathrm{id}_M$. As $f \in \mathsf{rad}(M, N)$, we have $\gamma_2 p_2 f \in \mathsf{rad}(M, M) = \mathsf{rad}\,\mathsf{End}_A(M)$ and therefore $\mathrm{id}_M - \gamma_2 p_2 f$ is invertible in $\mathsf{End}_A(M)$. We then have that

$$(\mathrm{id}_M - \gamma_2 p_2 f)^{-1} \gamma_1 h = \mathrm{id}_M$$

and h is a section. This completes the proof that $p_1 f$ is irreducible. $\square$

6.2.9. Proposition. *Suppose that*

$$0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} P \longrightarrow 0$$

is an exact sequence of modules.

(*i*) *The injection f is irreducible iff for every morphism $h : Q \to P$ there is either a morphism $h_1 : Q \to N$ such that $gh_1 = h$ or a morphism $h_2 : N \to Q$ such that $hh_2 = g$.*

(*ii*) *The surjection g is irreducible iff for every morphism $k : M \to Q$ there is eithr a morphism $k_1 : N \to Q$ such that $k_1 f = k$ or a morphism $k_2 : Q \to M$ such that $k_2 k = f$.*

Proof. To be done □

6.2.10. the cokernel of an irreducible mono and the kernel of an irreducible epi are indecomposable

6.2.11. the maps to the new indecomposables are not irreducible!

6.2.12. Proposition. *The duality $D : {}_A\mathsf{mod} \to \mathsf{mod}_A$ preserves irreducibility of morphisms.*

Proof. Indeed, a morphism $f : M \to N$ in ${}_A\mathsf{mod}$ is a section or a retraction exactly when $D(f) : D(N) \to D(M)$ is a retraction or a section, respectively, so the result follows at once, using the contravariance of D. □

6.2.13. Proposition. *Let e be a primitive idempotent in A and let $S = Ae/\operatorname{rad} Ae$.*

(*i*) *If S is not projective, the inclusion map $i : \operatorname{rad} Ae \to Ae$ is irreducible.*

(*ii*) *If S is not injective and $j : S \to I$ is an injective envelope for S, then j is irreducible.*

Proof. (*i*) If i were a retracton, it would be surjective and therefore an isomorphism: this is impossible as then we would have $Ae = \operatorname{rad} Ae$. On the other hand, if i were a section, then $\operatorname{rad} Ae$ would be a direct summand of Ae, and this is oly possible if $\operatorname{rad} Ae = 0$. In that is case, we have $S = Ae$ and S is projective, contradicting the hypothesis.

Suppose now that Z in a module, that $g : M \to Ae$ and $h : \operatorname{rad} Ae \to M$ are morphisms and $gh = i$. If g is surjective, then as Ae is projective there exists a morphism $u : Ae \to M$ such that $gu = \mathrm{id}_{Ae}$: this means that g is a retraction. If instead g is not surjctive, then its image is contained in $\operatorname{rad} Ae$, as this is the unique maximal submodule of Ae, and then $gh = \mathrm{id}_{\operatorname{rad} Ae}$, so that h is a section.

(*ii*) corresponds to (*i*) under the duality D. □

CHAPTER A

Homological algebra

§1.1. The first extension group

1.1.1. Let us fix an algebra A throughout this section.

1.1.2. If M is a module and $f : P \to M$ is a surjective morphism with P projective, we let $K_f = \ker f$ and write $i_f : K_f \to P$ the inclusion map. For every module N, we have an induced map $i_f^* : \hom_A(P, N) \to \hom_A(K_f, N)$ and we may then consider the vector space $\mathrm{Ext}^1_A(M, N)_f = \operatorname{coker} i_f^*$ and the canonical projection $q_f : \hom_A(K_f, N) \to \mathrm{Ext}^1_A(M, N)_f$. We have an exact sequence

$$0 \longrightarrow \hom_A(M,N) \xrightarrow{f^*} \hom_A(P,N) \xrightarrow{i_f^*} \hom_A(K_f,N) \xrightarrow{q_f} \mathrm{Ext}^1_A(M,N)_f \longrightarrow 0$$

1.1.3. Proposition. *Let $\psi : M \to M'$ be a morphism and let $f : P \to M$ and $f' : P' \to M'$ be two surjective morphisms of modules with projective domains.*

(*i*) *The set $\mathscr{H}(f, f'; \psi)$ of morphisms $h : P \to P'$ such that the diagram*

$$\begin{tikzcd} P \arrow[r, "f"] \arrow[d, "h"'] & M \arrow[d, "\psi"] \\ P' \arrow[r, "f'"] & M' \end{tikzcd}$$

commutes is not empty. If $h \in \mathscr{H}(f, f'; \psi)$, then we have $h(K_f) \subseteq K_{f'}$, so that there exists a unique morphism $\kappa_{f,f'}(h) : K_f \to K_{f'}$ such that $i_{f'}\kappa_{f,f'}(h) = hi_f$.

(*ii*) *There exists a unique morphism of vector spaces*

$$\mathrm{Ext}^1_A(\psi, N)_{f,f'} : \mathrm{Ext}^1_A(M', N)_{f'} \to \mathrm{Ext}^1_A(M, N)_f$$

such that the diagram

$$\begin{tikzcd} \hom_A(P',N) \arrow[r, "i_{f'}^*"] \arrow[d, "h^*"'] & \hom_A(K_{f'},N) \arrow[r, "q_{f'}"] \arrow[d, "\kappa_{f,f'}(h)^*"'] & \mathrm{Ext}^1_A(M',N)_{f'} \arrow[r] \arrow[d, "\mathrm{Ext}^1_A(\psi,N)_{f,f'}"] & 0 \\ \hom_A(P,N) \arrow[r, "i_f^*"] & \hom_A(K_f,N) \arrow[r, "q_f"] & \mathrm{Ext}^1_A(M,N)_f \arrow[r] & 0 \end{tikzcd}$$

commutes and the map $\mathsf{Ext}^1_A(\psi, N)_{f,f'}$ *does not depend on the choice of* h *in* $\mathscr{H}(f, f'; \psi)$.

(*iii*) *If* $\psi' : M' \to M''$ *is another morphism and* $f'' : P'' \to M''$ *another surjective morphism with projective domain, we have*

$$\mathsf{Ext}^1_A(\psi, N)_{f,f'} \circ \mathsf{Ext}^1_A(\psi', N)_{f',f''} = \mathsf{Ext}^1_A(\psi' \circ \psi, N)_{f,f''}. \tag{29}$$

(*iv*) *The linear map*

$$\mathsf{Ext}^1_A(\mathrm{id}_M, N)_{f,f} : \mathsf{Ext}^1_A(M, N)_f \to \mathsf{Ext}^1_A(M, N)_f$$

is the identity of $\mathsf{Ext}^1_A(M, N)_f$.

Proof. The set $\mathscr{H}(f, f'; \psi)$ is not empty because f' is surjective and the module P projective. If $h \in \mathscr{H}(f, f'; \psi)$, then $f'h(K_f) = \psi f(K_f) = 0$, so that $h(K_f) \subseteq K_{f'}$ and there is therefore a unique morphism $\kappa_{f,f'}(h) : K_f \to K_{f'}$ such that $i_{f'}\kappa_{f,f'}(h) = \kappa_{f,f'}(h) i_f$. This proves (*i*) and it follows from it that there is a commutative diagram with exact rows of the form

$$\begin{tikzcd}
\mathsf{hom}_A(P', N) \arrow[r, "i^*_{f'}"] \arrow[d, "h^*"'] & \mathsf{hom}_A(K_{f'}, N) \arrow[r, "q_{f'}"] \arrow[d, "\kappa_{f,f'}(h)^*"'] & \mathsf{Ext}^1_A(M', N)_{f'} \arrow[r] \arrow[d, dashed, "\bar{h}"] & 0 \\
\mathsf{hom}_A(P, N) \arrow[r, "i^*_f"] & \mathsf{hom}_A(K_f, N) \arrow[r, "q_f"] & \mathsf{Ext}^1_A(M, N)_f \arrow[r] & 0
\end{tikzcd} \tag{30}$$

and this implies that there is a morphism $\bar{h} : \mathsf{Ext}^1_A(M', N)_{f'} \to \mathsf{Ext}^1(M, N)_f$ which completes the diagram preserving its commutativity.

If we have two elements $h, k \in \mathscr{H}(f, f'; \psi)$, then

$$f'(h - k) = f'h - f'k = \psi f - \psi f = 0,$$

so that the image of $h - k$ is contained in $K_{f'}$ and there is a morphism $s : P \to K_{f'}$ such that $i_{f'}s = h - k$. Then

$$i_{f'} s i_f = h i_f - k i_f = i_{f'}\kappa_{f,f'}(h) - i_{f'}\kappa_{f,f'}(k) = i_{f'}(\kappa_{f,f'}(h) - \kappa_{f,f'}(k))$$

and, since $i_{f'}$ is injective, we see that $s i_f = \kappa_{f,f'}(h) - \kappa_{f,f'}(k)$. If now $\phi \in \mathsf{hom}_A(K_{f'}, N)$, then

$$\kappa_{f,f'}(h)^*(\phi) - \kappa_{f,f'}(k)^*(\phi) = \phi\kappa_{f,f'}(h) - \phi\kappa_{f,f'}(k) = \phi s i_f = i^*_f(\phi s)$$

and this implies that the linear maps $\bar{h}$ and $\bar{k}$ are equal. We put $\mathsf{Ext}^1_A(\psi, N)_{f,f'} = \bar{h}$; our argument shows that this is independent of the choice of h in $\mathscr{H}(f, f'; \psi)$.

Let us consider a second morphism $\psi' : M' \to M''$ and a third surjective morphism $f'' : P'' \to M''$ with P'' projective and let $l \in \mathscr{H}(f', f''; \psi')$, so that the diagram

$$\begin{tikzcd}
\hom_A(P'',N) \arrow[r, "i_{f''}^*"] \arrow[d, "l^*"'] & \hom_A(K_{f''},N) \arrow[r, "q_{f''}"] \arrow[d, "\kappa_{f',f''}(l)^*"'] & \operatorname{Ext}^1_A(M'',N)_{f''} \arrow[r] \arrow[d, dashed, "\operatorname{Ext}^1_A(\psi',N)_{f',f''}"] & 0 \\
\hom_A(P',N) \arrow[r, "i_{f'}^*"] & \hom_A(K_{f'},N) \arrow[r, "q_{f'}"] & \operatorname{Ext}^1_A(M',N)_{f'} \arrow[r] & 0
\end{tikzcd} \tag{31}$$

is commutative. We have $i_{f''}\kappa_{f',f''}(l)\kappa_{f,f'}(h) = lhi_f$, so that $\kappa_{f,f''}(lh) = \kappa_{f',f''}(l)\kappa_{f,f'}(h)$. As $h^*l^* = (lh)^*$ and $\kappa_{f,f'}(h)^*\kappa_{f',f''}(l)^* = (\kappa_{f',f''}(l)\kappa_{f,f'}(h))^*$, the commutativity of the diagrams (30) and (31) implies that the diagram

$$\begin{tikzcd}
\hom_A(P'',N) \arrow[r, "i_{f''}^*"] \arrow[d, "(lh)^*"'] & \hom_A(K_{f''},N) \arrow[r, "q_{f''}"] \arrow[d, "\kappa_{f,f''}(lh)^*"'] & \operatorname{Ext}^1_A(M'',N)_{f''} \arrow[r] \arrow[d, dashed, "\operatorname{Ext}^1_A(\psi,N)_{f,f'}\circ\operatorname{Ext}^1_A(\psi',N)_{f',f''}"] & 0 \\
\hom_A(P,N) \arrow[r, "i_{f}^*"] & \hom_A(K_{f},N) \arrow[r, "q_{f}"] & \operatorname{Ext}^1_A(M,N)_{f} \arrow[r] & 0
\end{tikzcd}$$

is also commutative. As $lh \in \mathscr{H}(f, f''; \psi' \circ \psi)$, this tells us, in view of what we have already proved, that the equality (29) holds.

To prove the remaining statement (*iv*) we need only observe that $\mathrm{id}_P \in \mathscr{H}(f, f; \mathrm{id}_M)$, that $\kappa_{f,f}(\mathrm{id}_M) = \mathrm{id}_{K_f}$, and that the diagram

$$\begin{tikzcd}
\hom_A(P,N) \arrow[r, "i_{f}^*"] \arrow[d, "\mathrm{id}_P^*"'] & \hom_A(K_{f},N) \arrow[r, "q_{f}"] \arrow[d, "\kappa_{f,f}(\mathrm{id}_P)^*"'] & \operatorname{Ext}^1_A(M,N)_{f} \arrow[r] \arrow[d, dashed, "\mathrm{id}_{\operatorname{Ext}^1_A(M,N)_f}"] & 0 \\
\hom_A(P,N) \arrow[r, "i_{f}^*"] & \hom_A(K_{f},N) \arrow[r, "q_{f}"] & \operatorname{Ext}^1_A(M,N)_{f} \arrow[r] & 0
\end{tikzcd}$$

is commutative. □

1.1.4. A first consequence of Proposition 1.1.3 is the following result that means that $\operatorname{Ext}^1_A(M,N)_f$ is in a sense independent of f:

Corollary. *Let M be a module and let $f : P \to M$ and $f' : P' \to M$ be two surjective morphisms with projective domains. For every module N the linear map*

$$\operatorname{Ext}^1_A(\mathrm{id}_M, N)_{f,f'} : \operatorname{Ext}^1_A(M,N)_{f'} \to \operatorname{Ext}^1_A(M,N)_f$$

is an isomorphism.

It is an important and remarkable fact that this isomorphism is canonical.

Proof. Indeed, according to parts (*iii*) and (*iv*) of Proposition 1.1.3 we have

$$\operatorname{Ext}^1_A(\mathrm{id}_M, N)_{f,f'} \circ \operatorname{Ext}^1_A(\mathrm{id}_M, N)_{f',f} = \operatorname{Ext}^1_A(\mathrm{id}_M, N)_{f,f} = \mathrm{id}_{\operatorname{Ext}^1_A(M,N)_f}$$

and, similarly,

$$\mathsf{Ext}^1_A(\mathrm{id}_M, N)_{f',f} \circ \mathsf{Ext}^1_A(\mathrm{id}_M, N)_{f,f'} = \mathrm{id}_{\mathsf{Ext}^1_A(M,N)_{f'}}.$$

The maps $\mathsf{Ext}^1_A(\mathrm{id}_M, N)_{f',f}$ and $\mathsf{Ext}^1_A(\mathrm{id}_M, N)_{f,f'}$ are therefore mutually inverse. □

1.1.5. Let M be a module, $\phi : N \to N'$ a morphism and $f : P \to M$ a surjective morphism with projective domain. The solid arrows in the diagram

$$\begin{tikzcd} \mathsf{hom}_A(P,N) \arrow[r, "i_f^*"] \arrow[d, "\phi_*"] & \mathsf{hom}_A(K_f,N) \arrow[r, "q_f"] \arrow[d, "\phi_*"] & \mathsf{Ext}^1_A(M,N)_f \arrow[r] \arrow[d, dashed, "\mathsf{Ext}^1_A(M,\phi)_f"] & 0 \\ \mathsf{hom}_A(P,N') \arrow[r, "i_f^*"] & \mathsf{hom}_A(K_f,N') \arrow[r, "q_f"] & \mathsf{Ext}^1_A(M,N')_f \arrow[r] & 0 \end{tikzcd}$$

commute and the rows are exact, so there is exactly one linear map

$$\mathsf{Ext}^1_A(M,\phi)_f : \mathsf{Ext}^1_A(M,N)_f \to \mathsf{Ext}^1_A(M,N')_f$$

which completes the diagram preserving the commutativity.

1.1.6. Proposition. *Let M be a module and let $f : P \to M$ be a surjective morphism of modules with P projective.*

(*i*) *If N is a module, then we have*

$$\mathsf{Ext}^1_A(M, \mathrm{id}_N)_f = \mathrm{id}_{\mathsf{Ext}^1_A(M,N)_f} : \mathsf{Ext}^1_A(M,N)_f \to \mathsf{Ext}^1(M,N)_f.$$

(*ii*) *If $\phi : N \to N'$ and $\phi' : N' \to N''$ are morphisms of modules, then*

$$\mathsf{Ext}^1_A(M,\phi')_f \circ \mathsf{Ext}^1_A(M,\phi)_f = \mathsf{Ext}^1_A(M,\phi' \circ \phi)_f.$$

(*iii*) *If $\psi : M \to M'$ is a morphism and $f' : P' \to M'$ is another surjective morphism with projective domain and $\phi : N \to N'$ is a morphism of modules, then the diagram*

$$\begin{tikzcd} \mathsf{Ext}^1_A(M',N)_{f'} \arrow[r, "\mathsf{Ext}^1_A(M,\phi)_{f'}"] \arrow[d, "\mathsf{Ext}^1_A(\psi,N)_{f,f'}"'] & \mathsf{Ext}^1_A(M',N')_{f'} \arrow[d, "\mathsf{Ext}^1_A(\psi,N')_{f,f'}"] \\ \mathsf{Ext}^1_A(M,N)_f \arrow[r, "\mathsf{Ext}^1_A(M,\phi)_f"] & \mathsf{Ext}^1_A(M,N')_{f'} \end{tikzcd}$$

commutes.

Proof. To prove (*i*) we need only observe that the diagram

$$\begin{tikzcd} \mathsf{hom}_A(P,N) \arrow[r, "i_f^*"] \arrow[d, "(\mathrm{id}_N)_*"] & \mathsf{hom}_A(K_f,N) \arrow[r, "q_f"] \arrow[d, "(\mathrm{id}_N)_*"] & \mathsf{Ext}^1_A(M,N)_f \arrow[r] \arrow[d, dashed, "\mathrm{id}_{\mathsf{Ext}^1_A(M,N)_f}"] & 0 \\ \mathsf{hom}_A(P,N) \arrow[r, "i_f^*"] & \mathsf{hom}_A(K_f,N) \arrow[r, "q_f"] & \mathsf{Ext}^1_A(M,N)_f \arrow[r] & 0 \end{tikzcd}$$

commutes. Similarly, the claim of (*ii*) follows at once from the commutativity of

$$\begin{tikzcd}
\hom_A(P,N) \arrow[r, "i_f^*"] \arrow[d, "(\phi'\phi)_*"] & \hom_A(K_f,N) \arrow[r, "q_f"] \arrow[d, "(\phi'\phi)_*"] & \operatorname{Ext}^1_A(M,N)_f \arrow[r] \arrow[d, dashed, "\operatorname{Ext}^1_A(M,\phi')_f \circ \operatorname{Ext}^1_A(M,\phi)_f"] & 0 \\
\hom_A(P,N'') \arrow[r, "i_f^*"] & \hom_A(K_f,N'') \arrow[r, "q_f"] & \operatorname{Ext}^1_A(M,N'')_f \arrow[r] & 0
\end{tikzcd}$$

To be done □

1.1.7. Proposition. *Let M and N be a modules and let $f : P \to M$ and $f' : P' \to M$ be surjective morphisms with projective domains.*

(*i*) *There is a right $\operatorname{End}_A(M)$-module structure on $\operatorname{Ext}^1_A(M,N)_f$ with action such that*

$$\xi \cdot \psi = \operatorname{Ext}^1_A(\psi,N)_{f,f}(\xi)$$

for all $\xi \in \operatorname{Ext}^1_A(M,N)_f$ and all $\psi \in \operatorname{End}_A(M)$. The linear map

$$\operatorname{Ext}^1_A(\mathrm{id}_M,N)_{f,f'} : \operatorname{Ext}^1_A(M,N)_{f'} \to \operatorname{Ext}^1(M,N)_f$$

is an isomorphism of right $\operatorname{End}_A(M)$-modules.

(*ii*) *There is a left $\operatorname{End}_A(N)$-module structure on $\operatorname{Ext}^1_A(M,N)_f$ with action given by*

$$\phi \cdot \xi = \operatorname{Ext}^1_A(M,\phi)_f(\xi)$$

for all $\phi \in \operatorname{End}_A(N)$ and all $\xi \in \operatorname{Ext}^1_A(M,N)_f$. The linear map

$$\operatorname{Ext}^1_A(\mathrm{id}_M,N)_{f,f'} : \operatorname{Ext}^1_A(M,N)_{f'} \to \operatorname{Ext}^1_A(M,N)_f$$

is an isomorphism of $\operatorname{End}_A(N)$-modules.

Proof. REWRITE The action of $\operatorname{End}_A(M)$ described in (*i*) is linear because the map $\operatorname{Ext}^1_A(\psi,N)_{f,f}$ is linear for all $\psi \in \operatorname{End}_A(M)$. The associativity and unitality of this action, on the other hand, follow immediately from parts (*iii*) and (*iv*) of Proposition 1.1.3.

Similarly, to show that the map $\operatorname{Ext}^1_A(\mathrm{id}_M,N)_{f,f'}$ of (*ii*) is an isomorphism of right $\operatorname{End}_A(M)$-modules we have to show that it is bijective, and this is the content of Corollary 1.1.4, and that for all $\psi \in \operatorname{End}_A(M)$ we have

$$\operatorname{Ext}^1_A(\psi,M)_{f,f} \circ \operatorname{Ext}^1_A(\mathrm{id}_M,N)_{f,f'} = \operatorname{Ext}^1_A(\mathrm{id}_M,N)_{f,f'} \circ \operatorname{Ext}^1_A(\psi,N)_{f',f'}.$$

This follows at once from part (*iii*) of Proposition 1.1.3. □

Proof. That the action of $\operatorname{End}_A(N)$ on $\operatorname{Ext}^1_A(M,N)_f$ defined in (*i*) is unital and associative precisely is precisely the content of (*i*) and (*ii*) of Proposition 1.1.6. Since it is clearly linear, it does therefore define a module structure.

(*ii*) To be done □

1.1.8. Proposition. *If M and N are modules and $f : P \to M$ is a surjective morphism with projective domain, then the left $\mathsf{End}_A(N)$-module structure and the right $\mathsf{End}_A(M)$-module structure on $\mathsf{Ext}^1_A(M, N)_f$ constructed in Proposition 1.1.7 turn this vector space into an $(\mathsf{End}_A(N), \mathsf{End}_A(M))$-bimodule.*

Proof. To be done $\square$

§1.2. Extensions

References

[Art1927] Emil Artin, *Zur Theorie der hyperkomplexen Zahlen*, Abh. Math. Sem. Univ. Hamburg **5** (1927), no. 1, 251–260 (German). MR3069481

[Büh2010] Theo Bühler, *Exact categories*, Expo. Math. **28** (2010), no. 1, 1–69, available at http://arxiv.org/abs/0811.1480v2. MR2606234 (2011e:18020)

[Bur1905] William Burnside, *On the Condition of Reducibility of any Group of Linear Substituions*, Proc. London Math. Soc. **S2-3** (1905), no. 1, 430, available at http://plms.oxfordjournals.org/content/s2-3/1/430.full.pdf+html. MR1575942

[Fit1935] Hans Fitting, *Über die direkten Produktzerlegungen einer Gruppe in direkt unzerlegbare Faktoren*, Math. Z. **39** (1935), no. 1, 16–30, available at http://resolver.sub.uni-goettingen.de/purl?PPN266833020_0039. MR1545486

[Hig1954] Donald G. Higman, *Indecomposable representations at characteristic p*, Duke Math. J. **21** (1954), 377–381.

[Höl1889] Otto Hölder, *Zurückführung einer beliebigen algebraischen Gleichung auf eine Kette von Gleichungen.*, Math. Ann. **34** (1889), 26–56, available at http://resolver.sub.uni-goettingen.de/purl?PPN235181684_0034.

[Jor1989] Camille Jordan, *Traité des substitutions et des équations algébriques*, Les Grands Classiques Gauthier-Villars. [Gauthier-Villars Great Classics], Éditions Jacques Gabay, Sceaux, 1989 (French). Reprint of the 1870 original. MR1188877 (94c:01039)

[Kap1969] Irving Kaplansky, *Fields and rings*, The University of Chicago Press, Chicago, Ill.-London, 1969. MR0269449 (42 #4345)

[Kar] Gregory Karpilovsky, *The Jacobson radical of group algebras*. To be done.

[Kru1925] Wolfgang Krull, *Über verallgemeinerte endliche Abelsche Gruppen*, Math. Z. **23** (1925), no. 1, 161–196, available at http://resolver.sub.uni-goettingen.de/purl?GDZPPN002368528. MR1544736

[Lam1998] Tsit Yuen Lam, *A Theorem of Burnside on Matrix Rings*, The American Mathematical Monthly **105** (1998), no. 7, 651–653, available at http://www.jstor.org/stable/2589248.

[Mas1899] Heinrich Maschke, *Beweis des Satzes, dass diejenigen endlichen linearen Substitutionsgruppen, in welchen einige durchgehends verschwindende Coefficienten auftreten, intransitiv sind*, Math. Ann. **52** (1899), no. 2-3, 363–368, available at http://resolver.sub.uni-goettingen.de/purl?PPN235181684_0052. MR1511061

[Mas1898] Heinrich Maschke, *Ueber den arithmetischen Charakter der Coefficienten der Substitutionen endlicher linearer Substitutionsgruppen*, Math. Ann. **50** (1898), no. 4, 492–498, available at http://resolver.sub.uni-goettingen.de/purl?PPN235181684_0050. MR1511011

[vN1936] John von Neumann, *On regular rings*, Proc. Natl. Acad. Sci. USA **22** (1936), 707–713.

[Rem1911] Robert Remak, *Über verallgemeinerte endliche Abelsche Gruppen*, J. Crelle **139** (1911), no. 1, 293–308, available at http://resolver.sub.uni-goettingen.de/purl?GDZPPN00216731X.

[Sch1929] Otto Schmidt, *Über unendliche Gruppen mit endlicher Kette*, Math. Z. **29** (1929), 34–41, available at `http://resolver.sub.uni-goettingen.de/purl?GDZPPN002370557`. MR1544991

[Sch1905] Issai Schur, *Neue Begründung der Theorie der Gruppencharaktere*, Berliner Sitzungsber. (1905), 406–432, available at `http://resolver.sub.uni-goettingen.de/purl?GDZPPN002252120`.

[Wal1961] D. A. R Wallace, *On the radical of a group algebra*, Proc. Amer. Math. Soc. **72** (1961), 133–137.

[Wed1908] J. H. MacLagan Wedderburn, *On Hypercomplex Numbers*, Proc. London Math. Soc. **S2-6** (1908), no. 1, 77. MR1575142