Representation theory of finite-dimensional algebras

Markus Linckelmann

November 18, 2014

Introduction

The representation theory of finite-dimensional algebras over fields is the systematic study of module categories of algebras - or, in less mundane terminology, the theory of subalgebras of matrix algebras. While algebras have been studied for a long time and in many areas of mathematics, some of the concepts which are the foundational corner stones of a systematic theory are more recent. This includes, for instance the notion of a quiver of an algebra, which appears in work of Gabriel during the 1970s. It also includes the systematic use of categorical and homological methods. For the purpose of the present notes, we have chosen to make category theoretic comments from the very beginning, and collect in an appendix the relevant terminology as a reference. The same applies for the tensor product, which will be mentioned early on, with an appendix describing its construction and main properties in a systematic way.

Contents

1 Associative algebras

If not stated otherwise we denote by k a field.

Definition 1.1. A k-algebra is a nonzero k-vector space A together with a unital associative k-bilinear map

$$A \times A \to A, \quad (a, b) \mapsto ab \ ,$$

called the *product* or *multiplication in* A; more explicitly, there is an element 1_A in A, called *unit element*, such that $1_A a = a = a 1_A$ for all $a \in A$, and we have $(ab)c = a(bc)$ for all a, b, $c \in A$.

There is an equivalent way of defining algebras as follows. The multiplication in A is by definition k-bilinear and associative. Thus the map sending $\lambda \in k$ to $\lambda 1_A \in A$ is a ring homomorphism. The image of this ring homomorphism is contained in the *center of* A, denoted $Z(A)$, and defined by

$$Z(A) = \{z \in A \mid az = za \ \forall \ a \in A\} \ .$$

Conversely, if A is a ring together with a ring homomorphism $\sigma : k \to Z(A)$, then σ induces a k-vector space structure on A in such a way that the multiplication in A becomes k-bilinear, and hence A becomes a k-algebra. A k-algebra A is *commutative* if $ab = ba$ for all a, $b \in A$, or equivalently, if $A = Z(A)$.

Since the multiplication in A is bilinear, it extends uniquely to a linear map $A \otimes_k A \to A$ sending $a \otimes b$ to ab, for all a, $b \in A$. The unit element 1_A of A is easily seen to be unique: if e is another element in A satisfying $ea = a = ae$ for all $a \in A$, then $e = e1_A = 1_A$. The condition that the multiplication on A is associative with a unit element is equivalent to asserting that A, endowed with the multiplication, is a monoid. There are some important examples of algebras which are neither unital nor associative - such as Lie algebras - but we will not consider these in this course. The definition of a k-algebra makes sense with k replaced by an arbitrary commutative ring. Any ring R can be viewed as a $\mathbb{Z}$-algebra.

Whenever possible we consider mathematical objects with their structure preserving maps as a category. The k-algebras form a category, with the following notion of morphisms.

Definition 1.2. Let A and B be k-algebras. A *homomorphism of k-algebras from A to B* is a k-linear map $\alpha : A \to B$ satisfying $\alpha(ab) = \alpha(a)\alpha(b)$ for all a, $b \in A$ and $\alpha(1_A) = 1_B$. The *kernel of* α is the subspace $\ker(\alpha) = \{a \in A \mid \alpha(a) = 0\}$ of A.

The composition of two algebra homomorphisms is an algebra homomorphism. The identity map on A is an algebra homomorphism. An algebra homomorphism $\alpha : A \to B$ is called an *isomorphism* if there exists an algebra homomorphism $\beta : B \to A$ such that $\beta \circ \alpha = \mathrm{Id}_A$ and $\alpha \circ \beta = \mathrm{Id}_B$. An algebra homomorphism $A \to A$ which is an isomorphism is called an *automorphism* of A. An algebra homomorphism is a ring homomorphism, but not every ring homomorphism between two k-algebras is an algebra homomorphism in general because it need not be compatible with the scalar multiplication. It is possible for two k-algebras to be isomorphic as rings but not as k-algebras. A *subalgebra of a k-algebra* A is a k-subspace B of A containing 1_A such that the multiplication in A restricts to a multiplication on B, or equivalently, such that the inclusion map $B \subseteq A$ is an algebra homomorphism. For instance, $Z(A)$ is a commutative subalgebra of A.

We have the usual ringtheoretic notions of ideals in an algebra A. A *left ideal of* A is a subset I of A satisfying $aI \subseteq I$, a *right ideal of* A is a subspace J of A satisfying $Ja \subseteq J$, and a 2-*sided* *ideal*, or simply *ideal of* A is a subspace I which is both a left and right ideal in A. A left or right or two-sided ideal I in A is automatically a k-subspace of A, since it must satisfy $\lambda a = a\lambda \in I$ for any $a \in I$ and any $\lambda \in k$.

An ideal (or left ideal or right ideal) in A is called *proper* if it is different from A. If I is a proper ideal in A, then the vector space quotient A/I inherits a well-defined algebra structure with multiplication induced by that in A; that is, $(a+I)(b+I) = ab + I$ for all a, $b \in A$, and the unit element of A/I is $1 + I$; morover, the canonical surjection $A \to A/I$ sending a to $a + I$ is a surjective algebra homomorphism with kernel equal to I.

Proposition 1.3. *Let* A, B *be* k*-algebras, and let* $\alpha : A \to B$ *be a* k*-algebra homomorphism. Then* $\mathrm{Im}(\alpha)$ *is a subalgebra of* B, $\ker(\alpha)$ *is an ideal in* A, *and we have an algebra isomorphism* $A/\ker(\alpha) \cong \mathrm{Im}(\alpha)$ *sending* $a + \ker(\alpha)$ *to* $\varphi(a)$.

Proof. Clearly $\ker(\alpha)$ and $\mathrm{Im}(\alpha)$ are k-subspaces in A and B, resepctively, and the standard isomorphism theorem for vector spaces implies that we have an isomorphism of vector spaces $A/\ker(\alpha) \cong \mathrm{Im}(\alpha)$ mapping $a + \ker(\alpha)$ to $\varphi(a)$, for all $a \in A$. If b, $b' \in \mathrm{Im}(\alpha)$, then there exist a, $a' \in A$ such that $\alpha(a) = b$ and $\alpha(a') = b'$. Thus $bb' = \alpha(a)\alpha(a') = \alpha(aa') \in \mathrm{Im}(\alpha)$. We have $1_B = \alpha(1_A) \in \mathrm{Im}(\alpha)$. This implies that $\mathrm{Im}(\alpha)$ is a subalgebra of B. Let $a \in \ker(\alpha)$ and $a' \in A$. Then $\alpha(aa') = \alpha(a)\alpha(a') = 0$, hence $\ker(\alpha)$ is a right ideal. A similar argument shows that $\ker(\alpha)$ is a left ideal, hence an ideal in A. A trivial verification shows that the linear isomorphism $A/\ker(\alpha) \cong \mathrm{Im}(\alpha)$ sending $a + \ker(\alpha)$ to $\alpha(a)$ is compatible with the products, hence an isomorphism of k-algebras. $\square$

If I, J are two ideals in a k-algebra, then the set $I + J = \{a + b \mid a \in I,\ b \in J\}$ is again an ideal in A, called the sum of I and J. The set IJ consisting of all finite sums of the form $\sum_{i=1}^{n} a_i b_i$, with $a_i \in I$, $b_i \in J$, is again an ideal, called the product of I and J. Note that it is not sufficient to define IJ as the set of elements of the form ab, with $a \in I$ and $b \in J$, because this set is not closed under taking sums. The definition of sums and products of two ideals extend to finitely many ideals in the obvious way.

Examples 1.4.

(1) The field k is itself a k-algebra. More generally, for any positive integer n, the vector space $M_n(k)$ of $n \times n$ matrices with coefficients in k, together with the usual matrix multiplication, is a k-algebra.

(2) Let V be a k-vector space. The space $\mathrm{End}_k(V)$ of all k-linear transformations on V, with the composition of maps as multiplication, is a k-algebra. If $\dim_k(V) = n$ is finite, then by choosing a k-basis of V and writing endomorphisms of V in terms of this basis yields an isomorphism of k-algebras $\mathrm{End}_k(V) \cong M_n(k)$.

(3) The polynomial ring $k[X_1, X_2, \ldots, X_n]$ in n commuting variables is a k-algebra.

(4) Let G be a group. The group algebra of G over k, denoted kG, is the vector space having a basis indexed by the elements of G, with multiplication obtained by extending the product in G bilinearly. More explicitly, kG is the set of all formal sums $\sum_{x \in G} \lambda_x x$ with $\lambda_x \in k$ of which only finitely many are non zero, componentwise sum and scalar multiplication, and product given by

$$(\sum_{x\in G} \lambda_x x)(\sum_{y \in G} \mu_y y) = \sum_{z \in Z} \tau_z z \ ,$$

where for each $z \in G$ we have $\tau_z = \sum_{(x,y)} \lambda_x \mu_y$, with (x, y) running over all pairs in $G \times G$ such that $xy = z$. The assignment sending a group G to its group algebra kG is a functor from the category **Grps** of groups to the category $\mathbf{Alg}(k)$ of k-algebras: any group homomorphism $\varphi : G \to H$ induces a unique algebra homomorphism $kG \to kH$ which sends the basis element x in kG to the basis element $\varphi(x)$ in kH, where $x \in G$. This example makes sense with k replaced by an arbitrary commutative ring.

(5) Let $\mathcal{C}$ be a small category. The *category algebra of* $\mathcal{C}$ *over* k is the k-vector space, denoted $k\mathcal{C}$, having as a basis the set $\mathrm{Hom}_{\mathcal{C}}$ of all morphisms in $\mathcal{C}$, with unique bilinear multiplication given by $\psi\varphi = \psi \circ \varphi$ if φ, ψ are two morphisms in $\mathcal{C}$ for which the composition $\psi \circ \varphi$ is defined, and $\psi\varphi = 0$ in $k\mathcal{C}$ if the morphisms ψ and φ cannot be composed in this order. Unlike the preceding examples, a category alegbra need not be unitary. More precisely, $k\mathcal{C}$ is unital if and only if the object set $\mathrm{Ob}(\mathcal{C})$ is finite; in that case, the formal sum $\sum_{X \in \mathrm{Ob}(\mathcal{C})} \mathrm{Id}_X$ of all identity morphisms is the unit element in $k\mathcal{C}$. Group algebras are special cases of category algebras: given a group G, we define a category $\mathbf{G}$ with a single object $*$ and endomorphism set equal to G, such that the composition of morphisms in $\mathbf{G}$ is induced by the product in G. Then the group algebra kG is isomorphic in an obvious way to the category algebra $k\mathbf{G}$. As before, this example makes sense with k replaced by an arbitrary commutative ring.

Definition 1.5. Let A be a k-algebra and $a \in A$. The element a is called *invertible* if there exists an element a^{-1} such that $aa^{-1} = 1_A = a^{-1}a$. We denote by $A^\times$ the set of invertible elements in A. The element a is called *nilpotent* if $a^n = 0$ for some positive integer n.

The set $A^\times$ is a group with unit element 1_A. This is the subgroup of invertible elements of the multiplicative monoid $(A, \cdot)$. If a is invertible, then its inverse a^{-1} is unique. Indeed, if a' also satisfies $aa' = 1_A = a'a$, then $a' = a'1_A = a'(aa^{-1}) = (a'a)a^{-1} = 1_A a^{-1} = a^{-1}$. If A is finite-dimensional and if a, $a' \in A$ such that $aa' = 1_A$, then a is invertible and $a' = a^{-1}$. Indeed, if $aa' = 1$, then the map sending $b \in A$ to ba is injective; since if $ba = 0$, then also $0 = baa' = b1_A = b$. But A is a finite-dimensional vector space, so an injective map on A is also surjective. Thus there exists $b \in A$ such that $ba = 1_A$. Then $b = b1_A = b(aa') = (ba)a' = 1_A a' = a'$, and hence $a' = a^{-1}$. If a is nilpotent, then $1 - a$ is invertible. Indeed, let n be a positive integer such that $a^n = 0$. Then $1 = 1 - a^n = (1 - a)(1 + a + a^2 + \cdots + a^{n-1})$, hence $1 - a$ is invertible with inverse $\sum_{i=0}^{n-1} a^i$. If $c \in A^\times$, then the map $a \mapsto {}^c a = cac^{-1}$ given by conjugation with c is an algebra automorphism of A. Any algebra automorphism of A given by conjugation with an element in $A^\times$ is called an *inner automorphism of* A.

There are various ways to construct new algebras from given algebras.

Definition 1.6. The *opposite algebra of a* k*-algebra* A, denoted A^{op}, is defined as the k-algebra which is equal to A as a k-vector space, but endowed with the opposite multiplication $a \cdot b = ba$ for all a, $b \in A$. Here $a \cdot b$ is the product in A^{op} and ba the product in the original algebra A.

Clearly $(A^{\mathrm{op}})^{\mathrm{op}} = A$. We have $A = A^{\mathrm{op}}$ if and only if A is commutative. It is though possible for a noncommutative algebra to be isomorphic to its opposite algebra, albeit via a nontrivial isomorphism. This is, for instance the case if A is a group algebra, because a group is isomorphic to its opposite via the map sending a group element to its inverse. Similarly, any matrix algebra is isomorphic to its opposite algebra via the map sending a matrix to its transpose; see the exercises at the end of this section.

Definition 1.7. Let A and B be k-algebras. The direct product of A and B is the k-algebra which is as a k-vector space equal to the Cartesian product

$$A \times B = \{(a, b) \mid a \in A,\ b \in B\}$$

endowed with the componentwise multiplication $(a, b)(a', b') = (aa', bb')$, where a, $a' \in A$ and b, $b' \in B$. An algebra is called *indecomposable* if it cannot be written as a direct product of two algebras.

The unit element of $A \times B$ is $(1_A, 1_B)$, and we have an obvious isomorphism of groups of invertible elements $(A \times B)^\times \cong A^\times \times B^\times$. More precisely, we have $(a, b) \in (A \times B)^\times$ if and only if $a \in A^\times$ and $b \in B^\times$, and in that case we have $(a, b)^{-1} = (a^{-1}, b^{-1})$. Given two k-algebras A and B, we have two canonical maps $\pi_A : A \times B \to A$ and $\pi_B : A \times B \to B$ sending $(a, b) \in A \times B$ to a and b, respectively. These two maps are algebra homomorphisms, called the *canonical projections of $A \times B$ onto A and B.* They satisfy the following universal property.

Proposition 1.8. *Let A, B be k-algebras, and let π_A, π_B be the canonical projections of $A \times B$ onto A and B, respectively. Then for any triple (C, τ_A, τ_B) consisting of a k-algebra C and algebra homomorphisms $\tau_A : C \to A$ and $\tau_B : C \to B$, there is a unique algebra homomorphism $\alpha : C \to A \times B$ satisfying $\tau_A = \pi_A \circ \alpha$ and $\tau_B = \pi_B \circ \alpha$.*

Proof. Given (C, τ_A, τ_B) as in the statement, we define α by $\alpha(c) = (\tau_A(c), \tau_B(c))$. This is an element in $A \times B$. Since both τ_A, τ_B are algebra homomorphisms, so is α. The equalities $\tau_A = \pi_A \circ \alpha$ and $\tau_B = \pi_B \circ \alpha$ hold trivially. We need to verify that α is unique with this property. Since an element in $A \times B$ is uniquely determined by its projections into A and B, it follows that α is unique with this property. □

The universal property of the direct product of algebras is used to extend the notion of a direct product to objects in arbitrary categories. What 1.8 says is that $(A \times B, \pi_A, \pi_B)$ is a terminal object in the category of triples of the form (C, τ_A, τ_B). Note that A and B are not unitary subalgebras of $A \times B$. Last but not least, taking the tensor product $A \otimes_k B$ of two k-algebras A and B yields an algebra, with multiplication satisfying

$$(a \otimes b)(a' \otimes b') = (ab) \otimes (a'b')$$

for all a, $a' \in A$ and b, $b' \in B$.

Exercises 1.9. Most of the following exercises are verifications of statements in the preceding section.

(1) Let A be a k-algebra and I a proper ideal. Show that the vector space quotient A/I has a unique k-algebra structure with multiplication given by $(a + I)(b + I) = ab + I$ for all a, $b \in A$. Deduce that the canonical map $A \to A/I$ sending $a \in A$ to $a + I$ is a surjective algebra homomorphism with kernel I.

(2) Let A and B be k-algebras. Show that every ideal in $A \times B$ is of the form $I \times J$ for some ideal I in A and some ideal J in B.

(3) Let G be a group. Show that there is a canonical k-algebra isomorphism $kG \cong (kG)^{\mathrm{op}}$ induced by the map sending any group element to its inverse.

(4) Let G be a finite group. For $x \in G$ denote by $\underline{x}$ the sum, in kG, of all elements in G which are conjugate to x (that is, of the form yxy^{-1} for some $y \in G$). We call $\underline{x}$ the *conjugacy class sum of x in G*. Show that $\underline{x} \in Z(kG)$. Show that $\underline{x} = \underline{y}$ if and only if x and y are conjugate in G. Show that the set of conjugacy class sums $\underline{x}$, with x running over a set of representatives of the conjugacy classes in G, is a k-basis of $Z(kG)$.

(5) Let G, H be groups. Show that there is a canonical k-algebra isomorphism $k(G \times H) \cong kG \otimes_k kH$.

(6) Let n be a positive integer. Show that there is a canonical k-algebra isomorphism $M_n(k) \cong M_n(k)^{\mathrm{op}}$ sending a matrix to its transpose.

(7) Let A be a finite-dimensional k-algebra, and let a, $b \in A$. Show that $ab \in A^\times$ if and only if $a \in A^\times$ and $b \in A^\times$.

(8) Let A be a k-algebra.

(i) Show that the set of algebra automorphisms of A is a group. This group will be denoted by $\mathrm{Aut}(A)$.

(ii) Let $c \in A^\times$. Show that the map sending $a \in A$ to cac^{-1} is an algebra automorphism of A. Any automorphism of this form is called an *inner automorphism* of A. The set of inner automorphisms of A is denoted by $\mathrm{Inn}(A)$.

(iii) Show that $\mathrm{Inn}(A)$ is a normal subgroup of $\mathrm{Aut}(A)$. The corresponding quotient group $\mathrm{Out}(A) = \mathrm{Aut}(A)/\mathrm{Inn}(A)$ is called the *outer automorphism group of A*.

(9) Let A and B be k-algebras.

(i) Show that $Z(A^{\mathrm{op}}) = Z(A)$.

(ii) Show that $Z(A \times B) = Z(A) \times Z(B)$.

(iii) Show that $Z(A \otimes_k B) = Z(A) \otimes_k Z(B)$. *Hint:* Show first that $Z(A \otimes_k B)$ is contained in $A \otimes_k Z(B)$.

(9) Let n be a positive integer. Let T_n be the set of all upper diagonal matrices in $M_n(k)$; that is, T consists of all matrices $(a_{ij})_{1\leq i,j\leq n}$ in $M_n(k)$ such that $a_{ij} = 0$ whenever $i > j$. Show that T is a subalgebra of $M_n(k)$. Let I be the set of all strict upper diagonal matrices in T; that is, I consists of all matrices $(a_{ij})_{1\leq i,j\leq n}$ in $M_n(k)$ such that $a_{ij} = 0$ whenever $i \geq j$. Show that I is an ideal in T satisfying $I^n = \{0\}$.

(10) Let n be a positive integer and let $(\mathcal{P}, \leq)$ be a finite partially ordered set with n elements. Consider $\mathcal{P}$ as a category, with exactly one morphism $i \to j$ for any i, $j \in \mathcal{P}$ such that $i \leq j$. Show that the set of $n \times n$-matrices, with rows and columns labelled by the elements of $\mathcal{P}$, given by

$$k\mathcal{P} = \{(m_{ij})_{i,j\in\mathcal{P}} \mid m_{ij} = 0 \text{ if } i \not\leq j\}$$

is a k-subalgebra of $M_n(k)$, and show that this algebra is canonically isomorphic to the category algebra of $\mathcal{P}$ over k, so there is no conflict of notation. This algebra is called the *incidence algebra of the partially ordered set $\mathcal{P}$*. Show that for some labelling $\mathcal{P} = \{i_1, i_2, .., i_n\}$, the incidence algebra $k\mathcal{P}$ is identified with a subalgebra of the algebra T_n of upper triangular matrices in $M_n(k)$.

2 Modules

Modules of an algebra A provide ways of identifying A with subalgebras of matrix algebras. We will see that every k-algebra A can be identified with a subalgebra of the linear endomorphism algebra $\mathrm{End}_k(A)$; this is an analogue for algebras of Cayley's theorem, which states that every group G can be identified with a subgroup of the symmetric group S_G of permutations of G.

Definition 2.1. Let A be a k-algebra. A *left A-module* is a k-vector space U together with a k-bilinear map

$$A \times U \to U, \quad (a,u) \mapsto au \ ,$$

satisfying $1_A u = u$ for all $u \in U$ and $(ab)u = a(bu)$ for all a, $b \in A$ and all $u \in U$. Analogously, a *right A-module* is a k-vector space V with a k-bilinear map

$$V \times A \to V, \quad (v,a) \mapsto va \ ,$$

satisfying $v1_A = v$ for all $v \in V$ and $v(ab) = (va)b$ for all a, $b \in A$ and all $v \in V$.

As before, the bilinear map $A \times U \to U$ in the above definition extends uniquely to a linear map $A \otimes_k U \to U$, $a \otimes u \mapsto au$, where $a \in A$, $u \in U$. The linearity in the second argument of the map $A \times U \to U$ means that $a(u+u') = au + au'$ and $a(\lambda u) = \lambda au$, where $a \in A$, u, $u' \in U$, and $\lambda \in k$. In other words, left multiplication by $a \in A$ on U induces a k-linear endomorphism $\varphi_a \in \mathrm{End}_k(U)$ satisfying $\varphi_a(u) = au$. The linearity in the first argument, the property $1_A u = u$ for all $u \in U$, and the associativity condition imply that the map sending $a \in A$ to $\varphi_a \in \mathrm{End}_k(U)$ is a unital k-algebra homomorphisms

$$A \longrightarrow \mathrm{End}_k(U) \ .$$

This is sometimes called the *structural homomorphism of U*, since is determines the A-module structure on U. Specifying a left A-module structure on a k-vector space U is in fact equivalent to specifying a k-algebra homomorphism $A \to \mathrm{End}_k(U)$. Any right A-module V can be considered as a left A^{op}-module via $a \cdot v = va$, where $a \in A$ and $v \in V$. Similarly, any left A-module can be considered as a right A^{op}-module. Therefore, specifying a right A-module structure on V is equivalent to specifying an algebra homomorphism

$$A^{\mathrm{op}} \longrightarrow \mathrm{End}_k(V) \ .$$

Definition 2.2. Let A and B be k-algebras. An *A-B-bimodule* is a k-vector space M which is both a left A-module and a right B-module, satisfying $(am)b = a(mb)$ for all $a \in A$, $b \in B$, $m \in M$.

Note that the left and right module structure of A and B on a bimodule M induce the same vector space structure, so that we can consider an A-B-bimodule as an $A \otimes_k B^{\mathrm{op}}$-module.

Examples 2.3.

(1) A k-algebra A is itself a left and right A-module, via multiplication in A. This is called the *regular* left or right A-module. In this way, A becomes an A-A-bimodule.

(2) If A is a k-algebra and I a left ideal, then I is a left A-module; similarly for right ideals. The ideals in A are exactly the subbimodules of the bimodule A. In particular, every element $x \in A$

gives rise to a left module $Ax = \{ax \mid a \in A\}$, to a right A-module $xA = \{xa \mid a \in A\}$ and to an A-A-bimodule AxA consisting of finite sums of elements of the form axa', where a, $a' \in A$.

(3) Let n be a positive integer. The space V of all column vectors with n entries in k is a left $M_n(k)$-module, and similarly, the space of n-dimensional row vectors is a right $M_n(k)$-module.

(4) Let V be a k-vector space. Then V has a natural $\mathrm{End}_k(V)$-module structure given by $\varphi \cdot v = \varphi(v)$ for all $\varphi \in \mathrm{End}_k(V)$ and $v \in V$. If V has finite dimension n, then the $\mathrm{End}_k(V)$-module V corresponds to the $M_n(k)$-module of n-dimensional column vectors through an algebra isomorphism $\mathrm{End}_k(V) \cong M_n(k)$ determined by a choice of a k-basis in V.

(5) Let G be a finite group and M a finite set on which G acts. The G-action on M extends linearly to an action of kG on the vector space kM having M as a basis. The resulting kG-module kM is called a *permutation kG-module*. If M is a transitive G-set, then kM is called a *transitive permutation kG-module*. If M is a transitive G-set and H the stabiliser in G of a fixed element $m \in M$, then the G-set M is isomorphic to the G-set of H-cosets $G/H = \{xH \mid x \in G\}$ via the isomorphism sending xH to xm.

A *submodule of an A-module U* is a k-subspace V of U such that the restriction to $A \times V$ of the map $A \times U \to U$ has image contained in V, or equivalently, satisfies $av \in V$ for all $a \in A$ and $v \in V$. Given a submodule V of U, the vector space quotient U/V becomes an A-module with the k-bilinear map $A \times U/V \to U/V$ sendig $(a, u + V)$ to $au + V$, where $a \in A$, $u \in U$. We have similar notions for right modules.

Example 2.4. Let G be a group. For any x, $y \in G$ we have $(xy)^{-1} = y^{-1}x^{-1}$. Thus the linear map on kG induced by sending $x \in G$ to x^{-1} is an antiautomorphism of kG, or equivalently, an isomorphism $kG \cong (kG)^{\mathrm{op}}$. This isomorphism is its own inverse since $(x^{-1})^{-1} = x$ for all $x \in G$.

We will later need vector spaces which have both a left and right module structure. In what follows we use the term module for left modules. We consider A-modules with their structure preserving maps.

Definition 2.5. Let A be a k-algebra, and let U, V be A-modules. An *A-homomorphism from U to V* is a k-linear map $\varphi : U \to V$ satisfying $\varphi(au) = a\varphi(u)$ for all $a \in A$, $u \in U$. We write $\mathrm{Hom}_A(U, V)$ for the set of all A-homomorphisms from U to V.

We have the obvious analogue of this definition for homomorphisms between right A-modules. Since right A-modules can be viewed as left A^{op}-modules, we will typically denote the space of A-homomorphisms between right A-modules U' and V' by $\mathrm{Hom}_{A^{\mathrm{op}}}(U', V')$. The A-modules form a category $\mathrm{Mod}(A)$, with A-homomorphisms as morphisms The morphism set $\mathrm{Hom}_A(U, V)$ is itself a k-vector space, and the composition of A-homomorphisms is k-bilinear. In particular, the set of *endomorphisms* $\mathrm{End}_A(U) = \mathrm{Hom}_A(U, U)$ of an A-module U is again a k-algebra, with multiplication given by the composition of endomorphisms of U and the identity map Id_U on U as unit element. The category of right A-modules can be identified with the category $\mathrm{Mod}(A^{\mathrm{op}})$ of left A^{op}-modules. The finite-dimensional A-modules form a category denoted $\mathrm{mod}(A)$; this is a full subcategory of $\mathrm{Mod}(A)$.

Example 2.6. Let A be a k-algebra and U an A-module. Then U is also an $\mathrm{End}_A(U)$-module, with module structure defined by $\varphi \cdot u = \varphi(u)$ for all $u \in U$ and $\varphi \in \mathrm{End}_A(U)$.

There is a notion of direct sum of two A-modules which we will review in a moment, and hence $\mathrm{Mod}(A)$ is a k-linear category. In fact, the category $\mathrm{Mod}(A)$ is a k-linear abelian category; that is, we have an isomorphism theorem of the following form:

Theorem 2.7. *Let A be a k-algebra, let U, V be A-modules, and let $\varphi : U \to V$ be an A-homomorphism. Then $\ker(\varphi) = \{u \in U \mid \varphi(u) = 0\}$ is a submodule of U, $\mathrm{Im}(\varphi) = \{\varphi(u) \mid u \in U\}$ is a submodule of V, and the map φ induces an isomorphis*

$$U/\ker(\varphi) \cong \mathrm{Im}(\varphi)$$

sending the class $u + \ker(\varphi)$ to φ, for all $u \in U$.

Proof. Trivial verification. □

The submodule $\ker(\varphi)$ of U is called the *kernel of* φ, and the submodule $\mathrm{Im}(\varphi)$ of V is called the *image of* φ.

Theorem 2.8. *Let A be a k-algebra, let U be an A-module and W a submodule of U. Any submodule of U/W is equal to V/W for some submodule V of U containing W, and there is a canonical isomorphism of A-modules $(U/W)/(V/W) \cong U/V$.*

Proof. Let M be a submodule of U/W. One verifies that then $V = \{v \in U \mid v + W \in M\}$ is a submodule of U containing W and satisfying $M = V/W$. Since V contains W, there is a unique surjective A-homomorphism $U/W \to U/V$ sending $a + W$ to $a + V$. The kernel of this homomorphism is V/W, and hence the isomorphism $(U/W)/(V/W) \cong U/V$ is a special case of 2.7. □

Let A be a k-algebra. A submodule V of an A-module U is called a *proper submodule of* U if it is different from U, and it is called a *maximal submodule of* U, if it is maximal with respect to the inclusion amongst all proper submodules, or equivalently, if there is no proper submodule of U containing V as a proper submodule.

Definition 2.9. Let A be a k-algebra. Given two A-modules V, W, the *direct sum of* V and W is the A-module

$$V \oplus W = \{(v, w) \mid v \in V,\ w \in W\}$$

with componentwise sum, scalar multiplication, and action of $a \in A$ on (v, w) given by $a(v, w) = (av, aw)$.

As a set, the direct sum $U \oplus V$ coincides with the Cartesian product $U \times V$. We have canonical injective A-homomorphisms $\iota_V : V \to V \oplus W$ sending $v \in V$ to $(v, 0)$ and $\iota_W : W \to V \oplus W$ sending $w \in W$ to $(0, w)$. Through these injective maps, we can identify V and W canonically to the submodules $V \times \{0\}$ and $\{0\} \times W$ of $V \oplus W$. The module $V \oplus W$ is then equal to the sum of these two submodules, and the intersection of these two submodules is zero. Conversely, if U is an A-module and if V, W U are submodules of U such that $V + W = U$ and such that $V \cap W = \{0\}$, then $V \oplus W \cong U$ via the obvious map sending $(v, w) \in V \oplus W$ to $v + w \in U$. In that situation, every element $u \in U$ can be written uniquely in the form $u = v + w$ for some $v \in V$ and $w \in W$, and we identify $U = V \oplus W$. The point of the next result is that it characterises the direct sum of two modules in terms of a universal property. This universal property is used to extend the notion of direct sums to arbitrary categories.

Proposition 2.10. *Let A be a k-algebra, and let V, W be A-module. Denote by $\iota_V : V \to V \oplus W$ and $\iota_W : W \to V \oplus W$ the canonical injections. The triple $(V \oplus W, \iota_V, \iota_W)$ satisfies the following universal property: for any other triple (X, φ, ψ) consisting of an A-module X and A-homomorphisms $\varphi : V \to X$ and $\psi : W \to X$, there is a unique A-homomorphism $\alpha : V \oplus W \to X$ satisfying $\alpha \circ \iota_V = \varphi$ and $\alpha \circ \iota_W = \psi$.*

Proof. Define α by $\alpha(v, w) = \varphi(v) + \psi(w)$, where $v \in V$ and $w \in W$. One checks that this is an A-homomorphism. Moreover, we have $\alpha(\iota_V(v)) = \alpha(v, 0) = \varphi(v) + \psi(0) = \varphi(v)$, hence $\alpha \circ \iota_V = \varphi$. Similarly we have $\alpha \circ \iota_W = \psi$. This shows the existence of α. For the uniqueness, suppose that $\beta : V \oplus V \to X$ satisfies $\beta \circ \iota_V = \varphi$ and $\beta \circ \iota_W = \psi$. Thus $\varphi(v) = \beta(\iota_V(v)) = \beta(v, 0)$. Similarly, $\psi(w) = \beta(0, w)$. Thus $\beta(v, w) = \beta((v, 0) + (0, w)) = \beta(v, 0) + \beta(0, w) = \varphi(v) + \psi(w) = \alpha(v, w)$. This shows the uniqueness of α. $\square$

The universal property describing direct sums is 'opposite' to that describing direct products in the sense that one is obtained from the other by reversing the direction of morphisms. It happens so that the direct sum of two modules is also the direct product of two modules (this is a general fact in additive categories). The direct product of two algebras is, however, not a direct sum in the category of k-algebras. One can show that the direct sum in the category of commutative k-algebras is the tensor product of the two algebras over k, but these considerations will not be needed.

Definition 2.11. Let A be a k-algebra and let U be an A-module. We say that U is a *simple A-module* if U is nonzero and if U has no nonzero proper submodule, or equivalently, if $\{0\}$ is a maximal submodule of U. We say that U is an *indecomposable* if U is nonzero and if U cannot be written as a direct sum of two proper nonzero submodules.

Remark 2.12. Any simple module is indecomposable, but in general, indecomposable modules need not be simple. A simple A-module S is isomorphic to a quotient of A. Indeed, if s is a nonzero element in S, then the map $A \to S$ sending $a \in A$ to as is an A-homomorphism which is nonzero, and hence surjective as S is simple. In particular, every simple module of a finite-dimensional k-algebra has finite dimension. Every one-dimensional A-module is simple, because it does not even have a proper nonzero k-subspace.

Example 2.13. Let V be a finite-dimensional k-vector space. Then V is a simple $\mathrm{End}_k(V)$-module. Indeed, if W is a nonzero proper k-subspace of V, then for any nonzero $w \in W$ and any nonzero $v \in V \setminus W$ there is a linear transformation τ of V such that $\tau(w) = v$. Then $\tau \in \mathrm{End}_k(V)$, and $\tau(W)$ is not contained in V. Thus W is not an $\mathrm{End}_k(V)$-module, and hence V is simple. Equivalently, the space k^n of n-dimensional column vectors is a simple $M_n(k)$-module.

Proposition 2.14. *Let A be a k-algebra and let U be an A-module. A submodule V of U is maximal if and only if U/V is simple.*

Proof. Suppose that U/V is simple. Let W be a proper submodule of U such that $V \subseteq W$. Then W/V is a proper submodule of U/V, hence zero as U/V is simple, and hence $W = V$. This shows that V is a maximal submodule of U. Conversely, suppose that V is a maximal submodule of U. Let M be a nonzero submodule of U/V. Then $M = W/V$ for some submodule W of U contaning V. Since M is nonzero, the module W must contain V properly. Thus $W = U$, as V is maximal, and hence $M = U/V$. This shows that U/V is simple. $\square$

Every finite-dimensional A-module U has a maximal submodule V; indeed, take for V a proper submodule of maximal possible dimension. Infinite-dimensional modules need not have any maximal submodules, or equivalently, may not have any simple quotients. Using Zorn's Lemma one can show that if U is a finitely generated module over an arbitrary algebra and V a proper submodule of U, then there exists a maximal submodule M of U which contains V.

Definition 2.15. Let A be a k-algebra. A *composition series of an A-module M* is a finite chain $M = M_0 \supset M_1 \supset \cdots \supset M_n = \{0\}$ of submodules M_i in M such that M_{i+1} is maximal in M_i for $0 \leq i \leq n-1$. The simple factors M_i/M_{i+1} arising this way are called the *composition factors* of this series and the nonnegative integer n is called its length . Two composition series of A-modules M and M', respectively, are called *equivalent* if they have the same length n and if there is a bijection between the sets of composition factors of each of these series such that corresponding composition factors are isomorphic.

Lemma 2.16. *Let A be a k-algebra, let M be an A-module, let U and N be submodules of M, and let V be a maximal submodule of U. We have $U + N = V + N$ if and only if $V \cap N \subsetneq U \cap N$. If this is the case then $U/V \cong (U \cap N)/(V \cap N)$. Otherwise, $U/V \cong (U + N)/(V + N)$.*

Proof. We have $V \subseteq (U \cap N) + V \subseteq U$. Since V is maximal in U either $V = (U \cap N) + V$ or $(U \cap N) + V = U$. In the first case, $U \cap N = V \cap N$ and $(U+N)/(V+N) \cong U/(U \cap (V+N)) = U/V$. In the second case, $V + N = U + N$ and $U/V = ((U \cap N) + V)/V \cong (U \cap N)/(V \cap N)$. □

Theorem 2.17 (Jordan-Hölder)**.** *Let A be a k-algebra, and let M be a finite-dimensional A-module. Then M has a composition series, and any two composition series of M are equivalent.*

Proof. We construct a composition series inductively by $M_0 = M$ and M_{i+1} maximal in M_i if M_i is nonzero. In particular, $\dim_k(M_{i+1}) < \dim_k(M_i)$. Since $\dim_k(M)$ is finite, we have $M_i = \{0\}$ for i large enough. This shows that M has a composition series. Let $M = M_0 \supset M_1 \supset \cdots \supset M_n = \{0\}$ and $M = N_0 \supset N_1 \supset \cdots \supset N_k = \{0\}$ be two composition series of M. If $n \leq 1$, then either M is zero or simple, so we are done. Suppose that $n > 1$. Set $N = N_1$; note that the N_j, with $1 \leq j \leq k$ form a composition series of N of length $k - 1$. Consider the chain

$$M = M_0 + N \supset M_1 + N \supset .. \supset M_n + N = N = M_0 \cap N \supset M_1 \cap N \supset .. \supset M_n \cap N = \{0\}.$$

Since N is maximal in M there is exactly one index i, $0 \leq i \leq n-1$, such that

$$M = M_0 + N = .. = M_i + N \supset M_{i+1} + N = .. = M_n + N = N$$

and by 2.16 this is also the unique index i for which $M_i \cap N = M_{i+1} \cap N$. It follows that we have a composition series

$$M = M_i + N \supset M_{i+1} + N = N = M_0 \cap N \supset \cdots \supset M_i \cap N = M_{i+1} \cap N \supset \cdots \supset M_n \cap N = \{0\}.$$

Deleting the first term in this series yields a series of N of length $n - 1$. Thus, by induction, this series of N is equivalent to the series of the N_j, $1 \leq j \leq k$ which is of length $k-1$. This means that we have $k = n$ and up to a permutation, the composition factors $(M_j \cap N)/(M_{j+1} \cap N) \cong M_j/M_{j+1}$ for $0 \leq j \leq n-1$ and $j \neq i$ are isomorphic to the factors N_j/N_{j+1} for $1 \leq j \leq n-1$. The remaining factor M_i/M_{i+1} is, by 2.16, isomorphic to $(M_i + N)/(M_{i+1} + N) \cong M/N_1$, which completes the proof. □

One can show more generally for a module M over an arbitrary algebra, that M has a composition series if and only if M is Noetherian and Artinian.

Definition 2.18. Let A be a k-algebra. An A-module U is called *uniserial* if U has a unique composition series.

Being uniserial is a strong restriction on the structure of a nonzero A-module U. It means that U has a unique maximal submodule U_1 which in turn is either zero or has a unique maximal submodule U_2, and so on. A uniserial module is automatically indecomposable: a direct sum $U \oplus V$ of two nonzero modules U, V has at least two maximal submodules, namely one of the form $U' \oplus V$ for some maximal submodule U' of U, and another of the form $U \oplus V'$ for some maximal submodule V' of V. We will later characterise uniserial modules in more detail.

Exercises 2.19.

(1) Let A be a k-algebra and let U be an indecomposable A-module with a composition series of length 2. Show that U is uniserial.

(2) Let A be a k-algebra, and let U, V be finite-dimensional A-modules. Suppose that no composition factor of U is isomorphic to a composition factor of V. Then every submodule of $U \oplus V$ is equal to $U' \oplus V'$ for some submodule U' of U and some submodule V' of V.

(3) Let A be a finite-dimensional k-algebra and S a simple A-module. Suppose that the field k is infinite. Show that $S \oplus S$ has infinitely many submodules, and that any proper nonzero submodule of $S \oplus S$ is isomophic to S.

(4) Let A be a k-algebra and U a finite-dimensional nonzero A-module. Show that if U has a unique maximal submodule, then U is indecomposable.

3 Idempotents and blocks

Definition 3.1. Let A be a k-algebra. An element $i \in A$ is called an *idempotent* if $i \neq 0$ and $i^2 = i$. Two idempotents i, $j \in A$ are called *orthogonal* if $ij = 0 = ji$. An idempotent $i \in A$ is called *primitive* if i cannot be written as a sum of two orthogonal idempotents. A *primitive decomposition of an idempotent e in A* is a finite set I of pairwise orthogonal primitive idempotents in A such that $e = \sum_{i \in I} i$.

The unit element 1 in a k-algebra A is an idempotent, but we adopt the convention that we do not consider 0 as an idempotent. If i is an idempotent in A such that $i \neq 1$, then $1 - i$ is an idempotent which is orthogonal to i. Indeed, since $i \neq 1$ we have $1 - i \neq 0$, and $(1 - i)^2 = 1^2 - 2i + i^2 = 1 - 2i + i = 1 - i$, so $1 - i$ is an idempotent. We have $(1 - i)i = i - i^2 = i - i = 0$, and similarly, $(1 - i) = 0$, so i and $1 - i$ are orthogonal. If i and j are orthogonal idempotents, then $i + j$ is an idempotent. Indeed, we have $(i + j)i = i^2 + ij = i^2 = i$, and similarly, $(i + j)j = j$. This shows that $i + j$ is nonzero, and that $(i + j)^2 = (i + j)i + (i + j)j = i + j$, hence $i + j$ is an idempotent. If i and j are two idempotents which commute, then either $ij = 0$ or ij is an idempotent. Indeed, we have $(ij)^2 = ijij = iijj = ij$. If i is an idempotent in A, then the vector space iAi is closed under multiplication in A, and hence iAi is a k-algebra with unit element i (so this is not a unital subalgebra of A). An arbitrary idempotent in an algebra may not necessarily have a primitive decomposition, but a straightforward dimension counting argument below shows that every idempotent in a finite-dimensional algebra has a primitive decomposition.

Proposition 3.2. *Let A be a k-algebra, and let i be an idempotent in A. The following are equivalent.*

(i) The idempotent i is primitive in A.

(ii) The idempotent i is primitive in the algebra iAi.

(iii) The idempotent i is the unique idempotent in the algebra iAi.

Proof. If i is not the unique idempotent in iAi, then there exists an idempotent $j \in iAi$ different from i. Then $i - j$ is an idempotent in iAi which is orthogonal to j and satisfies $i = j + (i - j)$. This shows that i is not primitive in A, whence the implication (i)$\Rightarrow$ (iii). The implication (iii) $\Rightarrow$ (ii) is trivial. Suppose that i is not primitive. Then $i = j + j'$ for some orthogonal idempotents j, j'. Thus $ij = j^2 + j'j = j$. A similar argument shows that $ji = j$. Thus $j \in iAi$, and hence i is not primitive in iAi. This shows the implication (ii) $\Rightarrow$ (i), whence the result. $\square$

Example 3.3. The field k has a unique idempotent, namely its unit element. Let n be a positive integer. For $1 \le i \le n$ denote by E_i the matrix in $M_n(k)$ such that the diagonal entry at (i, i) is 1 and such that all other entries are zero. Then $E_i^2 = E_i \neq 0$; that is, E_i is an idempotent. For $1 \le i, j \le n$ such that $i \neq j$ we have $E_iE_j = 0$. Thus the E_i are pairwise orthogonal idempotents. We have $E_iM_nE_i \cong k$, because $E_iM_n(k)M_i$ consists of all matrices which are zero in all entries except possibly in the diagonal entry (i, i). Thus E_i is a primitive idempotent in $M_n(k)$. We have $\sum_{i=1}^{n} E_i = \mathrm{Id}_n$, the identity matrix in $M_n(k)$, and hence $\{E_i \mid 1 \le i \le n\}$ is a primitive decomposition of Id_n.

The following example illustrates that idempotents are closely related to direct sum decompositions of modules.

Example 3.4. Let A be a k-algebra and let U be a nonzero A-module. Let ι be an idempotent in $\mathrm{End}_A(U)$. Then $\iota(U)$ is a direct summand of U; more precisely, we have

$$U = \iota(U) \oplus (\mathrm{Id} - \iota)(U) \ ,$$

where Id is the identity endomorphism of U. Indeed, since $\mathrm{Id} = \iota + (\mathrm{Id} - \iota)$, we have $u = \iota(u) + (\mathrm{Id} - \iota)(u)$ for all $u \in U$. Thus $U = \iota(U) + (\mathrm{Id} - \iota)(U)$. To see that this sum is direct, we need to show that the intersection of these two submodules is zero. Let $u \in \iota(U) \cap (\mathrm{Id} - \iota)(U)$. That is, there are v, $w \in U$ such that $u = \iota(v) = (\mathrm{Id} - \iota)(w)$. We have $u = \iota(\iota(v))$ because ι is an idempotent. Thus $u = \iota((\mathrm{Id} - \iota)(w)) = \iota(w) - \iota(\iota(w)) = 0$, again because ι is an idempotent. Thus $\iota(U) \cap (\mathrm{Id} - \iota)(U) = \{0\}$. Conversely, if $U = V \oplus W$ for two nonzero submodules V, W of U, then any element $u \in U$ can be written uniquely in the form $u = v + w$ for some $v \in V$ and some $w \in W$, and the canonical projections of U onto V and W sending $u = v + w$ to v and w, respectively, are orthogonal idempotents in $\mathrm{End}_A(U)$. As a consequence of these considerations, we get that a nonzero A-module U is indecomposable if and only if Id_U is a primitive idempotent in $\mathrm{End}_A(U)$.

Lemma 3.5. *Let A be a k-algebra and let U be an A-module. Let i, j be orthogonal idempotents in A, and set $e = i + j$. Then $eU = iU \oplus jU$ as k-vector spaces.*

Proof. Let $u \in eU$. Then $u = eu = (i + j)u = iu + ju$, hence $eU = iU + jU$. Let $v \in iU \cap jU$. Since $i^2 = i$ we have $v = iv$; similarly, we have $v = jv$. Thus $v = iv = ijv = 0$, hence $iU \cap jU = \{0\}$. $\square$

We have an analogous statement for right modules.

Lemma 3.6. *Let A be a finite-dimensional k-algebra. Every idempotent e in A has a primitive decomposition.*

Proof. We argue by induction over $\dim_k(eA)$. If e is primitive, then $I = \{e\}$ is a primitive decomposition of e, so we may assume that e is not primitive. Then $e = i + j$ for two orthogonal idempotents i, j. Thus $eA = iA \oplus jA$ by 3.5. Both iA, jA are nonzero, hence have smaller dimension than that of eA. It follows by induction that both i and j have primitive decompositions. The union of these is a primitive decomposition of e. □

Lemma 3.7. *Let A be a k-algebra and e an idempotent in A. Let U, V be nonzero submodules of Ae as a left A-module such that $Ae = U \oplus V$. Then there are unique orthogonal idempotents i and j in eAe such that $U = Ai$ and $V = Aj$. Moreover, i and j satisfy $i + j = e$. In particular, Ae is indecomposable if and only if e is primitive in A.*

Proof. Since $Ae = U \oplus V$, there are unique elements $i \in U$ and $j \in V$ such that $e = i + j$. Since e is an idempotent and $i, j \in Ae$, we have $i = ie$ and $j = je$. We also have $e = e^2 = ei + ej$, and $ei \in U$, $ej \in V$. The uniqueness of i, j implies that $ei = i$ and $ej = j$. Thus i and j are idempotents in eAe satisfying $i + j = e$. It follows that $i = i(i + j) = i^2 + ij$ As $i^2 \in U$ and $ij \in V$ this forces $ij = 0$ and $i^2 = i$. A similar argument yields $j^2 = j$ and $ji = 0$. Thus i and j are orthogonal idempotents in eAe satisfying $e = i + j$, and hence $Ae = Ai \oplus Aj$ by 3.5 for right modules. Since $Ai \subseteq U$ and $Aj \subseteq V$ and $Ae = U \oplus V$, comparing dimensions yields $U = Ai$ and $V = Aj$. Note that this implies $Uj = \{0\} = Vi$, because i and j are orthogonal. We need to show that i, j are unique. Suppose i' and j' are orthogonal idempotents such that $Ai = Ai'$ and $Aj = Aj'$. The elements in Ai are invariant under right multiplication with i because i is an idempotent, and they are annihilated by right multiplication with j, because i and j are orthogonal. Since $i' \in Ai$, this implies that $i' = i'i$ and $i'j = 0$. Similarly, $ii' = i$ and $ji' = 0$. Thus $i' = ei' = (i+j)i' = ii' + ji' = i$, and similarly $j' = j$. This completes the proof. □

This does not mean that for a nonzero direct summand U of Ae as a left A-module there is a unique idempotent i satisfying $U = Ai$. The uniqueness of i requires the choice of a complement V satisfying $U \oplus V = Ae$ as left A-modules. For fixed U there can in general be infinitely many complements in Ae.

Proposition 3.8. *Let A be a k-algebra and U a nonzero finite-dimensional A-module. Then the k-algebra $\mathrm{End}_A(U)$ is finite-dimensional, and if I is a primitive decomposition of Id_U in $\mathrm{End}_A(U)$, then $U = \oplus_{\iota \in I}\ \iota(U)$ is a direct sum decomposition of U as a direct sum of indecomposable A-modules. This correspondence induces a bijection between primitive decompositions of Id_U in $\mathrm{End}_A(U)$ and decompositions of U as direct sum of indecomposable A-modules.*

Proof. Extend the considerations in 3.4 to finitely many summands. □

Lemma 3.9. *Let A be a k-algebra, i an idempotent in A and U an A-module. There is a k-linear isomorphism*

$$\mathrm{Hom}_A(Ai, U) \cong iU$$

sending $\varphi \in \mathrm{Hom}_A(Ai, U)$ to $\varphi(i)$. The inverse of this isomorphism sends iu to the map $Ai \to U$ sending ai to aiu, for all $a \in A$ and $u \in U$.

Proof. Let $\varphi \in \mathrm{Hom}_A(Ai, U)$. Since $i^2 = i$, we have $\varphi(i) = \varphi(i^2) = i\varphi(i) \in iU$. Thus $\varphi \mapsto \varphi(i)$ is a k-linear map from $\mathrm{Hom}_A(Ai, U)$ to iU. This map is injective: if $\varphi(i) = 0$, then $\varphi(ai) = a\varphi(i) = 0$ for all $a \in A$, hence $\varphi = 0$. The map is surjective: if $u \in U$, then the map ψ defined by $\psi(ai) = aiu$ is an A-homomorphism satisfying $\psi(i) = iu$. The result follows. □

Theorem 3.10. *Let A be a k-algebra, and let i, j be indempotents in A. There is a k-linear isomorphism*

$$\mathrm{Hom}_A(Ai, Aj) \cong iAj$$

sending $\varphi \in \mathrm{Hom}_A(Ai, Aj)$ to $\varphi(i)$. The inverse of this isomorphism sends $c \in jAi$ to the unique homomorphisms $Ai \to Aj$ sending $a \in Ai$ to $ac \in Aj$. Moreover, if $i = j$, this isomorphism is a k-algebra isomorphism

$$\mathrm{End}_A(Ai) \cong (iAi)^{\mathrm{op}} .$$

Proof. The k-linear isomorphism $\mathrm{Hom}_A(Ai, Aj) \cong iAj$ is the special case of the previous lemma appliesd with $U = Aj$. Suppose now that $i = j$. Let φ, $\psi \in \mathrm{End}_A(Ai)$. Then for any $a \in A$ we have $(\psi \circ \varphi)(ai) = \psi(\varphi(ai)) = \psi(a\varphi(i)) = a\psi(\varphi(i)) = a\psi(\varphi(i)i) = a\varphi(i)\psi(i)$. Thus $\psi \circ \varphi$ is the endomorphism given by right multiplication with $\varphi(i)\psi(i)$, which shows that the k-linear isomorphism $\mathrm{End}_A(Ai) \cong iAi$ from above is an antiisomorphism, or equivalently, is an isomorphism $\mathrm{End}_A(Ai) \cong (iAi)^{\mathrm{op}}$. □

Corollary 3.11. *Let A be a k-algebra. The map sending $c \in A$ to the A-endomorphism $a \mapsto ac$ of A is a k-algebra isomorphism $A^{\mathrm{op}} \cong \mathrm{End}_A(A)$.*

Proof. This is the case $i = j = 1$ in the theorem. □

We have right module versions for the above theorem and its corollary: with the notation above, we have a k-linear isomorphism $\mathrm{Hom}_{A^{\mathrm{op}}}(iA, jA) \cong jAi$ mapping φ to $\varphi(i)$; for $i = j$ this is a k-algebra isomorphism $\mathrm{End}_{A^{\mathrm{op}}}(iA) \cong iAi$, and for $i = j = 1$ this yields an algebra isomorphism $A \cong \mathrm{End}_{A^{\mathrm{op}}}(A)$ sending $c \in A$ to the endomorphism $a \mapsto ca$ for all $a \in A$.

Corollary 3.12. *Let A be a k-algebra. We have an isomorphism of k-algebras $Z(A) \cong \mathrm{End}_{A\otimes_k A^{\mathrm{op}}}(A)$ sending $z \in Z(A)$ to the map given by left or right multiplication with z on A.*

Proof. The algebra $\mathrm{End}_{A\otimes_k A^{\mathrm{op}}}(A)$ is a subalgebra of $\mathrm{End}_A(A)$. Thus for any $\varphi \in \mathrm{End}_{A\otimes_k A^{\mathrm{op}}}(A)$ there is $c \in A$ such that $\varphi(a) = ac$ for all $a \in A$. But φ is also a homomorphism of right A-mdoules, hence $\varphi(a) = \varphi(1)a$ for all $a \in A$, which is equivalent to $ac = ca$ for all $a \in A$, hence equivalent to $c \in Z(A)$. The result follows. □

Idempotents in the centre $Z(A)$ of a k-algebra A are closely related to direct factors of A. Let b be an idempotent in $Z(A)$. Then $Ab = bAb$ is a k-algebra with b as unit element. If $b \neq 1$, then $1 - b$ is an idempotent in $Z(A)$, and the idempotents b and $1 - b$ are orthogonal. We have an algebra isomorphism

$$A \cong Ab \times A(1 - b)$$

sending a to $(ab, a(1 - b))$. Indeed, this map is an algebra homomorphism since b and $1 - b$ are central idempotents. It is injective since if $ab = a(1 - b) = 0$, then $a = ab + a(1 - b) = 0$. It is surjective: if c, $d \in A$, then $(cb, d(1 - b))$ is the image of $cb + d(1 - b)$ because b and $1 - b$ are orthogonal. This shows that any central idempotent in $Z(A)$ different from 1 gives rise to a decomposition of A as a direct product of two algebras. We abusively identify $A = Ab \times A(1-b)$ through this isomorphisms. Conversely, if A is a direct product of two algebras, say

$$A = B \times C \ ,$$

then $(1_B, 0)$ and $(0, 1_C)$ are two central orthogonal idempotents in A, and their sum is $1_A = (1_B, 1_C)$. Thus a k-algebra A is indecomposable if and only if 1_A is a primitive idempotent in $Z(A)$. In particular, if $A = B \times C$, then B is indecomposable if and only if 1_B is a primitive idempotent in $Z(A)$.

Definition 3.13. Let A be a k-algebra. A *block idempotent of A* is a primitive idempotent b in $Z(A)$. A block algebra of A is an indecomposable direct factor B of A.

If b is a block of A, then Ab is the corresponding block algebra, and by the preceding remarks, any block algebra of A is equal to Ab for a uniquely determined primitive idempotent in $Z(A)$. The map sending $a \in A$ to Ab is a surjective k-algebra homomorphism $A \to Ab$, but Ab is not a unitary subalgebra of A (unless of course $b = 1_A$). Thus primitive decompositions of 1_A in $Z(A)$ and decompositions of A as a direct product of block algebras correspond bijectively to each other. It follows from 3.12 and 3.8 that primitive decompositions of 1_A in $Z(A)$ correspond also bijectively to direct sum decompositions of A as a direct sum of indecomposable A-A-bimodules. If A is a finite-dimensional k-algebra, then there is a unique block decomposition of A, or equivalently, 1_A has a unique primitive decomposition in $Z(A)$.

Theorem 3.14. *Let A be a finite-dimensional k-algebra.*

(i) Any two primitive idempotents in $Z(A)$ are either equal or orthogonal.

(ii) There is a unique primitive decomposition $\mathcal{B}$ of 1_A in $Z(A)$. In particular, $Z(A)$ has only finitely many idempotents.

(iii) There is a unique decomposition of A as a direct product of its block algebras, up to the order of the factors; more precisely, this decomposition is equal to the product

$$A = \prod_{b \in \mathcal{B}} Ab \ .$$

(iii) There is a unique decomposition of A as a direct sum of A-A-bimodules, up to the order of the factors; more precisely, this decomposition is equal to the direct sum

$$A = \oplus_{b \in \mathcal{B}} Ab \ .$$

Proof. Let b, b' be two primitive idempotents in $Z(A)$. Since b and b' commute, we have either $bb' = 0$ or bb' is an idempotent in $Z(A)$. If $bb' = 0$, then b, b' are orthogonal, so there is nothing to prove. Supose that $b' \neq 0$. Similarly, either $b(1-b') = 0$ or $b(1-b')$ is an idempotent in $Z(A)$. We have $b = bb' + b(1-b')$. The summands are orthogonal and they are either zero or idempotents in $Z(A)$. Since b is primitive and $bb' \neq 0$, it follows that $b(1-b') = 0$. Then $b = bb'$. But we also have $b' = bb' + b'(1-b)$, which forces $b' = bb'$, hence $b' = b$. This shows (i). Since $Z(A)$ is finite-dimensional, the unit element 1_A has a primitive decomposition $\mathcal{B}$ in $Z(A)$, by 3.6. In order to show that $\mathcal{B}$ is unique, we show that every primitive idempotent $b \in Z(A)$ is contained in $\mathcal{B}$. Let b be a primitive idempotent in $Z(A)$. We have $1_A = \sum_{b' \in \mathcal{B}} b'$, and this is a sum of pairwise orthogonal primitive idempotents in $Z(A)$. Multiplying this sum by b yields $b = \sum_{b' \in \mathcal{B}} bb'$. The summands are pairwise orthogonal, and the nonzero summands are idempotents. Since b is primitive, it follows that there is exactly one $b' \in \mathcal{B}$ such that $bb' \neq 0$. But then $b = b'$ by (i). The equivalence between (ii) and (iii), (iv) follows from the remarks and results above. $\square$

If A is a k-algebra, U an A-module and b an idempotent in $Z(A)$, then the vector space decomposition

$$U = bU \oplus (1-b)U$$

from 3.5 is a direct sum of A-modules, because b and $1-b$ are both central. Note that b acts as identity on the summand bU but annihilates $(1-b)U$. In particular, bU can be viewed as an Ab-module. Although b is primitive in $Z(A)$, the A-module bU need not be indecomposable. Similarly, $(1-b)U$ can be viewed as an $A(1-b)$-module. Thus the block decomposition of a finite-dimensional k-algebra induces a direct sum decomposition of any A-module in such a way that the summands correspond to modules for the block algebras of A.

Example 3.15. Let n be a positive integer. We have $Z(M_n(k)) = k\mathrm{Id}_n$, where Id_n is the identity matrix in $M_n(k)$. Thus Id_n is primitive in $Z(M_n(k))$, or equivalently, Id_n is the unique block idempotent in $M_n(k)$. If $n > 1$, then Id_n is, however, not primitive in $M_n(k)$; see Example 3.3 above.

A more structural viewpoint of the above remarks is as follows. Let

$$\lambda : A \to \mathrm{End}_k(U)$$

be the structural homomorphism, sending any $a \in A$ to the linear endomorphism $\lambda_a \in \mathrm{End}_k(U)$ given by $\lambda_a(u) = au$ for all $u \in U$. If a belongs to $Z(A)$, then λ_a is an A-endomorphism; indeed, if $a \in Z(A)$, then for all $c \in A$ we have $c\lambda_a(u) = cau = acu = \lambda_a(cu)$, where $u \in U$. Thus λ induces an algebra homomorphism, abusively still denoted by the same letter,

$$\lambda : Z(A) \to \mathrm{End}_A(U) \ .$$

If b is an idempotent in $Z(A)$, then λ_b is an idempotent in $\mathrm{End}_A(U)$, and hence $\lambda_b(U) = bU$ is a direct summand of U. Even if b is primitive in $Z(A)$, its image λ_b in $\mathrm{End}_A(U)$ need not be primitive, which explains the fact mentioned above that bU need not be indecomposable.

Proposition 3.16. *Let A be a finite-dimensional k-algebra, let $\mathcal{B}$ be the set of block idempotents of A, and let U be an A-mdoule. We have a direct sum decomposition of U as an A-module of the form*

$$U = \oplus_{b \in \mathcal{B}} \, bU \ .$$

In particular, if U is an indecomposable A-module, then there is a unique $b \in \mathcal{B}$ such that $bU = U$ and such that $b'U = \{0\}$ for all $b' \in \mathcal{B} \setminus \{b\}$.

Proof. Since $\mathcal{B}$ is a primitive decomposition of 1_A in $Z(A)$, it follows from 3.5 that $U = \oplus_{b \in \mathcal{B}} bU$ as vector spaces. Since the $b \in \mathcal{B}$ are central, this is a direct sum decomposition of A-modules. If U is indecomposable, then exactly one of those summands is nonzero, whence the result. $\square$

Definition 3.17. Let A be a k-algebra and b a block idempotent in $Z(A)$. An A-module U is said to *belong to the block* b or *to the block algebra* Ab if $bU = U$.

If U and V are two A-modules which belong to the same block b of A, then U and V can be viewed as A-mdoules or as Ab-modules, and we have

$$\mathrm{Hom}_A(U, V) = \mathrm{Hom}_{Ab}(U, V) \ .$$

This means that $\mathrm{Mod}(Ab)$ is a full subcategory of $\mathrm{Mod}(A)$, and it also means that the map sending an A-module U to the Ab-module bU yields a functor $\mathrm{Mod}(A) \to \mathrm{Mod}(Ab)$ which restricts to the identity functor on $\mathrm{Mod}(Ab)$. If U and V belong to two different blocks b and c, respectively, of a k-algebra A, then $\mathrm{Hom}_A(U, V) = \{0\}$. Indeed, for any $\varphi \in \mathrm{Hom}_A(U, V)$ and any $u \in U$ we have $u = bu$, hence $\varphi(u) = \varphi(bu) = b\varphi(u)$. But since $\varphi(u) \in V$ we also have $\varphi(u) = c\varphi(u)$. Together we get that $\varphi(u) = bc\varphi(u) = 0$. This shows that $\mathrm{Mod}(A)$ is the direct sum of the full subcategories $\mathrm{Mod}(Ab)$ of the block algebras of A, modulo giving a precise definition of the direct sum of two module categories. The point of these trivial formal considerations is this: in order to understand the module category of a finite-dimensional algebras, we may decompose the algebra first into into its blocks, and then describe the module categories of the block algebras.

Exercises 3.18.

(1) Let A be a k-algebra and i an idempotent in A different from 1_A. Show that i is not invertible in A.

(2) Let A be a k-algebra, and let i, j be idempotents in A. Suppose that i and j are conjugate by an element in $A^\times$; that is, $j = cic^{-1}$ for some $c \in A^\times$. Show that $Ai \cong Aj$ as A-modules and that $iAi \cong jAj$ as k-algebras.

(3) Let A be a k-algebra, i an idempotent in A and I an ideal in A which does not contain i. Set $j = i + I$. Show that j is an idempotent in A/I, that $I \cap iAi$ is an ideal in iAi, and that we have a k-algebra isomorphism $jA/Ij \cong iAi/I \cap iAi$.

(4) Let A be a finite-dimensional k-algebra, i a primitive idempotent in A and b a block idempotent of A. Show that the A-module Ai belongs to the block b if and only if $bi \neq 0$.

(5) Let $\mathcal{P}$ be a finite partially ordered set. Show that the blocks of the incidence algebra $k\mathcal{P}$ correspond bijectively to the connected components of $\mathcal{P}$.

4 Semisimple modules and the Jacobson radical

Definition 4.1. Let A be a k-algebra. An A-module U is called *semisimple* if U is the sum of its simple submodules.

The following theorem characterising finite-dimensional semisimple modules remains true for arbitrary modules (the proof in this generality would require Zorn's Lemma).

Theorem 4.2. *Let A be a k-algebra and let U be a finite-dimensional A-module. The following are equivalent:*

(i) U is semisimple.

(ii) U is a finite direct sum of simple modules.

(iii) Every submodule V of U has a complement; that is, there is a submodule W of U such that $U = V \oplus W$.

Proof. Suppose that (i) holds. That is, $U = \sum_{i\in I} S_i$, where I is an indexing set an S_i is a simple submodule of M for any $i \in I$. Let V be a submodule of U. Choose a maximal subset J of I such that $V \cap (\sum_{j\in J} S_j) = \{0\}$. Set $W = \sum_{j\in J} S_j$. Thus $V \cap W = \{0\}$; in order to show (iii) we will show that $U = V + W$. If not, then there is $i \in I$ such that S_i is not contained in $V + W$. But then $S_i \cap (V + W) = \{0\}$ because S_i is simple. Thus $V \cap (W + S_i) = \{0\}$. Indeed, if $v = w + s$ for some $v \in V$, $w \in W$, $s \in S_i$, then $v - w = s_i \in S_i \cap (V + W) = \{0\}$. This implies that $v = w$ and $s_i = 0$, hence $v = w \in V \cap W = \{0\}$, which implies $v = w = 0$. Therefore, the sum $V + (\sum_{j\in J\cup\{i\}} S_j)$ is still direct a direct sum, contradicting the maximality of J. This shows that $U = V \oplus W$, and hence (i) implies (iii). Suppose that (iii) holds. We show that then (ii) holds by induction over $\dim_k(U)$. Let S be a simple submodule of U. Then S has a complement W in U. Thus $U = S \oplus W$, and $\dim_k(W) < \dim_k(U)$. One sees easily that the hypothesis (iii) passes to the submodule W. By induction, W is a finite direct sum of simple modules, and hence so is U. This shows that (iii) implies (ii). Statement (ii) trivially implies (i). □

Corollary 4.3. *Let A be a k-algebra and U a finite-dimensional semisimple A-module. Then every quotient and every submodule of A is semisimple.*

Proof. Let V be a submodule of U. The image of a simple submodule of U in U/V is either zero or simple, and hence U/V is the sum of its simple submodules. This shows that U/V is semisimple. Let W be a complement of V in U. Then $U/W = (V \oplus W)/W \cong V$ is semisimple. □

Definition 4.4. A k-algebra A is called a *division algebra* if $A^\times = A\setminus\{0\}$; that is, if every nonzero element in A is invertible.

Thus a commutative division k-algebra is a field extension of k.

Theorem 4.5 (Schur's Lemma)**.** *Let A be a k-algebra. For any simple A-module S the k-algebra $\mathrm{End}_A(S)$ is a division algebra. For any two nonisomorphic simple A-modules S, T we have $\mathrm{Hom}_A(S,T) = \{0\}$.*

Proof. Let S, T be simple A-modules, and suppose there is a nonzero A-homomorphism $\varphi : S \to T$. Then $\ker(\varphi) \neq S$, hence $\ker(\varphi) = \{0\}$ because S is simple. Thus φ is injective. In particular, $\mathrm{Im}(\varphi) \neq \{0\}$. Since T is simple this implies $\mathrm{Im}(\varphi) = T$. Thus φ is an isomorphism. The result follows. □

If A is a finite-dimensional k-algebra, then every simple A-module S is finite-dimensional. In that case $\mathrm{End}_A(S)$ is a finite-dimensional division algebra over k and its center $Z(\mathrm{End}_A(S))$ is a finite-dimensional extension field of k. If k is algebraically closed, then every finite-dimensional division k-algebra is equal to k, and hence in that case we have $\mathrm{End}_A(S) \cong k$, which forces $\mathrm{End}_A(S) = \{\lambda \mathrm{Id}_S \mid \lambda \in k\}$; that is, the only A-endomorphisms of S are the scalar multiples of the identity map.

Corollary 4.6. *Suppose that k is an algebraically closed field, and let A be a k-algebra. For any simple A-module S of finite dimension over k we have $\mathrm{End}_A(S) = \{\lambda \mathrm{Id}_S \mid \lambda \in k\}$.*

Proof. Let $\varphi : S \to S$ be an A-endomorphism of S such that $\varphi \neq 0$. Since k is algebraically closed, the characteristic polynomial of φ has a root (in fact, all of its roots) in k, and hence φ has an eigenvalue $\lambda \in k$. If v is an eigenvector for λ, we have $\varphi(v) = \lambda v$, which is equivalent to $v \in \ker(\varphi - \lambda \mathrm{Id}_S)$. Thus $\varphi - \lambda \mathrm{Id}_S \in \mathrm{End}_A(S)$ is not injective and hence is zero by Schur's Lemma 4.5, and so $\varphi = \lambda \mathrm{Id}_S$. □

For U a module over some algebra A and B a subalgebra we denote by $\mathrm{Res}^A_B(U)$ the B-module obtained from restricting the action of A on U to the subalgebra B. If $A = kG$ for some group G and $B = kH$ for some subgroup H of G we write $\mathrm{Res}^G_H(U)$ instead of $\mathrm{Res}^A_B(U)$.

Theorem 4.7 (Clifford)**.** *Let G be a finite group and N a normal subgroup of G. For any simple kG-module S the restriction $\mathrm{Res}^G_N(S)$ of S to kN is a semisimple kN-module. Moreover, if T, T' are simple kN-submodules of $\mathrm{Res}^G_N(S)$ then there is an element $x \in G$ such that $T' \cong xT$. In other words, the isomorphism classes of simple kN-submodules of $\mathrm{Res}^G_N(S)$ are permuted transitively by the action of G.*

Proof. Let T be a simple kN-submodule of S restricted to kN. Let $x \in G$. The subset xT is again a simple kN-submodule of S restricted to kN. Indeed, it is a submodule because for $n \in N$ we have $nxT = x(x^{-1}nx)T \subseteq xT$ as N is normal in G. It is also simple because if V is a kN-submodule of xT then $x^{-1}V$ is a kN-submodule of T. This shows that if we take the sum of all simple kN-submodules of S of the form xT, with $x \in G$, we get a kG-submodule of S. Since S is simple this implies that S is the sum of the xT. □

Definition 4.8. The *Jacobson radical* $J(A)$ of a k-algebra A is the intersection of the annihilators of all simple left A-modules. More explicitly, $J(A)$ is equal to the set of all $a \in A$ satisfying $aS = \{0\}$ for every simple A-module S.

We will show that $J(A)$ is also the annihilator of all simple right A-modules. Clearly $J(A)$ is an ideal in A. For I an ideal in A and U an A-module, we denote by IU the A-submodule of U consisting of all finite sums of elements of the form au, where $a \in A$, $u \in U$. For I, J ideals in A, we denote by $I + J$ the ideal consisting of all elements of the form $a + b$, where $a \in I$, $b \in J$, and we denote by IJ the ideal consisting of all finite sums of elements of the form ab, where as before $a \in I$, $b \in J$. The sum and product of two ideals extend in the obvious ways to sums and products of finitely many ideals. In particular, for n a positive integer, the n-th power I^n of an ideal I consists of all finite sums of elements of the form $a_1 a_2 \cdots a_n$, where $a_i \in I$ for $1 \leq i \leq n$. For $n = 0$ we adopt the convention $I^0 = A$. An ideal I in A is called *nilpotent* if $I^n = \{0\}$ for some positive integer n. Since I^n contains all elements of the form a^n, where $a \in I$, it follows that all elements in a nilpotent ideal are nilpotent. There are however nonnilpotent ideals all of whose elements are nilpotent. We will show that if A is a finite-dimensional k-algebra, then $J(A)$ is the largest nilpotent ideal in A.

Lemma 4.9. *Let A be a k-algebra, U a nonzero A-module and let V be a maximal submodule of U. Then $J(A)U \subseteq V$. In particular, if U is finite-dimensional nonzero, then $J(A)U$ is a proper submodule of U.*

Proof. Since V is maximal in U it follows that U/V is a simple A-module. Thus $J(A)U/V = \{0\}$. This is equivalent to $J(A)U \subseteq V$. If U is finite-dimensional nonzero, then U has a maximal submodule (take any proper submodule of maximal dimension, for instance), and $J(A)U$ is contained in that maximal submodule by the first statement. □

Theorem 4.10 (Nakayama's Lemma). *Let A be a k-algebra. Let U be a finite-dimensional A-module. If V is a submodule of U such that $U = V + J(A)U$ then $U = V$. In particular, if $J(A)U = U$, then $U = \{0\}$.*

Proof. If $U = V + J(A)U$, then the quotient $M = U/V$ satisfies $J(A)M = M$. As U is finite-dimensional, so is M, and hence $M = \{0\}$ by 4.9. This implies $V = U$. The last statement is an equivalent reformulation of 4.9, and follows also from applying the first with $V = \{0\}$. □

Lemma 4.11. *Let I and J be nilpotent ideals in a k-algebra A. Then $I + J$ is a nilpotent ideal in A.*

Proof. Let m, n be positive integers such that $I^m = \{0\} = J^n$. The elements in $(I + J)^{m+n}$ are finite direct sums of products of the form $\prod_{1\leq i\leq m+n} (a_i + b_i)$, where $a_i \in I$ and $b_i \in J$. As I and J are ideals, any such expression is contained in $I^m + J^n = \{0\}$. □

Lemma 4.12. *Let A be a k-algebra and I a nilpotent ideal in A. Then I is contained in $J(A)$.*

Proof. Let S be a simple A-module. Then IS is a submodule of S, hence either equal to S or zero. If $IS = S$, then $I^nS = S$ for any positive integer n. In particular, I^n is nonzero for any positive integer n, contradicting the assumptions. Thus IS is zero for any simple A-module S, and hence $I \subseteq J(A)$. □

Theorem 4.13. *Let A be a finite-dimensional k-algebra. Then $J(A)$ is equal to any of the following ideals.*

(i) The unique maximal nilpotent ideal in A.

(ii) The intersection of all maximal left ideals in A.

(iii) The intersection of all maximal right ideals in A.

Proof. Since $J(A)$ contains every nilpotent ideal, in order to prove (i), it suffices to prove that $J(A)$ is nilpotent. If n is a positive integer such that $J(A)^n \neq \{0\}$, then Nakayama's Lemma 4.10 implies that $J(A)^{n+1}$ is properly contained in $J(A)$. Since A has finite dimension, it follows that $J(A)^n$ is zero for n large enough. This proves (i). If U is a maximal left ideal in A, then A/U is a simple A-module, hence annihilated by $J(A)$, or equivalently, $J(A) \subseteq U$. Thus $J(A)$ is contained in the intersection N of all maximal left ideals in A. If $J(A)$ were properly contained in N, then there is a simple A-module S such that $NS \neq \{0\}$. Thus there is $s \in S \setminus \{0\}$ such that $Ns = S$. Then $-s = xs$ for some $x \in N$, hence $(1+x)s = 0$. Thus $1+x$ is contained in the left annihilator of s, which is a proper left ideal (as it does not contain 1) and hence $1 + x$ is contained in a maximal left ideal M of A. Then $x \in N \subseteq M$, so $1 = (1 + x) - x \in M$, a contradiction. Thus $J(A) = N$, proving (ii). Since the characterisation of $J(A)$ as maximal nilpotent ideal does not refer to left or right modules, the same argument as in the proof of (ii) but with right modules proves (iii). □

Corollary 4.14. *Let A be a finite-dimensional k-algebra and B a subalgebra of A. We have $J(A) \cap B \subseteq J(B)$.*

Proof. One verifies easily that $J(A) \cap B$ is an ideal in B. Since $J(A)$ is nilpotent, so is $J(A) \cap B$, and hence $J(A) \cap B$ is contained in $J(B)$. □

Theorem 4.15. *Let A be a finite-dimensional k-algebra and U a finite-dimensional A-module. We have $J(A)U = \{0\}$ if and only if U is semisimple. In particular, $A/J(A)$ is semisimple as a left and right A-module.*

Proof. One direction is trivial: if U is semisimple, then $J(A)U = \{0\}$, because $J(A)$ annihilates every simple submodule of U. Suppose conversely that $J(A)U = \{0\}$. Since U is the sum of the submodules Au, where $u \in U$, it suffices to show that Au is semisimple. Note that Au is a quotient of A via the map sending $a \in A$ to au. Since $J(A)u = \{0\}$, this map contains $J(A)$ in its kernel, and hence it follows that Au is a quotient of $A/J(A)$ It suffices therefore to show that $A/J(A)$ is semisimple as a left A-module. By 4.13, $J(A)$ is the intersection of all maximal left ideals. But A has finite dimension, and hence after finitely many steps, taking intersections will no longer affect this intersection. Thus $J(A)$ is equal to the intersection of finitely many maximal left ideals; say $J(A) = \cap_{i=1}^{n} M_i$, where the M_i are maximal left ideals in A. By taking the sum of the canonical maps $A \to A/M_i$, we obtain a map $A \to \oplus_{i=1}^{n} A/M_i$. Each quotient A/M_i is simple, so the right side in this map is a semisimple A-module. The kernel of this map is the intersection of the M_i, hence equal to $J(A)$. Thus this map induces an injective A-homomorphism $A/J(A) \to \oplus_{i=1}^{n} A/M_i$. Since the right side is semisimple, so is $A/J(A)$. The same argument for right modules concludes the proof. □

Corollary 4.16. *Let A be a finite-dimensional k-algebra and U a finite-dimensional A-module. Then $J(A)U$ is equal to the intersection of all maximal submodules of U, and also equal to the smallest submodule V such that U/V is semisimple.*

Proof. By 4.15 applied to U/V, we have $J(A)U \subseteq V$ if and only if U/V is semisimple. This shows that $J(A)U$ is the smallest submodule such that the corresponding quotient by this submodule is semisimple. By 4.9, $J(A)U$ is contained in the intersection of all maximal submodules of U. Write $U/J(A)U$ as a direct sum of simple modules; say $U/J(A)U = \oplus_{i=1}^{n} S_i$. For $1 \leq i \leq n$, take for M_i the inverse image in U of the maximal submodule $S_1 \oplus \cdots S_{i-1} \oplus S_{i+1} \oplus \cdots \oplus S_n$. Then U/M_i is isomorphic to the simple A-module S_i, hence M_i is a maximal submodule of U, and $J(A)U = \cap_{i=1|}^{n} M_i$. Thus $J(A)U$ is equal to the intersection of a finite family of maximal submodules, but also contained in the intersection of all maximal submodules, so these intersections must be equal. □

Proposition 4.17. *Let A be a finite-dimensional k-algebra and let I be a proper ideal in A. Then $J(A/I) = J(A) + I/I$. In particular, if I is contained in $J(A)$, then $J(A/I) = J(A)/I$, and we have $J(A/J(A)) = \{0\}$.*

Proof. Since $J(A)$ is a nilpotent ideal, so is its image $J(A) + I/I$ in A/I, and hence $J(A) + I/I$ is contained in $J(A/I)$. For the reverse inclusion, we consider the canonical map $A/I \to A/(J(A)+I)$. This is a surjective homomorphism of A/I-modules with kernel $J(A) + I/I$, hence induces an isomorphism of A/I-modules

$$(A/I)/(J(A) + I/I) \cong A/J(A) + I.$$

The right side, when viewed as an A-module, is annihilated by $J(A)$, and therefore semisimple as an A-mdoule. But then so is the left side. Since the left side is annihilated by I, it follows that the left side is semisimple as an A/I-module. It follows from 4.15 that $J(A) + I/I$ contains $J(A/I)$. □

The next theorem shows that in order to detect whether a subset of an an algebra A generates A as an algebra, it suffices to show that it generates $A/J(A)^2$.

Theorem 4.18. *Let A be a finite-dimensional k-algebra and B a subalgebra of A such that $A = B + J(A)^2$. Then $A = B$.*

Proof. Since $J(A)$ is nilpotent, it suffices to show that $A = B+J(A)^n$ for any integer $n \geq 2$. Arguing by induction, suppose that $A = B + J(A)^n$ for some $n \geq 2$. Then $J(A) = (B \cap J(A)) + J(A)^n$. Thus $J(A)^n = ((B \cap J(A) + J(A)^n)^n$. It follows that any element a in $J(A)^n$ can be written in the form $a = (b + c)^n$, where $b \in B \cap J(A)$ and $c \in J(A)^n$. Developing the expression $(b + c)^n$ shows that any summand which involves at least one factor c is in $J(A)^{n+1}$, because $c \in J(A)^n \subseteq J(A)^2$. The only summand in the development of $(b + c)^n$ which does not involve c is the summand b^n, and this is an element in B. This shows that $a \in B + J(A)^{n+1}$, and hence $A = B + J(A)^{n+1}$ as required. ☐

Theorem 4.19. *Let A be a finite-dimensional k-algebra and let I be an ideal in A such that $I \subseteq J(A)$. We have $1 + I \subseteq A^\times$, and for any element $a \in A$ we have $a \in A^\times$ if and only if $a + I \in (A/I)^\times$. In particular, the canonical map $A \to A/I$ induces a short exact sequence of groups*

$$1 \longrightarrow 1 + I \longrightarrow A^\times \longrightarrow (A/I)^\times \longrightarrow 1$$

Proof. Since $I \subseteq J(A)$, the elements in I are invertible, and hence $1 + I \subseteq A^\times$. If $a \in A^\times$ then clearly $a+I \in (A/I)^\times$. Conversely, if $a \in A$ such that $a+I \in (A/I)^\times$ then $A = Aa+I$. Nakayama's Lemma 4.10 implies that $A = Aa$. This shows that $a \in A^\times$. Thus in particular the canonical group hommorphism $A^\times \to (A/I)^\times$ is surjective and has $1 + I$ as kernel. ☐

The above theorem remains true for arbitrary algebras.

Theorem 4.20. *Let A be a k-algebra and let e be an idempotent in A.*

(i) For any simple A-module S either $eS = \{0\}$ or eS is a simple eAe-module.

(ii) For any simple eAe-module T there is a simple A-module S such that $eS \cong T$.

Proof. Let S be a simple A-module such that $eS \neq \{0\}$, and let V be a nonzero eAe-submodule of eS. Then, since S is simple and e is an idempotent we have $S = AV = AeV$, hence $eS = eAeV = V$, which proves (i). Let T be a simple eAe-module. Then the A-module $Ae \otimes_{eAe} T$ is generated by any element of the form $e \otimes t$ for t a nonzero element in T, hence his module is finite-dimensional. It is also nonzero, as eAe is a direct summand of $Ae = eAe \oplus (1 - e)Ae$ as a right eAe-module. Let M be a maximal submodule of $Ae \otimes_{eAe} T$. Thus $S = Ae \otimes_{eAe} T/M$ is a simple A-module. The canonical surjection $\pi : Ae \otimes_{eAe} T \to S$ is nonzero on the subspace $e \otimes T$ because this space generates $Ae \otimes_{eAe} T$ as an A-module. Thus multiplying π by e yields a nonzero eAe-homomorphism $T \to eS$. Since eS is simple by (i), this implies that $T \cong eS$, whence (ii). ☐

Corollary 4.21. *Let A be a k-algebra and let e be an idempotent in A. We have $J(eAe) = eJ(A)e$.*

Proof. Since e is an idempotent, we have $J(A) \cap eAe = eJ(A)e$. This is a nilpotent ideal, because $J(A)$ is a nilpotent ideal, and hence $eJ(A)e \subseteq J(eAe)$. Conversely, let $c \in J(eAe)$. Then $c = ce$ annihilates every simple A-module S by 4.20 (i), whence $J(eAe) \subseteq J(A)$. Since e is an idempotent, this implies $J(eAe) \subseteq eJ(A)e$, whence the result. ☐

Definition 4.22. Let A be a k-algebra and U an A-module. The *socle of* U is the sum of all simple submodules in U.

We have an obvious version for the socle of right modules. If U is finite-dimensional, then the characterisation of semisimple modules implies that $\mathrm{soc}(U)$ is the largest semisimple submodule of U, and hence that $U = \mathrm{soc}(U)$ if and only if U is semisimple. For a nonzero finite-dimensional A-module, we have the following obvious consequences of the above:

Proposition 4.23. *Let A be a finite-dimensional k-algebra and U a nonzero A-module. The following hold.*

(i) The module $U/J(A)U$ is simple if and only if $J(A)U$ is the unique maximal submodule of U.

(ii) The submodule $\mathrm{soc}(U)$ is simple if and only if $\mathrm{soc}(U)$ is the unique simple submodule of U.

Proof. Trivial. □

Definition 4.24. Let G be a finite group. The kG-module k endowed with the identity action of all group elements is called the *trivial kG-module*. The algebra homomorphism $\eta : kG \to k$ sending $\sum_{x\in G} \lambda_x x$ to $\sum_{x\in G} \lambda_x$ is called the *augmentation homomorphism* and the ideal $I(kG) = \ker(\eta)$ is called the *augmentation ideal of kG*.

The augmentation homomorphism $kG \to k$ is the algebra homomorphism induced by the unique group homomorphism $G \to \{1\}$. This is the structural homomorphism of the trivial kG-module k. The augmentation ideal $I(kG)$ has dimension $|G| - 1$ and is spanned by the elements of the form $x - 1$, where $x \in G \setminus \{1\}$. Since it has codimension 1 in kG, it is maximal as a left ideal or as a right ideal. In particular, the augmentation ideal $I(kG)$ contains the radical $J(kG)$.

Theorem 4.25. *Let p be a prime. Suppose that k is a field of characteristic p. Let P be a finite p-group. We have $I(kP)^{|P|} = \{0\}$. In particular, $J(kP) = I(kP)$, and the trivial kP-module k is, up to isomorphism, the unique simple kP-module.*

Proof. The augmentation ideal $I(kP)$ is a maximal ideal in kP because the quotient $kP/I(kP) \cong k$ is one-dimensional, hence simple as a left kP-module. Thus all we have to show is that the ideal $I(kP)^{|P|}$ is zero. We proceed by induction over the order of P. For $P = \{1\}$ there is nothing to prove. Suppose $|P| > 1$. Then $Z(P)$ is non-trivial. Thus $Z(P)$ has an element z of order p. Let $Z = \langle z\rangle$ be the cyclic central subgroup of order p in P generated by z. Consider the canonical group homomorphism $P \to P/Z$. An easy verification shows that the kernel of this algebra homomorphism is $I(kZ)kP$, which is clearly contained in $I(kP)$. Thus this algebra homomorphism sends $I(kP)$ to $I(kP/Z)$. By induction, $I(kP/Z)^{|P/Z|}$ is zero. This means that $I(kP)^{|P/Z|}$ lies in the kernel $I(kZ)kP$ of the algebra homomorphism $kP \to kP/Z$. It suffices therefore to show that the p-th power of this kernel is zero. Since k has characteristic p, we have $(z - 1)^p = z^p - 1^p = 0$ because z has order p. For any positive integer m we have $z^m - 1 = (z-1)(1+z+\cdots+z^{m-1})$, and hence $I(kZ) = (z-1)kZ$. Thus $I(kZ)^p = \{0\}$. Since $I(kZ)KP = kPI(kZ)$, we get that $(I(kZ)kP)^p = I(kZ)^p kP = \{0\}$. The result follows. □

Corollary 4.26. *Let p be a prime. Suppose that k is a field of characteristic p. Let P be a finite p-group*

(i) kP is indecomposable as a left or right kP-module.

(ii) The unit element of kP is the unique idempotent in kP.

(iii) The unit element of kP is the unique block of kP; equivalently, kP is indecomposable as a k-algebra.

Proof. Since $J(kP) = I(kP)$ has codimension 1 in kP, this must be the unique maximal left submodule of kP. A module with a unique maximal submodule is automatically indecomposable, whence (i). Let i be an idempotent in kP. Then kPi is a direct summand of the regular kP-module kP. Since kP is indecomposable we have $kPi = kP$, hence $i = 1$. This shows (ii), and (iii) is a trivial consequence of (ii). $\square$

Corollary 4.27. *Let p be a prime. Suppose that k is a field of characteristic p. Let P be a finite p-group. Every nonzero kP-module which is a quotient of the regular kP-module is indecomposable. In particular, for any subgroup Q of P the transitive permutation kP-module kP/Q is indecomposable.*

Proof. Any nonzero quotient of kP as a kP-module is isomorphic to kP/M for a proper left ideal M. Since $J(kP) = I(kP)$ is the unique maximal left ideal, it follows that M is contained in $J(kP)$. Thus $J(kP)/M$ is the unique maximal submodule of kP/M, and hence kP/M is indecomposable. $\square$

Theorem 4.28. *Let G be a finite group, p a prime and P be a normal p-subgroup in G. Suppose that k is a field of characteristic p. Then all elements in P act trivially on every simple kG-module, and we have $I(kP)kG \subseteq J(kG)$.*

Proof. We give two proofs. By Clifford's Theorem 4.7 every simple kG-module S restricted to kP is semisimple. But the trivial kP-module k is, up to isomorphism, the only simple kP-module, hence all elements of P act trivially on S. But then all elements of kG of the form $y - 1$ with $y \in P$ annihilate all simple modules, so $y - 1 \in J(kG)$. Since $J(kG)$ is an ideal it follows that $I(kP)kG \subseteq J(kG)$. Alternatively, it follows from 4.25 that $I(kP)$ is a nilpotent ideal in kP. Since P is normal in kG we get that $I(kP)kG = kGI(kP)$ is a nilpotent ideal in kG, hence contained in $J(kG)$. Since all elements of $J(kG)$ annihilate every simple kG-module, in particular all elements of the form $y - 1$ with $y \in P$ annihilate all simple kG-modules, which is equivalent to saying that all elements $y \in P$ act trivially on all simple kG-modules. $\square$

Exercises 4.29.

(1) Let A be a finite-dimensional k-algebra. Show that $J(Z(A)) = Z(A) \cap J(A)$.

(2) Let A be a finite-dimensional commutative k-algebra. Show that $J(A)$ is equal to the set of all nilpotent elements in A.

(3) Let n be a positive integer and le T_n be the subalgebra of $M_n(k)$ consisting of all upper triangular matrices. Show that $J(T_n)$ consists of all strict upper triangular matrices; that is, all upper triangular matrices with zdero in the diagonal.

(4) Let B and C be finite-dimensional k-algebras. Show that $J(B \times C) = J(B) \times J(C)$.

(5) Let N be a normal subgroup of a finite group G. Show that the kernel of the canonical algebra homomorphism $kG \to kG/N$ is equal to $I(kN)kG = kGI(kN)$.

(6) Suppose that $\mathrm{char}(k) = p > 0$. Let P be a finite cyclic p-group of order p^m. Show that there is an algebra isomorphism $kP \cong k[x]/(x^m)$.

(7) Show that $J(\mathbb{Z}) = \{0\}$, and that $\mathbb{Z}$ is indecomposable but not simple as a $\mathbb{Z}$-module.

(8) Let G be a finite group. Show that $k\sum_{x \in G} x$ is the unique trivial kG-submodule of the regular kG-module kG.

(9) Suppose that $\mathrm{char}(k) = p > 0$. Let P be a finite p-group. Show that $\mathrm{soc}(kP) \cong k$, where kP is viewed as the regular kP-module.

(10) Let G be a finite group. Show that the regular kG-module kG has a unique trivial submodule, and show that this trivial submodule is equal to $k(\sum_{x \in G} \ x)$.

5 Wedderburn's theorem and Maschke's theorem

Definition 5.1. A k-algebra A is called *simple* if A is nonzero and has no ideals other than $\{0\}$ and A.

A simple algebra A is necessarily indecomposable, because if $A = B \times C$ is the direct product of two algebras B and C, then $B \times \{0\}$ and $\{0\} \times C$ are proper nonzero ideals in A. If U is an A-module and n a positive integer, we denote by $U^n = U \oplus U \oplus \cdots \oplus U$ the direct sum of n copies of U.

Theorem 5.2. *Let A be a finite-dimensional k-algebra A. The following are equivalent.*

(i) The algebra A is simple.

(ii) There is a simple A-module S and a positive integer n such that $A \cong S^n$ as a left A-module.

(iii) There is a positive integer n and a finite-dimensional division k-algebra D such that $A \cong M_n(D)$ as a k-algebra.

Moreover, if A is simple, then S is up to isomorphism the unique simple A-module, A is semisimple as a left A-module, and we have $D \cong \mathrm{End}_A(S)^{op}$.

Proof. Suppose that A is simple. Let S be a simple submodule of A as a left module. Let $a \in A$. As S is a left submodule of A, also Sa is a left submodule of A. The map $S \to Sa$ sending $s \in S$ to $sa \in Sa$ is a surjective A-homomorphism. Thus either $Sa = \{0\}$ or $Sa \cong S$. Set $I = \sum_{a \in A} \ Sa$. This is now a two-sided ideal in A, hence equal to A. But I is also a sum of simple submodules, all isomorphic to S. It follows that A is a finite direct sum of copies of S as a left A-module, hence $A \cong S^n$. Thus (i) implies (ii). Suppose that (ii) holds. Since every simple A-module is a quotient of A this implies that every simple A-module is isomorphic to S. Thus $A \cong \mathrm{End}_A(A)^{op} \cong \mathrm{End}_A(S^n)^{op} \cong M_n(\mathrm{End}_A(S))^{op} \cong M_n(\mathrm{End}_A(S)^{op})$, where the last isomorphism sends a matrix to its transpose. Take $D = \mathrm{End}_A(S)^{\mathrm{op}}$; this is a division algebra by Schur's Lemma. This shows that (ii) implies (iii). The remaining implication, showing that a matrix algebra over a division algebra is simple, is an easy exercise. $\square$

In particular, $M_n(k)$ is simple for any positive integer n, and $M_n(k)$ has as unique simple module, up to isomorphism, the space of n-dimensional column vectors k^n. The n columns in $M_n(k)$ yield a decomposition of $M_n(k)$ as a direct sum of n copies of k^n. If k is algebraically closed, there are no other simple k-algebras because in that case there are no nontrivial finite-dimensional division k-algebras.

Corollary 5.3. *Suppose that k is algebraically closed. A finite-dimensional k-algebra A is simple if and only if $A \cong M_n(k)$ for some positive integer n.*

Definition 5.4. A k-algebra A is called *semisimple* if A is semisimple as a left A-module, or equivalently, if the regular left A-module is a direct sum of simple A-modules.

The following lemma implies that a finite-dimensional k-algebra is semisimple as a left A-module if and only if it is semisimple as a right A-module.

Lemma 5.5. *Let A be a finite-dimensional k-algebra. The following are equivalent.*

(i) A is semisimple.

(ii) $J(A) = \{0\}$.

(iii) Every finite-dimensional left or right A-module is semisimple.

Proof. It follows from 4.16 that $A/J(A)$ is the largest semisimple quotient of A as a left A-module, so (i) implies (ii). If $J(A)$ is zero, then every finite-dimensional A-module is semisimple by 4.15, and hence (ii) implies (iii). The implication (iii) $\Rightarrow$ (i) is trivial. $\square$

For algebras over arbitrary commutative rings it may happen that the radical is zero while the algebra is not semisimple as a left module. Wedderburn's Theorem shows that semisimple finite-dimensional algebras are exactly the finite direct products of simple algebras.

Theorem 5.6 (Wedderburn)**.** *A finite-dimensional k-algebra is semisimple if and only if it is a direct product of finitely many simple k-algebras. In that case, this direct product is unique up to order. More precisely, let A be a finite-dimensional semisimple k-algebra. Let $\{S_i \mid 1 \leq i \leq m\}$ be a system of representatives of the isomomorphism classes of simple A-modules. Set $D_i = \mathrm{End}_A(S_i)^{\mathrm{op}}$ and let n_i be the unique positive integer such that $A \cong \oplus_{1\leq i\leq m}\ (S_i)^{n_i}$ as a left A-module. Then we have an isomorphism of k-algebras*

$$A \;\cong\; \prod_{1\leq i\leq m} M_{n_i}(D_i)\ .$$

Each simple factor $M_{n_i}(D_i)$ has S_i as its unique simple module up to isomorphism.

Proof. We use the algebra isomorphism $\mathrm{End}_A(A) \cong A^{op}$ sending $\varphi \in \mathrm{End}_A(A)$ to $\varphi(1)$. We have

$$\mathrm{End}_A(A) = \mathrm{End}_A(\oplus_{1\leq i\leq m}\ (S_i)^{n_i}) \cong \prod_{1\leq i\leq m} \mathrm{End}_A((S_i)^{n_i}) \cong \prod_{1\leq i\leq m} M_{n_i}(D_i^{\mathrm{op}})$$

where we used Schur's Lemma 4.5 in the last two isomorphisms. Finally, the opposite of the matrix algebra $M_{n_i}(D_i^{\mathrm{op}})$ is isomorphic to $M_{n_i}(D_i)$, by taking the transpose of matrices. $\square$

Note in particular that the number of isomorphism classes of simple modules of a finite-dimensional semisimple k-algebra A is equal to the number of simple direct algebra factors of A. The simple direct algebra factors of A are indecomposable as algebras, and hence the product decomposition of A in Wedderburn's theorem is also the block decomposition of A.

Theorem 5.7. *Suppose that k is algebraically closed. Let A be a finite-dimensional k-algebra. For any simple A-module S the structural map $A \to \mathrm{End}_k(S)$ is surjective. Let $\{S_i\}_{1\leq i\leq h}$ be a system of representatives of the isomorphism classes of simple A-modules. The product of the structural homomorphisms $A \to \mathrm{End}_k(S_i)$ induces an isomorphism of k-algebras*

$$A/J(A) \cong \prod_{1\leq i\leq h} \mathrm{End}_k(S_i)$$

Proof. The product of the structural maps $A \to \mathrm{End}_k(S_i)$ has as kernel the Jacobson radical $J(A)$ and hence induces an injective algebra homomorphism $A/J(A) \to \prod_{1\leq i\leq h} \mathrm{End}_A(S_i)$. Since k is algebraically closed, it follows from Wedderburn's theorem that the algebra $A/J(A)$ is a direct product of matrix algebras $M_{n_i}(k)$. Thus both sides have the same dimension, whence the isomorphism as stated. □

Theorem 5.8 (Maschke's Theorem)**.** *Let G be a finite group. Then kG is semisimple if and only if either* $\mathrm{char}(k) = 0$ *or* $\mathrm{char}(k) = p$ *does not divide the order of G.*

Proof. Suppose that either $\mathrm{char}(k) = 0$ or $\mathrm{char}(k) = p$ does not divide the order of G. Thus $|G|$ is invertible in k. Let U be a finite-dimensional kG-module and let V be a submodule of U. We need to show that V is a direct summand of U as a kG-module, or equivalently, that V has a complement in U. Since V is in particular a k-subspace of U, there is clearly a k-subspace W of U such that $U = V \oplus W$ as k-vector spaces (but W need not be a kG-submodule). Let $\pi : U \to V$ be the k-linear projection of U onto V with kernel W. Define a map $\tau : U \to U$ by

$$\tau(u) = \frac{1}{|G|}\sum_{x\in G} x\pi(x^{-1}u)$$

for all $u \in U$. Since $\pi(V) \subseteq V$ we also have $\tau(V) \subseteq V$; we use here that V is a kG-submodule of U. For $v \in V$ we have $\pi(v) = v$, and hence $\pi(x^{-1}v) = x^{-1}v$ for all $x \in G$. Thus $\tau(v) = \frac{1}{|G|}\sum_{x\in G} xx^{-1}v = \frac{1}{|G|}|G|v = v$. This means that τ is again a linear projection of U onto V. But τ is also a kG-homomorphism: if $y \in G$ and $u \in U$, then

$$y\tau(y^{-1}u) = \frac{1}{|G|}\sum_{x\in G} yx\pi(x^{-1}y^{-1}u) = \frac{1}{|G|}\sum_{x\in G} x\pi(x^{-1}u) = \tau(u)\ ,$$

where we have made use of the fact that if x runs over the elements in G, then so does yx. It follows that τ is a projection of U onto V as a kG-module, and hence $\ker(\tau)$ is a complement of V in U. Thus M is semisimple by 4.2. For the converse, assume that $\mathrm{char}(k) = p$ divides $|G|$; that is, the image of $|G|$ in k is zero. Set $z = \sum_{x\in G} x$; we clearly have $xz = z = zx$ for any $x \in G$, and hence $z^2 = |G|z = 0$. Thus z is a nilpotent element in $Z(kG)$ and hence $zkG = kGz$ is a nilpotent ideal in kG, thus contained in $J(kG)$ by 4.12. □

Theorem 5.9. *Let G be a finite group. Suppose that k is algebraically closed and that either* $\mathrm{char}(k) = 0$ *or that* $\mathrm{char}(k) = p$ *for some prime number p which does not divide $|G|$. Then the number of isomorphism classes of simple kG-modules is equal to the number of conjugacy classes of G.*

Proof. We will show that both numbers are equal to the dimension of $Z(kG)$. By Maschke's theorem 5.8, the group algebra kG is semisimple. Thus, by Wedderburn's theorem 5.6, the algebra kG is isomorphic to a direct product of matrix algebras, say $kG \cong \prod_{i=1}^{h} M_{n_i}(k)$. Each matrix factor has a unique simple module, up to isomorphism, and hence h is the number of isomorphism classes of simple kG-modules. We have $Z(M_{n_i}(k)) \cong k$, hence $\dim_k(Z(kG)) = h$. By the exercise 1.9 (4), the number h is also equal to the number of conjugacy classes in G. $\square$

We mention without proof the following result.

Theorem 5.10 (Brauer)**.** *Let G be a finite group and k an algebraically closed field of prime characteristic p. Then the number of isomorphism classes of simple kG-modules is equal to the number of conjugacy classes of elements of order prime to p in G.*

Exercises 5.11.

(1) Let A be a finite-dimensional semisimple k-algebra. Show that every nonzero ideal in A is equal to AeA for some central idempotent in A. Deduce that A has only finitely many ideals. More precisely, show that the number of ideals in A is equal to 2^h, where h is the number of isomorphism classes of simple A-modules.

(2) Let V be a finite-dimensional k-vector space. Show that up to isomorphism, V is the unique simple $\mathrm{End}_k(V)$-module. Use this to show that every algebra automorphism of $\mathrm{End}_k(V)$ is an inner automorphism. (This is known as the Skolem-Noether theorem).

6 The Krull-Schmidt theorem and idempotent lifting

The Krull-Schmidt theorem states that a nonzero finite-dimensional module can be written uniquely, up to isomorphism and order, as a direct sum of indecomposable modules.

Theorem 6.1 (Krull-Schmidt)**.** *Let A be a finite-dimensional k-algebra and let U be a finite-dimensional A-module. Then U is a direct sum of finitely many indecomposable submodules of U. Suppose that $U = \oplus_{1 \leq i \leq n} U_i = \oplus_{1 \leq j \leq m} V_j$, where n, m are positive integers and U_i, V_j non zero indecomposable submodules of U for any i, j. Then we have $n = m$ and there is a permutation π on the set $\{1, 2, .., n\}$ such that $U_i \cong V_{\pi(i)}$ for all i, $1 \leq i \leq n$.*

If U is semisimple, then all U_i, V_j are simple, and hence the Krull-Schmidt theorem is in this case an easy consequence of Schur's lemma. We will use this observation in the proof. Since direct sum decompositions of a module U correspond to idempotent decompositions in the algebra $\mathrm{End}_A(U)$, one way to prove the Krull-Schmidt theorem is to prove the following more general result on primitive decompositions.

Theorem 6.2. *Let A be a finite-dimensional k-algebra, and let e be an idempotent in A. Then e has a primitive decomposition, and any two primitive decompositions I, J of e are conjugate in A; that is, there is $u \in A^\times$ such that $J = uIu^{-1}$.*

The key ingredient of the proof is the notion of a local algebra.

Definition 6.3. A k-algebra A is called *local* if $A/J(A)$ is a division k-algebra; that is, if all nonzero elements in $A/J(A)$ are invertible.

Finite-dimensional local algebras admit the following characterisation.

Proposition 6.4. *Let A be a finite-dimensional algebra. The following are equivalent.*

(i) The unit element 1_A is a primitive idempotent.

(ii) The algebra A is local; that is, $A/J(A)$ is a division k-algebra.

(iii) We have $A = A^\times \cup J(A)$, and this union is disjoint.

(iv) Every element in A is either invertible or nilpotent.

Proof. If (iii) holds, then every nonzero element in $A/J(A)$ is of the form $u+J(A)$ for some $u \in A^\times$, hence every nonzero element in $A/J(A)$ is invertible, and hence (ii) holds. If 1_A is not primitive, then A contains an idempotent i different from 1_A, and hence $i+J(A)$ is an idempotent in $A/J(A)$ or zero. But $J(A)$ contains no idempotent, and hence $i + J(A)$ is an idempotent different from $1 + J(A)$. An idempotent which is not 1 cannot be invertible, and hence $A/J(A)$ cannot be a division algebra. Thus (ii) implies (i). Suppose that (i) holds. Let $x \in A$. Consider the decreasing sequence of left ideals

$$A \supseteq Ax \supseteq Ax^2 \supseteq \cdots$$

This sequence will become eventually constant, as A has finite dimension. Thus there is a positive integer n such that $Ax^n = Ax^{n+2} = Ax^{n+2} \cdots$. Set $U = Ax^n$ and $V = \{a \in A \mid ax^n = 0\}$. That is, U is the image of the linear endomorphism sending $a \in A$ to ax^n, and V is the kernel of that endomorphism. Thus $\dim_k(A) = \dim_k(U) + \dim_k(V)$. Since $U = Ax^n = Ax^{2n}$ we have $U \cap V = \{0\}$, hence $A = U \oplus V$ as A-modules. It follows from 3.7 that $U = Ai$, where either $i = 0$, or i is an idempotent in A. Since 1 is the unique idempotent, we have either $i = 0$ or $i = 1$. If $i = 0$, then x is nilpotent. If $i = 1$, then x is invertible. In other words, all noninvertible elements in A are nilpotent. Thus (i) implies (iv). Suppose that (iv) holds; that is, all elements in $A \setminus A^\times$ are nilpotent. If x is nilpotent in A, then no element in Ax or xA is invertible, hence all elements in Ax and xA are nilpotent. Thus the nilpotent elements in A form an ideal. This is the unique maximal ideal and the unique maximal left ideal, because a proper (left) ideal contains no invertible elements, and hence this ideal is equal to $J(A)$. Thus (iv) implies (iii). $\square$

Corollary 6.5. *Let A be a k-algebra. A finite-dimensional A-module U is indecomposable if and only if the algebra $\mathrm{End}_A(U)$ is local, hence if and only if any endomorphism of U is either an automorphism or nilpotent.*

Proof. A module U is indecomposable if and only if Id_U is primitive in $\mathrm{End}_A(U)$. Thus 6.5 is a special case of 6.4 $\square$

The invertible elements in $\mathrm{End}_A(U)$ are the automorphisms of U as an A-module. Thus if U is finite-dimensional and φ is an A-endomorphism of U which is not an automorphism, then $\varphi \in J(\mathrm{End}_A(U))$, and in particular, φ is nilpotent.

Corollary 6.6. *Let A be a finite-dimensional local k-algebra, and let I be a proper ideal in A. Then $I \subseteq J(A)$, and the k-algebra A/I is local.*

Proof. The property $A = A^\times \cup J(A)$ passes down to the quotient algebra A/I. $\square$

Corollary 6.7. *Let A be a finite-dimensional k-algebra such that 1_A is primitive in A. Then $J(A)$ is the unique maximal left ideal, the unique maximal right ideal, and the unique maximal ideal in A.*

Proof. A proper left or right ideal of 2-sided ideal consists necessarily of noninvertible elements. By 6.4, if 1_A is primitive, then $J(A)$ is equal to the set of all noninvertible elements in A, whence the result. □

Corollary 6.8 (Rosenberg's lemma)**.** *Let M be a family of ideals in a finite-dimensional k-algebra A, and let i be a primitive idempotent in A such that $i \in \sum_{I \in M} I$. Then there is an ideal $I \in M$ such that $i \in I$.*

Proof. Since i is an idempotent, we have $i \in \sum_{I \in M} iIi$, each iIi is an ideal in iAi, and at least one of these ideals is not containd in $J(iAi)$. Since i is primitive, the algebra iAi is local, and therefore, if iIi is not contained in $J(iAi)$, then iIi contains an invertible element in iAi, hence $iIi = iAi$. This implies $i \in iIi \subseteq I$, whence the result. □

Proposition 6.9. *Let A be a k-algebra and let i, j be idempotents in A. For any A-homomorphism $\psi : Ai/J(A)i \to Aj/J(A)j$ there is an A-homomorphism $\varphi : Ai \to Aj$ which 'lifts' ψ; that is, which makes the following diagram commutative:*

$$\begin{tikzcd}
Ai \arrow[r, "\varphi"] \arrow[d] & Aj \arrow[d] \\
Ai/J(A)i \arrow[r, "\psi"'] & Aj/J(A)j
\end{tikzcd}$$

Here the vertical maps are the canonical surjections sending ai to $ai + J(A)i$ and aj to $aj + J(A)j$, for $a \in A$.

Proof. As a left A-module, Ai is generated by i, and hence $Ai/J(A)i$ is generated by $i + J(A)i$. Thus ψ is completely determined by $\psi(i+J(A)i)$. Write $\psi(i+J(A)i) = b+J(A)j$ for some $b \in Aj$. Define φ by $\varphi(ai) = aib$ for $a \in A$. A trivial verification shows that this is an A-homomorphism with the required properties. □

This proposition is a special case of lifting homomorphisms starting from a projective module through a surjective homomorphism - we will come back to this later.

Corollary 6.10. *Let A be a finite-dimensional k-algebra, and let i be a primitive idempotent in A. Then the A-module $Ai/J(A)i$ is simple. Equivalently, Ai has a unique maximal submodule.*

Proof. If $\varphi \in \mathrm{End}_A(Ai)$, then φ sends $J(A)i$ to $J(A)i$, hence induces an endomorphism $\bar{\varphi} \in \mathrm{End}_A(Ai/J(A)i)$. The map sending φ to $\bar{\varphi}$ is an algebra homomorphism from $\mathrm{End}_A(Ai)$ to $\mathrm{End}_A(Ai/J(A)i)$ By 6.9 applied wih $i = j$, this algebra homomorphism is surjective. Thus $\mathrm{End}_A(Ai/J(A)i)$ is a quotient algebra of $\mathrm{End}_A(Ai) \cong (iAi)^{\mathrm{op}}$. This, however, is a local algebra because i is primitive. It follows from 6.6 that $\mathrm{End}_A(Ai/J(A)i)$ is local. Thus $Ai/J(A)i$ is an indecomposable A-module. But $Ai/J(A)i$ is also semisimple. Thus $Ai/J(A)i$ is simple. □

Corollary 6.11. *Let A be a finte-dimensional k-algebra, S a simple A-module, and let i be a primitive idempotent in A. Then iS is nonzero if and only if $S \cong Ai/J(A)i$.*

Proof. By 3.9, the vector space iS is nonzero if and only if there is a nonzero A-homomrophism $\varphi : Ai \to S$. Since S is simple, any nonzero homomorphism to S is surjective. Thus iS is nonzero if and only if S is isomorphic to a quotient of Ai, hence isomorphic to Ai/M for some maximal submodule of Ai. By 6.10 the module $J(A)i$ is the unique maximal submodule of Ai, whence the result. $\square$

Corollary 6.12. *Let A be a finte-dimensional k-algebra, and let S be a simple A-module. Then there is a primitive idempotent $i \in A$ such that $S \cong Ai/J(A)i$.*

Proof. Let I be a primitive decomposition of 1. Since 1 acts as identity on S, we have $1 \cdot S \neq \{0\}$. Thus there is $i \in I$ such that $iS \neq \{0\}$. It follows from 6.11 that $S \cong Ai/J(A)i$. $\square$

Corollary 6.13. *Let A be a finite-dimensional k-algebra, and let i, j be primitive idempotents in A. We have $Ai \cong Aj$ if and only if $Ai/J(A)i \cong Aj/J(A)j$.*

Proof. If $Ai \cong Aj$, then any such isomorphic sends $J(A)i$ onto $J(A)j$ because these are the unique maximal submodules of Ai and Aj, respectively, and hence this induces an isomorphism $Ai/J(A)i \cong Aj/J(A)j$. Suppose conversely that we have an isomorphism $\psi : Ai/J(A)i \cong Aj/J(A)j$. By 6.9 there is an A-homomorphism $\varphi : Ai \to Aj$ which lifts ψ. Since $\psi \neq 0$ it follows that $\mathrm{Im}(\varphi)$ is not contained in the maximal submodule $J(A)j$. Thus $Aj = \mathrm{Im}(\varphi) + J(A)j$. Nakayama's lemma implies $Aj = \mathrm{Im}(\varphi)$; that is, φ is surjective. Exchanging the roles of Ai and Aj and using the inverse of ψ it follows that there is also a surjective map $Aj \to Ai$. But then Ai and Aj have the same dimension, and hence φ is an isomorphism. $\square$

Proof of Theorem 6.2. The existence of a primitive decomposition of e was noted earlier. Since $e = \sum_{i \in I} i = \sum_{j \in J} j$ we have two decompositions of the left A-module Ae as a direct sum of indecomposable $A-$modules $Ae = \oplus_{i \in I} Ai = \oplus_{j \in j} Aj$. Dividing by the radical yields $Ae/J(A)e = \oplus_{i \in I} Ai/J(A)i = \oplus_{j \in J} Aj/J(A)j$. By 6.10, the modules $Ai/J(A)i$, $Aj/J(A)j$ are simple. Thus there is a bijective map $\pi : I \longrightarrow J$ such that $Ai/J(A)i \cong A\pi(i)/J(A)\pi(i)$ for all $i \in I$. But then 6.13 implies that $Ai \cong A\pi(i)$ for all $i \in I$. Any such isomorphism is induced by right multiplication with an element $c_i \in iA\pi(i)$, and its inverse is induced by an element $d_i \in \pi(i)Ai$, such that $c_i d_i = i$ and $d_i c_i = \pi(i)$ for all $i \in A$. Set now $u = 1 - e + \sum_{i \in I} d_i$ and $v = 1 - e + \sum_{i \in I} c_i$. Since the elements of I (resp. J) are pairwise orthogonal, we have $uv = vu = 1$ and $uiv = \pi(i)$ for all $i \in I$, which implies the theorem. $\square$

Proof of Theorem 6.1. Any direct sum decomposition of an A-module U as a finite direct sum of indecomposable A-modules corresponds to a primitive decomposition of Id_U in the algebra $\mathrm{End}_A(U)$, namely the set consisting of the canonical projections onto the indecomposable direct summands. The module version of the Krull-Schmidt theorem follows from 6.2 applied to primitive decompositions in $\mathrm{End}_A(U)$. $\square$

Corollary 6.14. *Let A be a finite-dimensional k-algebra, and let i, j be idempotents in A. We have $Ai \cong Aj$ as left A-modules if and only if the idempotents i and j are conjugate in A.*

Proof. Write $A = Ai \oplus A(1-i) = Aj \oplus A(1-j)$. If $Ai \cong Aj$, then the Krull-Schmidt theorem implies that also $A(1-i) \cong A(1-j)$. Thus there are elements $c \in iAj$, $d \in jAi$ satisfying $cd = i$, $dc = j$, and there are elements $e \in (1-i)A(1-j)$, $f \in (1-j)A(1-i)$ satisfying $ef = 1-i$, $fe = 1-j$. set $u = c+e$ and $v = d+f$. We get that $uv = (c+e)(d+f) = cd + cf + ed + ef = i + (1-i) = 1$, and similarly, $vu = 1$. Moreover, $ujv = (c+e)j(d+f) = cjd = cd = i$, hence i and j are conjugate. Conversely, suppose that i and j are conjugate; that is, there is $u \in A^\times$ such that $uju^{-1} = i$. Then $Aj = Auj$, and hence right multiplication by u^{-1} sends Aj to $Auju^{-1} = Ai$. This is an isomorphism $Aj \cong Ai$, with inverse given by right multiplication with u. □

Corollary 6.15. *Let A be a finite-dimensional k-algebra, and let i, j be idempotents in A. Then i and j are not conjugate in A if and only if $iAj \subseteq J(A)$.*

Proof. Suppose that $iAj \subseteq J(A)$. Every A-homomorphism $Ai \to Aj$ is given by right multiplication with an element $c \in iAj \subseteq J(A)$, thus has image contained in $J(A) \cap Aj = J(A)j$. Thus there is no isomorphism $Ai \cong Aj$. It follows from 6.14 that i, j are not conjugate. For the converse, observe first that if there is a surjective A-homomorphism $Ai \to Aj$, then such a homomorphism is an isomorphism. Indeed, a surjective A-homomorphism $Ai \to Aj$ induces a surjective homomorphism $Ai/J(A)i \to Aj/J(A)j$. Both sides are simple modules, so this is an isomorphism, and hence i, j are conjugate, and $Ai \cong Aj$. Thus if i, j are not conjugate, then the image of every homomorphism $Ai \to Aj$ is a proper submodule of Aj, hence contained in the unique maximal submodule $J(A)j$ of Aj. Since right multiplication by any element $c \in iAj$ induces an A-homomorphism $\varphi : Ai \to Aj$ satisfying $\varphi(i) = c \in \mathrm{Im}(\varphi) \subseteq J(A)j$, it follows that $iAj \subseteq J(A)$. □

Corollary 6.16. *Let A be a finite-dimensional simple k-algebra. The map sending a primitive idempotent i in A to the simple A-module $Ai/J(A)i$ induces a bijection between the set of conjugacy classes of primitive idempotents in A and the set of isomorphism classes of simple A-modules.*

Proof. This follows from combining 6.10, 6.12, 6.13, and 6.14. □

Corollary 6.17. *Let A be a finite-dimensional simple k-algebra. Then A has a unique conjugacy class of primitive idempotents.*

Proof. By 5.2, A has a unique isomorphism class of simple modules S, and $J(A) = \{0\}$. Thus for any primitive idempotent $i \in A$ we have $Ai \cong S$, and hence all primitive idempotents in A are conjugate by 6.14. □

Let $f : A \to B$ be a homomorphism. If i is an idempotent in A, then either $f(i) = 0$, or $f(i)$ is an idempotent in B. We will show that if f is surjective, then f maps any primitive idempotent in A to either zero or to a primitive idempotent.

Theorem 6.18 (Lifting theorem of idempotents)**.** *Let A, B be finite-dimensional k-algebras, and let $f : A \to B$ be a surjective algebra homomorphism.*

(i) The homomorphism f maps $J(A)$ onto $J(B)$ and $A^\times$ onto $B^\times$.

(ii) For any primitive idempotent i in A either $i \in \ker(f)$ or $f(i)$ is a primitive idempotent in B.

(iii) For any primitive idempotent j in B there is a primitive idempotent i in A such that $f(i) = j$.

(iv) Any two primitive idempotents i, i' in A not contained in $ker(f)$ are conjugate in A if and only if $f(i)$, $f(i')$ are conjugate in B.

Proof. Since f is surjective, it follows that $f(J(A))$ is an ideal in B and that $B/f(J(A)) \cong A/J(A)$ is semisimple. Since $J(A)$ is nilpotent, so is $f(J(A))$. Thus $f(J(A)) = J(B)$. In order to show that f maps $A^\times$ onto $B^\times$, we first note that if A and B are semisimple, this follows from Wedderburn's theorem because in that case, f is a projection of A onto a subset of its simple direct factors. The general case follows from this and the fact that $A^\times$ is the inverse image of $(A/J(A))^\times$ by 4.19. This proves (i). If i is a primitive idempotent in A such that $f(i) \neq 0$, then iAi is a local algebra, hence $f(iAi) = f(i)Bf(i)$ is a local algebra by 6.6, and thus $f(i)$ is primitive in B, whence (ii). Let I be a primitive decomposition of 1_A in A. It follows from (i) that $f(I) - \{0\}$ is a primitive decomposition of 1_B in B. Thus $B = \oplus_{i \in I, f(i) \neq 0} Bf(i)$ as a left B-module. If j is a primitive idempotent in B, then Bj is an indecomposable direct summand of B, and hence $Bj \cong Bf(i)$ for some $i \in I$ by the Krull-Schmidt theorem 6.1. Therefore, by 6.14, there is $v \in B^\times$ such that $vjv^{-1} = f(i)$. By (i) there is $u \in A^\times$ such that $f(u) = v$, and then $u^{-1}iu$ is a primitive idempotent in A whose image under f in B is j. This shows (iii). Let i, i' be primitive idempotents in A not contained in $\ker(f)$ such that $f(i)$, $f(i')$ are conjugate in B. Since f is surjective, f induces a surjective map $Ai \to Bf(i)$. Since f maps $J(A)$ to $J(B)$ this induces a surjective map $Ai/J(A)i \to Bf(i)/J(B)f(i)$. Since $Ai/J(A)i$ is simple, this map is in fact an isomorphism (of A-modules, where we view any B-module as A-module with $a \in A$ acting as $f(a)$). Thus $Ai/J(A)i \cong Bf(i)/J(B)f(i) \cong Bf(i')/J(B)f(i') \cong Ai'/J(A)i'$, hence $Ai \cong Ai'$ by 6.13, and so i, i' are conjugate by 6.14, which completes the proof. $\square$

Corollary 6.19. *Let A be a finite-dimensional k-algebra. The canonical algebra homomorphism $A \to A/J(A)$ induces a bijection between the conjugacy classes of primitive idempotents in A and in $A/J(A)$.*

Proof. Since $J(A)$ is nilpotent, it contains no idempotent, and hence 6.19 is the special case of 6.18 applied with $A/J(A)$ instead of B and the canonical algebra homomorphism $A \to A/J(A)$ instead of f. $\square$

Occasionally, the following refinement of the lifting theorem is useful.

Theorem 6.20. *Let A, B be finite-dimensional k-algebras, let I be an ideal in A, let J be an ideal in B, and let $f : A \to B$ be an algebra homomorphism such that $f(I) = J$.*

(i) For any primitive idempotent i in A contained in I either $i \in ker(f)$ or $f(i)$ is a primitive idempotent in B contained in J.

(ii) For any primitive idempotent j in B contained in J there is a primitive idempotent i in A contained in I such that $f(i) = j$.

(iii) Any two primitive idempotents i, i' in A contained in I but not contained in $ker(f)$ are conjugate in A if and only if $f(i)$, $f(i')$ are conjugate in B.

Proof. One plays this back to the situation of 6.18 by replacing B by the image $f(A)$. An idempotent j in J which is primitive in $f(A)$ remains primitive in B; indeed, if $j = j_1 + j_2$ with orthogonal idempotents j_1, j_2 which commute with j, then $j_1 = jj_1 \in J$ and similarly $j_2 \in J$, contradicting the fact that j is primitive in $f(A)$. All parts of this corollary follow from the corresponding statements in 6.18 applied to $f(A)$ instead of B. $\square$

Exercises 6.21. Let A be a finite-dimensional k-algebra.

(1) Let U, V, W be finite-dimensional A-modules. Show that if $U \oplus V \cong U \oplus W$, then $V \cong W$.

(2) Let U, V, W be finite-dimensional A-modules. Suppose that W is indecomposable, and that W is isomorphic to a direct summand of $U \oplus V$. Show that W is isomorphic to a direct summand of U or of V.

(3) Let U be a finite-dimensional A-module. Let ι, κ be idempotents in $\mathrm{End}_A(U)$. Show that there is an isomorphism of A-modules $\iota(U) \cong \kappa(U)$ if and only if the idempotents ι, κ are conjugate in $\mathrm{End}_A(U)$.

(4) Let e, f be idempotents in A. Show that there is an element $u \in A^\times$ such that e and ufu^{-1} commute.

(5) Let B be a subalgebra of A such that $A = B + J(A)$. Show that every primitive idempotent i in B is primitive in A, and that two primitive idempotents i, j in B are conjugate in B if and only if they are conjugate in A.

(6) Let e be an idempotent in A, and i, j primitive indempotents in eAe. Show that i, j remain primitive in A, and that i, j are conjugate in eAe if and only if i, j are conjugate in A.

(7) Show that if I is an ideal in A which is not contained in $J(A)$, then I contains an idempotent.

(8) Let I be an ideal in A. Show that there exists a positive integer n such that $(I + J(A))^n \subseteq I$.

(9) Let I be a nonzero ideal in A. Show that we have $I^2 = I$ if and only if $I = AeA$ for some idempotent e in A. *Hint:* show this first for $A/J(A)$, using Wedderburn's theorem, and then in general using the previous exercise.

(10) Suppose that k is algebraically closed. Let S be a simple A-module and i a primitive idempotent such that $iS \neq \{0\}$. Show that $\dim_k(iS) = 1$. *Hint:* Use the fact that iS is a simple iAi-module.

(11) Show that the polynomial algebra in two variables $k[x, y]$ has a unique idempotent but is not local. (This illustrates the fact that 6.4 does not hold in general for infinite-dimensional algebras.)

7 Projective and injective modules

Definition 7.1. Let A be a k-algebra and F and A-mdoule. A subset X of F is called a *basis of* F, if every element in F can be written uniquely in the form $\sum_{x \in X} a_x x$ with elements $a_x \in A$ of which only finitely many are nonzero. An A-module F is called *free* if it has a basis. The module F is called *free of finite rank* n for some positive integer n, if F has a finite basis consisting of n elements.

If F is a free A-module and X a basis of F, then $F = \oplus_{x \in X} Ax$, and $Ax \cong A$ as a left module, for each $x \in A$. In other words, an A-module F is free if and only if F is isomorphic to a direct sum of (possibly infinitely many) copies of A. If F has a finite basis consisting of n elements, then any basis of F has n elements, and hence the notion of rank is well-defined. This follows, for instance, from the Krull-Schmidt theorem, but can also be seen easily directly, by writing the basis elements of one basis as linear combinations of another basis. Using standard techniques from linear algebra one observes that the resulting matrices are invertible. An A-module F is free of finite rank n if and only if $F \cong A^n$. Direct summands of free modules need not be free.

Definition 7.2. Let A be a k-algebra. An A-module P is called *projective* if P is a direct summand of a free A-module; that is, if there is an A-module P' such that $P \oplus P'$ is free.

Example 7.3. Let A be a k-algebra and let i be an idempotent in A. Then the left A-module Ai is projective. More precisely, we have $A = Ai \oplus A(1-i)$ as left A-modules, and Ai is projective indecomposable if and only if the idempotent i is primitive. We will show that if A is finite-dimensional, then every finite-dimensional projective indecomposable A-module is isomorphic to Ai for some primitive idempotent i in A.

Theorem 7.4. *Let A be a k-algebra, and let P be an A-module. The following are equivalent:*

(i) The A-module P is projective.

(ii) Any surjective A-homomorphism $\pi : U \to P$ from some A-module U to P splits; that is, there is an A-homomorphism $\sigma : P \to U$ such that $\pi \circ \sigma = \mathrm{Id}_P$.

(iii) For any surjective A-homomorphism $\pi : U \to V$ and any A-homomorphism $\psi : P \to V$ there exists an A-homomorphism $\varphi : P \to U$ such that $\pi \circ \varphi = \psi$.

Proof. Suppose that P is projective. Let $\pi : U \to V$ be a surjective A-homomorphism, and let $\psi : P \to V$ be an A-homomorphism. Let P' be an A-module such that $P \oplus P'$ is free and let S be a basis of $P \oplus P'$. Extend ψ to an A-homomorphism $P \oplus P' \to V$ in any which way (for instance, by sending P' to zero), still denoted by ψ. For $s \in S$ choose any element $u_s \in U$ such that $\pi(u_s) = \psi(s)$. Since $P \oplus P'$ is free with basis S there is a unique A-homomorphism $\varphi : P \oplus P' \to U$ such that $\varphi(s) = u_s$ for all $s \in S$. Thus $\pi \circ \varphi = \psi$ on $P \oplus P'$. Restricting φ to P yields the required lift of ψ on P. This shows that (i) implies (iii). Suppose that (iii) holds. Let $\pi : U \to P$ be a surjective A-homomorphism. Applying (iii) to π and to Id_P instead of ψ yields an A-homomorphism $\sigma : P \to U$ satisfying $\pi \circ \sigma = \mathrm{Id}_P$. Thus (iii) implies (ii). Suppose finally that (ii) holds. Let S be any generating set of P as A-module. Let F be the free A-module with basis S. Let $\pi : F \to P$ be the unique A-homomorphism sending s (viewed as basis element of F) to s (viewed as element in P). Since S generates P the map π is surjective. Applying (ii) yields a map $\sigma : P \to F$ satisfying $\pi \circ \sigma = \mathrm{Id}_P$, and hence P is isomorphic to a direct summand of the free module F. Thus (ii) implies (i). $\square$

The third characterisation in the above theorem states that homomorphisms from a projective module can be 'lifted' through surjective homomorphisms. This characterisation extends to objects in arbitrary categories, with surjective homomorphisms replaced by epimorphisms. Moreover, this characterisation has an interpretation in terms of functors. A functor from $\mathrm{Mod}(A)$ to $\mathrm{Mod}(k)$ is *exact* if it sends any exact sequence of A-modules to an exact sequence of k-modules. Given any A-homomorphism $\pi : U \to V$, composition with π induces a map $\mathrm{Hom}_A(P, U) \to \mathrm{Hom}_A(P, V)$ sending $\varphi \in \mathrm{Hom}_A(P, U)$ to $\pi \circ \varphi$. In this way, $\mathrm{Hom}_A(P, -)$ becomes a covariant functor from $\mathrm{Mod}(A)$ to $\mathrm{Mod}(k)$. Statement (iii) in 7.4 says that a projective module P is characterised by the property that if π is surjective then so is the induced map $\mathrm{Hom}_A(P, U) \to \mathrm{Hom}_A(P, V)$. Using this, one easily checks the following statement:

Theorem 7.5. *Let A be a k-algebra, and let P be an A-module. Then P is projective if and only if the functor $\mathrm{Hom}_A(P, -) : \mathrm{Mod}(A) \to \mathrm{Mod}(k)$ is exact.*

Before going further we mention the dual concept of injective modules.

Definition 7.6. Let A be a k-algebra. An A-module I is called *injective* if for every injective A-homomorphism $\iota : U \to V$ and any A-homomorphism $\psi : U \to I$ there exists an A-homomorphism $\varphi : V \to I$ such that $\varphi \circ \iota = \psi$.

Thus any homomorphism to an injective A-module 'extends' through any injective A-homomorphism. As before, this notion makes sense in an arbitrary category, with injective homomorphisms replaced by monomorphisms. Dualising the corresponding proofs for projective modules yields immediately the following statements for injective modules:

Theorem 7.7. *Let A be a k-algebra and let I be an A-module. The following are equivalent:*

(i) The A-module I is injective.

(ii) Any injective A-homomorphism $\iota : I \to V$ from I to some A-module V splits; that is, there is an A-homomorphism $\kappa : V \to I$ such that $\kappa \circ \iota = \mathrm{Id}_I$.

(iii) The contravariant functor $\mathrm{Hom}_A(-, I) : \mathrm{Mod}(A) \to \mathrm{Mod}(k)$ is exact.

Projective and injective modules can be used to give the followign characterisation of semisimple algebras.

Proposition 7.8. *Let A be a finite-dimensional algebra over a field. The following are equivalent.*

(i) We have $J(A) = \{0\}$.

(ii) Every finite-dimensional A-module is semisimple.

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

(iv) Every finite-dimensional A-module is injective.

(v) Every simple A-module is projective.

(vi) Every simple A-module is injective.

Proof. The equivalence of (i) and (ii) has been proved in 5.5. Let U, V be finite-dimensional A-modules. Suppose (ii) holds. Let $\pi : U \to V$ be a surjective A-homomorphism. Since U is semi-simple, $\ker(\pi)$ has a complement U' in U, which shows that π is split surjective. Thus V is projective. This shows that (ii) implies (iii), and a similar argument applied to the image of an injective homomorphism shows that (ii) implies (iv). The implications (iii) $\Rightarrow$ (v) and (iv) $\Rightarrow$ (vi) are trivial. Suppose that (v) holds. Let U be an A-module, and M a maximal submodule. Then U/M is simple, hence projective, and thus the canonical map $U \to U/M$ splits. It follows that $U \cong M \oplus U/M$. Arguing by induction over $\dim_k(U)$ we get that any finite-dimensional A-module is semisimple. Thus (v) implies (ii). A similar argument, using simple submodules of U, shows that (vi) implies (ii). □

Theorem 7.9. *Let A be a finite-dimensional k-algebra. The maps*

$$i \mapsto Ai \mapsto Ai/J(A)i$$

with i running over the primitive idempotents in A induce bijections between the sets of conjugacy classes of primitive idempotents in A, the isomorphism classes of projective indecomposable A-modules, and the isomorphism classes of simple A-modules.

Proof. This is a restatement of earlier results. Let P be a finite-dimensional projective indecomposable A-module. Then P is a direct summand of A^n for some positive integer. The Krull-Schmidt theorem implies that P is an indecomposable direct summand of A. Thus $P \cong Ai$ for some primitive idmpotent i in A. By 6.14, two primitive idempotents i, j are conjugate if and only if $Ai \cong Aj$. This shows that the map $i \mapsto Ai$ induces a bijection between conjugacy classes of primitive idempotents in A and isomorphism classes of projective indecomposable A-mdoules. The rest follows from 6.16. $\square$

A Appendix: Category theory

Category theory considers mathematical objects systematically together with the structure preserving maps between them. A category $\mathcal{C}$ consists of three types of data: an *object class*, a *morphism class*, and a partial binary map on $\mathrm{Hom}_{\mathcal{C}}$, called the *composition map*, satisfying a short list of properties one would expect any reasonable category of mathematical objects to have.

Definition A.1. A category $\mathcal{C}$ consists of a class $\mathrm{Ob}(\mathcal{C})$, called the *class of objects of* $\mathcal{C}$, for any X, $Y \in \mathrm{Ob}(\mathcal{C})$ a class $\mathrm{Hom}_{\mathcal{C}}(X,Y)$, called the *class of morphisms from* X *to* Y *in* $\mathcal{C}$, and, for any X, Y, $Z \in \mathcal{C}$ a map

$$\mathrm{Hom}_{\mathcal{C}}(X,Y) \times \mathrm{Hom}_{\mathcal{C}}(Y,Z) \to \mathrm{Hom}_{\mathcal{C}}(X,Z), \quad (f,g) \mapsto g \circ f \ ,$$

called the *composition map*, subject to the following properties.

(1) The classes $\mathrm{Hom}_{\mathcal{C}}(X,Y)$, with X, $Y \in \mathcal{C}$, are pairwise disjoint. Equivalently, any morphism f in $\mathcal{C}$ determines uniquely a pair (X,Y) of objects in $\mathcal{C}$ such that $f \in \mathrm{Hom}_{\mathcal{C}}(X,Y)$.

(2) (Identity morphisms) For any object $X \in \mathrm{Ob}(\mathcal{C})$, there is a distinghuished morphism $\mathrm{Id}_X \in \mathrm{Hom}_{\mathcal{C}}(X,X)$, called *identity morphism of* X, such that for any object $Y \in \mathcal{C}$, any $f \in \mathrm{Hom}_{\mathcal{C}}(X,Y)$ and any $g \in \mathrm{Hom}_{\mathcal{C}}(Y,X)$ we have $f \circ \mathrm{Id}_X = f$ and $\mathrm{Id}_X \circ g = g$.

(3) (Associativity) For any X, Y, Z, $W \in \mathrm{Ob}(\mathcal{C})$ and any $f \in \mathrm{Hom}_{\mathcal{C}}(X,Y)$, $g \in \mathrm{Hom}_{\mathcal{C}}(Y,Z)$, $h \in \mathrm{Hom}_{\mathcal{C}}(Z,W)$, we have $(h \circ g) \circ f = h \circ (g \circ f)$; this is an equality of morphisms in $\mathrm{Hom}_{\mathcal{C}}(X,W)$.

It is easy to verify that the identity morphisms are unique. A morphism $f \in \mathrm{Hom}_{\mathcal{C}}(X,Y)$ is typically denoted by $f : X \to Y$ or by $X \xrightarrow{f} Y$. Morphisms are also called *maps*, although one should note that the morphisms of a category may be abstractly defined and do not necessarily induce any maps in a set theoretic sense. We write $\mathrm{End}_{\mathcal{C}}(X) = \mathrm{Hom}_{\mathcal{C}}(X,X)$, and call the morphisms in $\mathrm{End}_{\mathcal{C}}(X)$ the *endomorphisms of* X. The set $\mathrm{End}_{\mathcal{C}}(X)$ together with the composition of morphisms is a monoid with unit element Id_X. A morphism $f : X \to Y$ in $\mathcal{C}$ is called an *isomorphism* if there exists a morphism $g : Y \to X$ such that $g \circ f = \mathrm{Id}_X$ and $f \circ g = \mathrm{Id}_Y$. In that case g is an isomorphism as well. The identity morphisms are isomorphisms, and the composition of any two isomorphisms is an isomorphism. An isomorphism which is an endomorphism of an object X is called an *automorphism* of X. The automorphisms of X form a subgroup of the monoid $\mathrm{End}_{\mathcal{C}}(X)$.

The objects of a category form in general a *class*, not necessarily a set. A category whose object and morphism classes are sets is called a *small category*. For the purpose of this course, we ignore set theoretic issues; since we will be dealing mostly with module categories, this will not cause any problems.

Definition A.2. Let $\mathcal{C}$ be a category. The *opposite category* $\mathcal{C}^{\mathrm{op}}$ of $\mathcal{C}$ is defined by $\mathrm{Ob}(\mathcal{C}^{\mathrm{op}}) = \mathrm{Ob}(\mathcal{C})$ and $\mathrm{Hom}_{\mathcal{C}^{\mathrm{op}}}(X,Y) = \mathrm{Hom}_{\mathcal{C}}(Y,X)$ for all X, $Y \in \mathrm{Ob}(\mathcal{C}^{\mathrm{op}}) = \mathrm{Ob}(\mathcal{C})$, with composition $g \bullet f$ in $\mathcal{C}^{\mathrm{op}}$ defined by $g \bullet f = f \circ g$, for any X, Y, $Z \in \mathrm{Ob}(\mathcal{C}^{\mathrm{op}})$, $f \in \mathrm{Hom}_{\mathcal{C}^{\mathrm{op}}}(X,Y) = \mathrm{Hom}_{\mathcal{C}}(Y,X)$ and $g \in \mathrm{Hom}_{\mathcal{C}^{\mathrm{op}}}(Y,Z) = \mathrm{Hom}_{\mathcal{C}}(Z,Y)$, and where $f \circ g$ is the composition in $\mathcal{C}$.

Definition A.3. Let $\mathcal{C}$ and $\mathcal{D}$ be categories. We say that $\mathcal{D}$ is a *subcategory* of $\mathcal{C}$ if $\mathrm{Ob}(\mathcal{D})$ is a subclass of $\mathrm{Ob}(\mathcal{C})$, and if for any X, Y in $\mathrm{Ob}(\mathcal{D})$, the class $\mathrm{Hom}_{\mathcal{D}}(X,Y)$ is a subclass of $\mathrm{Hom}_{\mathcal{C}}(X,Y)$, such that for any X, Y, $Z \in \mathrm{Ob}(\mathcal{D})$, the composition map $\mathrm{Hom}_{\mathcal{D}}(X,Y) \times \mathrm{Hom}_{\mathcal{D}}(Y,Z) \to \mathrm{Hom}_{\mathcal{D}}(X,Z)$ in $\mathcal{D}$ is the restriction of the composition map in $\mathcal{C}$. We say that the subcategory $\mathcal{D}$ of $\mathcal{C}$ is a *full subcategory*, if for any X, $Y \in \mathrm{Ob}(\mathcal{D})$ we have $\mathrm{Hom}_{\mathcal{D}}(X,Y) = \mathrm{Hom}_{\mathcal{C}}(X,Y)$.

Definition A.4. Let $\mathcal{C}$ be a category. An object E is *initial* if for every object Y in $\mathcal{C}$ there is a unique morphism $E \to Y$ in $\mathcal{C}$. An object T is *terminal* if for every object Y in $\mathcal{C}$ there is a unique morphism $Y \to T$ in $\mathcal{C}$. A *zero object* is an object which is both initial and terminal. If O is a zero object in $\mathcal{C}$ and $f : X \to Y$ a morphism in $\mathcal{C}$ such that $f = h \circ g$, where $g : X \to O$ and $h : O \to Y$ are the unique morphisms, then f is called a *zero morphism* in $\mathrm{Hom}_{\mathcal{C}}(X, Y)$.

The identity morphism of an initial or terminal object is its only endomorphism, and there is exactly one morphism between any two initial or terminal objects, and hence any such morphism is an isomorphism. Thus if a category has an initial or terminal or zero object, such an object is unique up to unique isomorphism. As a consequence, if $\mathcal{C}$ has a zero object, then for any two objects X, Y in $\mathcal{C}$ there is exactly one zero morphism in $\mathrm{Hom}_{\mathcal{C}}(X, Y)$. Composing the zero morphism with any other morphism yields again the zero morphism.

Examples A.5.

(1) We denote by **Sets** the category of sets, having as objects the class of sets and as morphisms arbitrary maps between sets. This is a large category - considering the set of all sets leads to what is known as *Russell's paradox.* The distinction between sets and classes is one way around this problem.

(2) Let k be a field. We denote by $\mathbf{Vect}(k)$ the category of k-vector spaces; that is, the objects of $\mathbf{Vect}(k)$ are the k-vector spaces, and the morphisms are k-linear maps between k-vector spaces. We denote by $\mathbf{vect}(k)$ the full subcategory of $\mathbf{Vect}(k)$ consisting of all finite-dimensional k-vector spaces.

(3) We denote by **Grps** the category of groups, with groups as objects and group homomorphisms as morphisms. We denote by **grps** the category of finite groups, as before, with group homomorphisms as morphisms. The category **grps** is a full subcategory of **Grps**.

(4) We denote by **Top** the category of topological spaces, with linear maps as morphisms.

(5) If $\mathcal{C}$ is a small category with a single object E, then $\mathrm{Hom}_{\mathcal{C}}(E, E)$ is a monoid. Conversely, if M is a monoid, we can consider M as a the morphism set of a category $\mathbf{M}$ with a single object $*$, such that the morphism set in $\mathbf{M}$ from $*$ to $*$ is equal to M, and such that composition of morphisms in $\mathbf{M}$ is equal to the product in M.

(6) We denote by $\mathbf{Alg}(k)$ the category of k-algebras, with algebra homomorphisms as morphisms.

(7) For A an algebra over a commutative ring k, we denote by $\mathrm{Mod}(A)$ the category of left A-modules, and by $\mathrm{mod}(A)$ the category of finitely generated left A-modules, with A-homomorphisms between modules as morphisms. The category $\mathrm{mod}(A)$ is a full subcategory of $\mathrm{Mod}(A)$.

Since morphisms in a category need not be maps between sets, one of the challenges is to extend standard notions such as the property of being injective or surjective without referring to elements in objects. The category theoretic version of surjective and injective maps are as follows.

Definition A.6. Let $\mathcal{C}$ be a category, and let $f : X \to Y$ be a morphism in $\mathcal{C}$. The morphism f is called an *epimorphism* if for any two morphisms g, g' from Y to any other object Z satisfying $g \circ f = g' \circ f$ we have $g = g'$. The morphism f is called a *monomorphism* if for any two morphisms g, g' from any other object Z to X satisfying $f \circ g = f \circ g'$ we have $g = g'$.

Thus a morphism in a category $\mathcal{C}$ is an epimorphism if and only if it is a monomorphism when viewed as a morphism in $\mathcal{C}^{\mathrm{op}}$. In the category of sets or the category of modules over an algebra, the monomorphisms are the injective maps, and the epimorphisms are the surjective maps. Any isomorphism in $\mathcal{C}$ is both an epimorphism and a monomorphism, but the converse need not be true. The composition of two epimorphisms or monomorphisms is again an epimophism or monomorphism, respectively.

Definition A.7. Let $f : X \to Y$ be a morphism in a category $\mathcal{C}$ with a zero object. A *kernel of* f is a pair consisting of an object in $\mathcal{C}$, denoted $\ker(f)$, and a morphism $i : \ker(f) \to X$, such that $f \circ i = 0$ and such that for any object Z and any morphism $g : Z \to X$ satisfying $f \circ g = 0$ there is a unique morphism $h : Z \to \ker(f)$ satisfying $g = i \circ h$. Dually, a *cokernel of* f is a pair consisting of an object in $\mathcal{C}$, denoted $\mathrm{coker}(f)$, and a morphism $p : Y \to \mathrm{coker}(f)$, such that $p \circ f = 0$ and such that for any object Z and any morphism $g : Y \to Z$ satisfying $g \circ f = 0$ there is a unique morphism $h : \mathrm{coker}(f) \to Z$ satisfying $g = h \circ p$.

The uniqueness properties in this definition imply that i is a monomorphism, p is an epimorphism, and the pairs $(\ker(f), i)$ and $(\mathrm{coker}(f), p)$, if they exist, are unique up to unique isomorphism. A kernel becomes a cokernel in the opposite category, and vice versa. We use the definition of epimorphisms and monomorphisms to extend the notion of projective and injective modules to arbitrary categories.

Definition A.8. Let $\mathcal{C}$ be a category. An object P in $\mathcal{C}$ is called *projective* if for any epimorphism $h : X \to Y$ and any morphism $f : P \to Y$ there is a morphism $g : P \to X$ such that $h \circ g = f$. An object I in $\mathcal{C}$ is called *injective* if for any monomorphism $i : X \to Y$ and any morphism $f : X \to I$ there is a morphism $g : Y \to I$ such that $g \circ i = f$.

Thus P is projective in $\mathcal{C}$ if and only if P is injective in $\mathcal{C}^{\mathrm{op}}$.

Definition A.9. Let $\mathcal{C}$ be a category, and let $\{X_j\}_{j\in I}$ be a familiy of objects in $\mathcal{C}$, where I is an indexing set. A *product of the family of objects* $\{X_j\}_{j\in I}$ is an object in $\mathcal{C}$, denoted $\prod_{j\in I} X_j$, together with a family of morphisms $\pi_i : \prod_{j\in I} X_j \to X_i$ for each $i \in I$, satisfying the following universal property: for any object Y in $\mathcal{C}$ and any family of morphisms $\varphi_i : Y \to X_i$, with $i \in I$, there is a unique morphism $\alpha : Y \to \prod_{j\in I} X_j$ satisfying $\varphi_i = \pi_i \circ \alpha$ for all $i \in I$.

The uniqueness of α implies that the product, if it exists at all, is uniquely determined up to unique isomorphism. By reversing the direction of morphisms, one obtains coproducts or direct sums.

Definition A.10. Let $\mathcal{C}$ be a category, and let $\{X_j\}_{j\in I}$ be a familiy of objects in $\mathcal{C}$, where I is an indexing set. A *coproduct or direct sum of the family of objects* $\{X_j\}_{j\in I}$ is an object in $\mathcal{C}$, denoted $\coprod_{j\in I} X_j$, together with a family of morphisms $\iota_i : X_i \to \coprod_{j\in I} X_j$ for each $i \in I$, satisfying the following universal property: for any object Y in $\mathcal{C}$ and any family of morphisms $\varphi_i : X_i \to Y$, with $i \in I$, there is a unique morphism $\alpha : \coprod_{j\in I} X_j \to Y$ satisfying $\varphi_i = \alpha \circ \iota_i$ for all $i \in I$.

Definition A.11. A category $\mathcal{C}$ with a zero object is called *additive* if the morphism classes $\mathrm{Hom}_{\mathcal{C}}(X, Y)$ are abelian groups, such that the composition of morphisms is biadditive, and such that coproducts of finite families of objects exist. A category $\mathcal{C}$ with a zero object is called *k-linear* if the morphism classes $\mathrm{Hom}_{\mathcal{C}}(X, Y)$ are k-vector spaces, such that the composition of morphisms is bilinear, and such that coproducts of finite families of objects exist.

Remark A.12. In an additive or k-linear category we also have products of finite families, and products and coproducts of finite families of objects are isomorphic. To see this, let I be a finite indexing set and let $\{X_i\}_{i\in I}$ be a finite family of objects in an additive category $\mathcal{C}$. In order to simplify notation, we write $\coprod$ instead of $\coprod_{j\in I}$. We need to construct morphisms $\coprod X_j \to X_i$ for any $i \in I$ satisfying the universal property as in the definition of the product of the X_i. Let $i \in I$. For $j \in I$, denote by $\varphi : X_i \to X_j$ the morphism Id_{X_i} if $i = j$, and the zero morphism if $i \neq j$. The universal property of the coproduct yields a unique morphism $\pi_i : X_i \to \coprod X_j$ with the property $\pi_i \circ \iota_i = \mathrm{Id}_{X_i}$ and $\pi_j \circ \iota_i = 0$, where $i, j \in I$, $i \neq j$. To see that $\coprod X_j$, together with the morphisms $\pi_i : \coprod X_j \to X_i$, is a product, we consider a family of morphisms $\psi_i : Y \to X_i$, for $i \in I$, where Y is some object in $\mathcal{C}$. Then $\alpha = \sum_{j\in I} \iota_j \circ \psi_j$ is a morphism from $Y \to \coprod X_j$; this is well-defined since I is finite. Thus $\pi_i \circ \alpha = \sum_{j\in I} \pi_i \circ \iota_j \circ \psi_j = \psi_i$ for all $i \in I$. To see the uniqueness of α with this property, note first that the endomorphism $\gamma = \sum_{j\in I} \iota_j \circ \pi_j$ of $\coprod X_j$ satisfies $\gamma \circ \iota_i = \iota_i$ for all $i \in I$. But the identity morphism of $\coprod X_j$ is the unique endomorphism with this propery, where we use the universal property of coproducts. Thus γ is equal to the identity on $\coprod X_j$. Therefore, if $\beta : Y \to \coprod X_j$ is any other morphism satisfying $\pi_i \circ \beta = \psi_i$ for all $i \in I$, then $\beta = \sum_{j\in I} \iota_j \circ \pi_j \circ \beta = \sum_{j\in J} \iota_j \circ \psi_j = \alpha$, which shows the uniqueness of α. This proves that $\coprod X_j$, together with the family of morphisms $\pi_i : \coprod X_j \to X_i$, with $i \in I$, is indeed product of the family $\{X_i\}_{i\in I}$.

Module categories are additive, but they have more structure: all morphisms have kernels and cokernels, and there are isomorphism theorems relating kernels and images. Consider a k-algebra A and a homomorphism of A-mdoules $\varphi : U \to V$. Then $U/\ker(\varphi)$ is obtained by first taking the kernel $\ker(\varphi)$ and then taking the cokernel of the inclusion $\ker(\varphi) \subseteq U$. The image $\mathrm{Im}(\varphi)$ is obtained by first taking the cokernel $V \to \mathrm{coker}(\varphi) = V/\mathrm{Im}(\varphi)$, and then $\mathrm{Im}(\varphi)$ is the kernel of the map $V \to \mathrm{coker}(\varphi)$. The isomorphism theorem $U/\ker(\varphi) \cong \mathrm{Im}(\varphi)$ amounts therefore to stating that taking kernels and cokernels 'commute' in a canonical way. These considerations can be extended to additive categories. If $\mathcal{C}$ is an additive category, then for any morphism $f : X \to Y$ in $\mathcal{C}$ which has a kernel $i : \ker(f) \to X$ and a cokernel $p : Y \to \mathrm{coker}(f)$ there is a canonical morphism $\mathrm{coker}(i) \to \ker(p)$. This morphism is constructed as follows. Taking the cokernel of i yields an epimorphism $q : X \to \mathrm{coker}(i)$, and taking the kernel of p yields a monomorphism $j : \ker(p) \to Y$. Since $f \circ i = 0$, the definition of $\mathrm{coker}(i)$ yields a uniqe morphism $h : \mathrm{coker}(i) \to Y$ such that $h \circ q = f$. Then $0 = p \circ f = p \circ h \circ q$. Since q is an epimorphism, this implies that $p \circ h = 0$. Then the definition of $\ker(p)$ yields a unique morphism $m : \mathrm{coker}(i) \to \ker(p)$ satisfying $j \circ m = h$.

$$
\begin{tikzcd}
\ker(f) \arrow[r, "i"] & X \arrow[r, "f"] \arrow[d, "q"'] & Y \arrow[r, "p"] & \mathrm{coker}(f) \\
& \mathrm{coker}(i) \arrow[r, "m"'] \arrow[ur, "h"] & \ker(p) \arrow[u, "j"'] &
\end{tikzcd}
$$

Definition A.13. An additive category $\mathcal{C}$ is called an *abelian category* if for every morphism $f : X \to Y$ there exists a kernel $i : \ker(f) \to X$ and a cokernel $p : Y \to \mathrm{coker}(f)$, and if the canonical morphism $\mathrm{coker}(i) \to \ker(p)$ is an isomorphism.

Every module category of a ring is an abelian category. Other examples of abelian categories include categories of sheaves on topological spaces. The Freyd-Mitchell embedding theorem states that every small abelian category is equivalent to a full subcategory of a module category of some ring A. (For the precise definition of equivalent categories see A.19 below.) The notion of exactness can be generalised as follows. A sequence of two composable A-homomorphisms in the category of A-modules

$$U \xrightarrow{\varphi} V \xrightarrow{\psi} W$$

is *exact* if $\mathrm{Im}(\varphi) = \ker(\psi)$. With the technique from above, describing $\mathrm{Im}(\varphi)$ as the kernel of a cokernel of φ, consider a sequence of morphisms

$$X \xrightarrow{\quad f \quad} Y \xrightarrow{\quad g \quad} Z$$

in an abelian category $\mathcal{C}$, such that $g \circ f = 0$. Let $p : Y \to \mathrm{coker}(f)$ be a cokernel of f. Since $g \circ f = 0$, there is a unique morphism $h : \mathrm{coker}(f) \to Z$ such that $h \circ p = g$. Let $j : \ker(p) \to Y$ be a kernel of p. Thus $p \circ j = 0$, hence $g \circ j = h \circ p \circ j = 0$. Let $m : \ker(g) \to Y$ be a kernel of g. Thus there is a unique morphism $n : \ker(p) \to \ker(q)$ satisfying $j = m \circ n$. We say that the above sequence is *exact* if n is an isomorphism in $\mathcal{C}$.

$$\begin{tikzcd}
 & \ker(p) \arrow[rr, "n"] \arrow[dr, "j"'] & & \ker(g) \arrow[dl, "m"] & \\
X \arrow[rr, "f"'] & & Y \arrow[rr, "g"] \arrow[dr, "p"'] & & Z \\
 & & & \mathrm{coker}(f) \arrow[ur, "h"'] &
\end{tikzcd}$$

The philosophy of considering any mathematical object together with its structure preserving maps applies to categories as well. Functors are 'morphisms' between categories.

Definition A.14. Let $\mathcal{C}$, $\mathcal{D}$ be categories. A *functor* or *covariant functor* $\mathcal{F}$ *from* $\mathcal{C}$ *to* $\mathcal{D}$ is a map $\mathcal{F} : \mathrm{Ob}(\mathcal{C}) \to \mathrm{Ob}(\mathcal{D})$ together with a family of maps, abusively all denoted by the same letter $\mathcal{F}$, from $\mathrm{Hom}_{\mathcal{C}}(X, Y)$ to $\mathrm{Hom}_{\mathcal{D}}(\mathcal{F}(X), \mathcal{F}(Y))$ for all X, $Y \in \mathrm{Ob}(\mathcal{C})$, with the following properties.

(a) For all objects X in $\mathrm{Ob}(\mathcal{C})$ we have $\mathcal{F}(\mathrm{Id}_X) = \mathrm{Id}_{\mathcal{F}(X)}$.

(b) For all objects X, Y, Z in $\mathrm{Ob}(\mathcal{C})$ and morphisms $\varphi : X \to Y$ and $\psi : Y \to Z$ we have

$$\mathcal{F}(\psi \circ \varphi) = \mathcal{F}(\psi) \circ \mathcal{F}(\varphi) \ .$$

Similarly, a *contravariant functor from* $\mathcal{C}$ *to* $\mathcal{D}$ is map $\mathcal{F} : \mathrm{Ob}(\mathcal{C}) \to \mathrm{Ob}(\mathcal{D})$ together with a family of maps $\mathcal{F} : \mathrm{Hom}_{\mathcal{C}}(X, Y) \to \mathrm{Hom}_{\mathcal{D}}(\mathcal{F}(Y), \mathcal{F}(X))$ for all X, $Y \in \mathrm{Ob}(\mathcal{C})$, with the following properties.

(c) For all objects X in $\mathrm{Ob}(\mathcal{C})$ we have $\mathcal{F}(\mathrm{Id}_X) = \mathrm{Id}_{\mathcal{F}(X)}$.

(d) For all objects X, Y, Z in $\mathrm{Ob}(\mathcal{C})$ and morphisms $\varphi : X \to Y$ and $\psi : Y \to Z$ we have

$$\mathcal{F}(\psi \circ \varphi) = \mathcal{F}(\varphi) \circ \mathcal{F}(\psi) \ .$$

Equivalently, a contravariant functor from $\mathcal{C}$ to $\mathcal{D}$ is a covariant functor from $\mathcal{C}^{\mathrm{op}}$ to $\mathcal{D}$.

Functors can be composed in the obvious way, by composing the maps on objects and on morphisms. Composing a covariant functor with a contravariant functor (in either order) yields a contravariant functor. Composing two contravariant functors yields a covariant functor. On every catagory $\mathcal{C}$ there is the identity functor $\mathrm{Id}_{\mathcal{C}}$ which is the identity map on $\mathrm{Ob}(\mathcal{C})$ and the family of identity maps on the morphism sets $\mathrm{Hom}_{\mathcal{C}}(X,Y)$, X, $Y \in \mathrm{Ob}(\mathcal{C})$. Since the object classes of categories need not be sets, we cannot consider the category having all categories as objects and functors as morphisms. We can though consider the category **Cat** having as objects small categories and as morphisms all functors between small categories; that is, for two small categories $\mathcal{C}$, $\mathcal{D}$, we denote by $\mathrm{Hom}_{\mathbf{Cat}}(\mathcal{C},\mathcal{D})$ the set of functors from $\mathcal{C}$ to $\mathcal{D}$.

Examples A.15.

(1) There is a class of trivial functors, called *forgetful functors*, obtained from ignoring a part of the structure of a mathematical object. For instance, we have a forgetful functor $\mathbf{Alg}(k) \to \mathbf{Vect}(k)$ which sends a k-algebra to its underlying k-vector space (that is, we ignore the multiplication in the algebra). Every k-vector space is in particular an abelian group, so this yields a forgetful functor $\mathbf{Vect}(k) \to \mathbf{Ab}$ sending a vector space to the underlying abelian group (that is, we ignore the scalar muliplication). Every abelian group is in particular a set, so we get a forgetful functor $\mathbf{Ab} \to \mathbf{Sets}$.

(2) There is a functor from **Grps** to $\mathbf{Alg}(k)$ sending a group G to the group algebra kG and sending a group homomorphism $\varphi : G \to H$ to the algebra homomorphism $kG \to kH$ obtained by extending φ linearly. There is also a functor $\mathbf{Alg}(k) \to \mathbf{Grps}$ sending a k-algebra A to the group of invertible elements $A^\times$. To see that this is functorial, one verifies that an algebra homomorphism $\alpha : A \to B$ sends $A^\times$ to $B^\times$, hence induces a group homomorphism $A^\times \to B^\times$.

(3) There is a class of functors called *representable functors*, defined as follows. Given a small category $\mathcal{C}$ and an object X in $\mathcal{C}$, we define a functor $\mathrm{Hom}_{\mathcal{C}}(X,-)$ as follows. For any object Y in $\mathcal{C}$, the functor $\mathrm{Hom}_{\mathcal{C}}(X,-)$ sends Y to the set $\mathrm{Hom}_{\mathcal{C}}(X,Y)$. For any morphism $f : Y \to Z$ in $\mathcal{C}$ the functor $\mathrm{Hom}_{\mathcal{C}}(X,-)$ sends f to the map, denoted $\mathrm{Hom}_{\mathcal{C}}(X,f)$ which is induced by composition with f; that is, which sends $h \in \mathrm{Hom}_{\mathcal{C}}(X,Y)$ to $f \circ h \in \mathrm{Hom}_{\mathcal{C}}(X,Z)$. One easily sees that this is a functor. This construction applied to $\mathcal{C}^{\mathrm{op}}$ yields also a contravariant functor $\mathrm{Hom}_{\mathcal{C}}(-,X)$, sending Y to $\mathrm{Hom}_{\mathcal{C}}(Y,X)$ and sending f to the map denoted $\mathrm{Hom}_{\mathcal{C}}(f,X)$ induced by precomposition with f; that is, $\mathrm{Hom}_{\mathcal{C}}(f,X)$ sends $h \in \mathrm{Hom}_{\mathcal{C}}(Z,X)$ to $h \circ f \in \mathrm{Hom}_{\mathcal{C}}(Z,Y)$. Depending on what additional structures the category $\mathcal{C}$ has, the representable functors may have as target category not just the category of sets but categories with more structure. For instance, if A is a k-algebra and U an A-module, then the representable functor $\mathrm{Hom}_A(U,-)$ and its contravariant analogue $\mathrm{Hom}_A(-,U)$ are functors from $\mathrm{Mod}(A)$ to $\mathrm{Mod}(k)$.

(4) Let A, B be k-algebras, and let M be an A-B-bimodule. There is a functor $M \otimes_B -$ from $\mathrm{Mod}(B)$ to $\mathrm{Mod}(A)$ sending a B-module V to the A-module $M \otimes_B V$ and a B-homomorphism $\psi : V \to V'$ to the A-homomorphism $\mathrm{Id}_M \otimes \psi : M \otimes_B V \to M \otimes_B V'$. There is a similar functor $- \otimes_A M$ from $\mathrm{Mod}(A^{\mathrm{op}})$ to $\mathrm{Mod}(B^{\mathrm{op}})$. There is a functor $\mathrm{Hom}_A(M,-)$ from $\mathrm{Mod}(A)$ to $\mathrm{Mod}(B)$, sending an A-module U to $\mathrm{Hom}_A(M,U)$, viewed as a B-module via $(b \cdot \varphi)(m) = \varphi(mb)$, where $\varphi \in \mathrm{Hom}_A(M,U)$, $m \in M$, $b \in B$. There is a similar functor $\mathrm{Hom}_{B^{\mathrm{op}}}(M,-)$ from $\mathrm{Mod}(B^{\mathrm{op}})$ to $\mathrm{Mod}(A^{\mathrm{op}})$.

Pushing our philosophy of considering mathematical objects with their structural maps even further, we view now functors as objects and define morphisms between functors as follows.

Definition A.16. Let $\mathcal{C}$, $\mathcal{D}$ be categories, and let $\mathcal{F}$, $\mathcal{F}'$ be functors from $\mathcal{C}$ to $\mathcal{D}$. A *natural transformation from $\mathcal{F}$ to $\mathcal{F}'$* is a family $\varphi = (\varphi(X))_{X \in \mathrm{Ob}(\mathcal{C})}$ of morphisms $\varphi(X) \in \mathrm{Hom}_{\mathcal{D}}(\mathcal{F}(X), \mathcal{F}'(X))$ such that for any morphism $f : X \to Y$ in $\mathcal{C}$ we have $\mathcal{F}'(f) \circ \varphi(X) = \varphi(Y) \circ \mathcal{F}(f)$; that is, we have a commutative diagram of morphisms in the category $\mathcal{D}$ of the form

$$\begin{tikzcd}
\mathcal{F}(X) \arrow[r, "\varphi(X)"] \arrow[d, "\mathcal{F}(f)"'] & \mathcal{F}'(X) \arrow[d, "\mathcal{F}'(f)"] \\
\mathcal{F}(Y) \arrow[r, "\varphi(Y)"'] & \mathcal{F}'(Y)
\end{tikzcd}$$

By considering contravariant functors from $\mathcal{C}$ to $\mathcal{D}$ as convariant functors from $\mathcal{C}^{\mathrm{op}}$ to $\mathcal{D}$ we get an abvious notion of natural transformation between contravariant functors from $\mathcal{C}$ to $\mathcal{D}$.

Every functor $\mathcal{F} : \mathcal{C} \to \mathcal{D}$ gives rise to the *identity transformation* $\mathrm{Id}_{\mathcal{F}} : \mathcal{F} \to \mathcal{F}$ consisting of the family of identity morphisms $\mathrm{Id}_{\mathcal{F}(X)}$, $X \in \mathrm{Ob}(\mathcal{C})$. Natural transformations can be composed: if $\mathcal{F}$, $\mathcal{F}'$, $\mathcal{F}^{''}$ are functors from $\mathcal{C}$ to $\mathcal{D}$ and $\varphi : \mathcal{F} \to \mathcal{F}'$, $\psi : \mathcal{F}' \to \mathcal{F}^{''}$ are natural transformations, then the family $\psi \circ \varphi$ of morphisms $\psi(X) \circ \varphi(X) : \mathcal{F}(X) \to \mathcal{F}^{''}(X)$ is a natural transformation from $\mathcal{F}$ to $\mathcal{F}^{''}$, and this composition of natural transformations is associative. As in the case of the category of categories there are set theoretic issues if we consider the category of functors from $\mathcal{C}$ to $\mathcal{D}$ with natural transformations as morphisms. If we assume that $\mathcal{C}$ is small, then the functors from $\mathcal{C}$ to an arbitrary category $\mathcal{D}$, together with natural transformations as morphisms, form a category.

Examples A.17.

(1) Let $\mathcal{C}$ be a category, X, X' objects, and let $\varphi : X \to X'$ be a morphism in $\mathcal{C}$. Then φ induces a natural transformation from $\mathrm{Hom}_{\mathcal{C}}(X', -)$ to $\mathrm{Hom}_{\mathcal{C}}(X, -)$, given by the family of maps $\mathrm{Hom}_{\mathcal{C}}(X', Y) \to \mathrm{Hom}_{\mathcal{C}}(X, Y)$ sending $\tau \in \mathrm{Hom}_{\mathcal{C}}(X', Y)$ to $\tau \circ \varphi$, and φ induces a natural transformation from $\mathrm{Hom}_{\mathcal{C}}(-, X)$ to $\mathrm{Hom}_{\mathcal{C}}(-, X')$ sending $\tau \in \mathrm{Hom}_{\mathcal{C}}(Y, X)$ to $\varphi \circ \tau$, for all objects Y in $\mathcal{C}$.

(2) Let A, B be k-algebras and let M, M' be A-B-bimodules. Any bimodule homomorphism $\alpha : M \to M'$ induces a natural transformation from $M \otimes_B -$ to $M' \otimes_B -$ given by the family of maps $\alpha \otimes \mathrm{Id}_V : M \otimes_B V \to M' \otimes_B V$ for all B-modules V. Similarly, any such α induces a natural transformation from $\mathrm{Hom}_A(M', -)$ to $\mathrm{Hom}_A(M, -)$, as in the previous example.

Definition A.18. Let $\mathcal{C}$, $\mathcal{D}$ be categories. Two functors $\mathcal{F}$, $\mathcal{F}'$ from $\mathcal{C}$ to $\mathcal{D}$ are called *isomorphic* if there are natural transformations $\varphi : \mathcal{F} \to \mathcal{F}'$ and $\psi : \mathcal{F}' \to \mathcal{F}$ such that $\psi \circ \varphi = \mathrm{Id}_{\mathcal{F}}$ and $\varphi \circ \psi = \mathrm{Id}_{\mathcal{F}'}$.

If $\varphi : \mathcal{F} \to \mathcal{F}'$ is a natural transformation such that all morphisms $\varphi(X) : \mathcal{F}(X) \to \mathcal{F}'(X)$ are isomorphisms, then the family of morphisms $\psi(X) = \varphi(X)^{-1}$ is a natural transformation from $\mathcal{F}'$ to $\mathcal{F}$ satisfying $\psi \circ \varphi = \mathrm{Id}_{\mathcal{F}}$ and $\varphi \circ \psi = \mathrm{Id}_{\mathcal{F}'}$.

Definition A.19. Two categories $\mathcal{C}$ and $\mathcal{D}$ are called *equivalent* if there are functors $\mathcal{F} : \mathcal{C} \to \mathcal{D}$ and $\mathcal{G} : \mathcal{D} \to \mathcal{F}$ such that $\mathcal{G} \circ \mathcal{F} \cong \mathrm{Id}_{\mathcal{C}}$ and $\mathcal{F} \circ \mathcal{G} \cong \mathrm{Id}_{\mathcal{D}}$, and the functors $\mathcal{F}$, $\mathcal{G}$ arising in this way are called *equivalences of categories.*

Thus an equivalence $\mathcal{F} : \mathcal{C} \to \mathcal{D}$ need not induce a bijection between $\mathrm{Ob}(\mathcal{C})$ and $\mathrm{Ob}(\mathcal{D})$, but it induces a bijection between the isomorphism classes in $\mathrm{Ob}(\mathcal{C})$ and $\mathrm{Ob}(\mathcal{D})$.

Definition A.20. Let $\mathcal{C}$, $\mathcal{D}$ be categories and let $\mathcal{F} : \mathcal{C} \to \mathcal{D}$, $\mathcal{G} : \mathcal{D} \to \mathcal{C}$ be covariant functors. We say that $\mathcal{G}$ is *left adjoint to* $\mathcal{F}$ and that $\mathcal{F}$ is *right adjoint to* $\mathcal{G}$, if there is an isomorphism of bifunctors $\mathrm{Hom}_{\mathcal{C}}(\mathcal{G}(-), -) \cong \mathrm{Hom}_{\mathcal{D}}(-, \mathcal{F}(-))$. If $\mathcal{G}$ is left and right adjoint to $\mathcal{F}$ we say that $\mathcal{F}$ and $\mathcal{G}$ are *biadjoint*.

An isomorphism of bifunctors as in A.20 is a familiy of isomorphisms $\mathrm{Hom}_{\mathcal{C}}(\mathcal{G}(V), U) \cong \mathrm{Hom}_{\mathcal{D}}(V, \mathcal{F}(U))$, with U an object in $\mathcal{C}$ and V an object in $\mathcal{D}$, such that for fixed U we get an isomorphism of contravariant functors $\mathrm{Hom}_{\mathcal{C}}(\mathcal{G}(-), U) \cong \mathrm{Hom}_{\mathcal{D}}(-, \mathcal{F}(U))$, and for fixed V we get an isomorphism of covariant functors $\mathrm{Hom}_{\mathcal{C}}(\mathcal{G}(V), -) \cong \mathrm{Hom}_{\mathcal{D}}(V, \mathcal{F}(-))$. Such an isomorphism of bifunctors, if it exists, need not be unique. If $\mathcal{C}$, $\mathcal{D}$ are k-linear categories for some commutative ring k, we will always require such an isomorphism of bifunctors to be k-linear. Given an adjunction isomorphism $\Phi : \mathrm{Hom}_{\mathcal{C}}(\mathcal{G}(-), -) \cong \mathrm{Hom}_{\mathcal{D}}(-, \mathcal{F}(-))$, evaluating Φ at an object V in $\mathcal{D}$ and $\mathcal{G}(V)$ yields an isomorphism $\mathrm{Hom}_{\mathcal{D}}(V, \mathcal{F}(\mathcal{G}(V))) \cong \mathrm{Hom}_{\mathcal{C}}(\mathcal{G}(V), \mathcal{G}(V))$; we denote by $f(V) : V \to \mathcal{F}(\mathcal{G}(V))$ the morphism corresponding to $\mathrm{Id}_{\mathcal{G}(V)}$ through this isomorphism; that is, $f(V) = \Phi(V, \mathcal{G}(V))(\mathrm{Id}_{\mathcal{G}(V)})$. One checks that the family of morphisms $f(V)$ defined in this way is a natural transformation

$$f : \mathrm{Id}_{\mathcal{D}} \to \mathcal{F} \circ \mathcal{G}$$

called the *unit* of the adjunction isomorphism Φ. Similarly, evaluating Φ at an object U in $\mathcal{C}$ and $\mathcal{F}(U)$ we get an isomorphism $\mathrm{Hom}_{\mathcal{C}}(\mathcal{G}(\mathcal{F}(U)), U) \cong \mathrm{Hom}_{\mathcal{D}}(\mathcal{F}(U), \mathcal{F}(U))$; we denote by $g(U) : \mathcal{G}(\mathcal{F}(U)) \to U$ the morphism corresponding to $\mathrm{Id}_{\mathcal{F}(U)}$ through the isomorphism $\mathrm{Hom}_{\mathcal{C}}(\mathcal{G}(\mathcal{F}(U)), U) \cong \mathrm{Hom}_{\mathcal{D}}(\mathcal{F}(U), \mathcal{F}(U))$; that is, $g(U) = \Phi(\mathcal{F}(U), U)^{-1}(\mathrm{Id}_{\mathcal{F}(U)})$. Again, this is a natural transformation

$$g : \mathcal{G} \circ \mathcal{F} \to \mathrm{Id}_{\mathcal{C}}$$

called the *counit* of the adjunction isomorphism Φ.

Example A.21. The functor $\mathbf{Grps} \to \mathbf{Alg}(k)$ sending a group G to the group algebra kG is left adjoint to the functor $\mathbf{Alg}(k) \to \mathbf{Grps}$ sending a k-algebra A to the group $A^\times$. Indeed, any group homomorphism $G \to A^\times$ extends uniquely to an algebra homomorphism $kG \to A$, and this correspondence yields a bijection

$$\mathrm{Hom}_{\mathbf{Grps}}(G, A^\times) \cong \mathrm{Hom}_{Alg(k)}(kG, A) \ ,$$

where G is a group and A a k-algebra. The adjunction unit of this adjunction is given by the inclusion maps $G \to (kG)^\times$ and the corresponding counit is given by the algebra homomorphisms $kA^\times \to A$ induced by the inclusion $A^\times \subseteq A$.

Another important example is the tensor-Hom adjunction in B.13 below. The following result shows that adjunction isomorphisms and units/counits determine each other.

Theorem A.22. *Let $\mathcal{C}$, $\mathcal{D}$ be categories and let $\mathcal{F} : \mathcal{C} \to \mathcal{D}$, $\mathcal{G} : \mathcal{D} \to \mathcal{C}$ be covariant functors. If there is an adjunction isomorphism $\Phi : \mathrm{Hom}_{\mathcal{C}}(\mathcal{G}(-), -) \cong \mathrm{Hom}_{\mathcal{D}}(-, \mathcal{F}(-))$ then the unit f and counit g of Φ have the property that the two compositions of natural transformations*

$$\mathcal{F} \xrightarrow{\ f\mathcal{F}\ } \mathcal{F} \circ \mathcal{G} \circ \mathcal{F} \xrightarrow{\ \mathcal{F}g\ } \mathcal{F}$$

$$\mathcal{G} \xrightarrow{\mathcal{G}f} \mathcal{G} \circ \mathcal{F} \circ \mathcal{G} \xrightarrow{g\mathcal{G}} \mathcal{G}$$

are equal to the identity transformations on $\mathcal{F}$ and $\mathcal{G}$ respectively. Conversely, for any two natural transformations $f : \mathrm{Id}_{\mathcal{D}} \to \mathcal{F}\circ\mathcal{G}$ and $g : \mathcal{G}\circ\mathcal{F} \to \mathrm{Id}_{\mathcal{C}}$ satisfying $(\mathcal{F}g)\circ(f\mathcal{F}) = \mathrm{Id}_{\mathcal{F}}$ and $(g\mathcal{G})\circ(\mathcal{G}f) = \mathrm{Id}_{\mathcal{G}}$ there is a unique adjunction isomorphism $\Phi : \mathrm{Hom}_{\mathcal{C}}(\mathcal{G}(-), -) \cong \mathrm{Hom}_{\mathcal{D}}(-, \mathcal{F}(-))$ such that f is the unit of Φ and g is the counit of Φ. Moreover, in that case, Φ is determined by $\Phi(V,U)(\varphi) = \mathcal{F}(\varphi)\circ f(V)$ for any object U in $\mathcal{C}$, any object V in $\mathcal{D}$ and any morphism $\varphi : \mathcal{G}(V) \to U$ in $\mathcal{C}$; the inverse of Φ is determined by $\Phi(V,U)^{-1}(\psi) = g(U)\circ\mathcal{G}(\psi)$ for any morphism $\psi : V \to \mathcal{F}(U)$ in $\mathcal{D}$. In particular, we have $\varphi = g(U)\circ\mathcal{G}(\mathcal{F}(\varphi\circ f(V))$ and $\psi = \mathcal{F}(g(U)\circ\mathcal{G}(\psi))\circ f(V)$.

Proof. Let U be an object in $\mathcal{C}$ and V an object in $\mathcal{D}$. Suppose we have an isomorphism of bifunctors $\Phi : \mathrm{Hom}_{\mathcal{C}}(\mathcal{G}(-), -) \cong \mathrm{Hom}_{\mathcal{D}}(-, \mathcal{F}(-))$. We have a commutative diagram

$$\begin{tikzcd}
\mathrm{Hom}_{\mathcal{C}}(\mathcal{G}(V),\mathcal{G}(V)) \arrow[r, "\mathrm{Hom}_{\mathcal{C}}(\mathcal{G}(V){,}\varphi)"] \arrow[d] & \mathrm{Hom}_{\mathcal{C}}(\mathcal{G}(V),U) \arrow[d] \\
\mathrm{Hom}_{\mathcal{D}}(V,\mathcal{F}(\mathcal{G}(V))) \arrow[r, "\mathrm{Hom}_{\mathcal{D}}(V{,}\mathcal{F}(\varphi))"'] & \mathrm{Hom}_{\mathcal{D}}(V,\mathcal{F}(U))
\end{tikzcd}$$

where the vertical arrows are the natural bijections and the horizontal arrows are the maps induced by φ and $\mathcal{F}(\varphi)$. Chase now the element $\mathrm{Id}_{\mathcal{G}(V)}$ in this diagram. The image of $\mathrm{Id}_{\mathcal{G}(V)}$ in $\mathrm{Hom}_{\mathcal{C}}(\mathcal{G}(V),U)$ is φ, and its image in $\mathrm{Hom}_{\mathcal{D}}(V,\mathcal{F}(U))$ is equal to $\mathcal{F}(\varphi)f(V)$. By considering a similar diagram with inverted rôles one constructs a map sending ψ to $g(U)\circ\mathcal{G}(\psi)$ which is then an inverse of the preceding map, hence $\varphi = g(U)\circ\mathcal{G}(\mathcal{F}(\varphi)\circ f(V))$. This equality applied to $\mathrm{Id}_{\mathcal{G}(V)}$ shows that $\mathrm{Id}_{\mathcal{G}(V)} = g(\mathcal{G}(V))\circ\mathcal{G}(\mathcal{F}(\mathrm{Id}_{\mathcal{G}(V)})\circ f(V)) = (g(\mathcal{G}(V)))\circ(\mathcal{G}(f(V)))$, which implies that the composition $(g\mathcal{G})\circ(\mathcal{G}f)$ is the identity transformation on $\mathcal{G}$. Similarly one shows that the other composition in the statement is the identity. Conversely, suppose that $f : \mathrm{Id}_{\mathcal{D}} \to \mathcal{F}\circ\mathcal{G}$ and $g : \mathcal{G}\circ\mathcal{F} \to \mathrm{Id}_{\mathcal{C}}$ are natural transformations satisfying $(\mathcal{F}g)\circ(f\mathcal{F}) = \mathrm{Id}_{\mathcal{F}}$ and $(g\mathcal{G})\circ(\mathcal{G}f) = \mathrm{Id}_{\mathcal{G}}$. Consider the diagram

$$\begin{tikzcd}
\mathcal{G}(V) \arrow[r, "\mathcal{G}(f(V))"] \arrow[d, "\mathrm{Id}_{\mathcal{G}(V)}"'] & \mathcal{G}(\mathcal{F}(\mathcal{G}(V))) \arrow[r, "g(\mathcal{G}(V))"] \arrow[d, "\mathcal{G}(\mathcal{F}(\varphi))"'] & \mathcal{G}(V) \arrow[d, "\varphi"] \\
\mathcal{G}(V) \arrow[r, "\mathcal{G}(\mathcal{F}(\varphi)\circ f(V))"'] & \mathcal{G}(\mathcal{F}(U)) \arrow[r, "g(U)"'] & U
\end{tikzcd}$$

This diagram is commutative; indeed, the left rectangle commutes since $\mathcal{G}$ is a functor, and the right rectangle commutes since g is a natural transformation. Since, by the hypotheses on f and g we have $g(\mathcal{G}(V))\mathcal{G}(f(V)) = Id_{\mathcal{G}(V)}$ it follows that $\varphi = g(U)\mathcal{G}(\mathcal{F}(\varphi)f(V))$. Similarly, we have a commutative diagram

$$\begin{tikzcd}
V \arrow[r, "f(V)"] \arrow[d, "\psi"'] & \mathcal{F}(\mathcal{G}(V)) \arrow[r, "\mathcal{F}(g(U)\circ\mathcal{G}(\psi))"] \arrow[d, "\mathcal{F}(\mathcal{G}(\psi))"'] & \mathcal{F}(U) \arrow[d, "\mathrm{Id}_{\mathcal{F}}(U))"] \\
\mathcal{F}(U) \arrow[r, "f(\mathcal{F}(U))"'] & \mathcal{F}(\mathcal{G}(\mathcal{F}(U))) \arrow[r, "\mathcal{F}(g(U))"'] & \mathcal{F}(U)
\end{tikzcd}$$

from which we deduce that $\psi = \mathcal{F}(g(U) \circ \mathcal{G}(\psi)) \circ f(V)$. This shows that the maps sending φ to $\mathcal{F}(\varphi) \circ f(V)$ and ψ to $g(U) \circ \mathcal{G}(\psi)$ are inverse bijections. One easily checks that these bijections are natural, hence they define an isomorphism of bifunctors $\mathrm{Hom}_{\mathcal{C}}(\mathcal{G}(-), -) \cong \mathrm{Hom}_{\mathcal{D}}(-, \mathcal{F}(-))$. as stated. $\square$

B Appendix: The tensor product

The tensor product of two finite-dimensional vector spaces U, V over some field k is a *pair* consisting of a k-vector space W and an embedding $U \times V \to W$ such that any bilinear map from $U \times V$ to some other k-vector space X extends uniquely to a k-linear map from W to X. Such a space W always exists: if $m = \dim_k(U)$ and $n = \dim_k(V)$ we can take for W any k-vectorspace with dimension mn. An embedding $U \times V \to W$ with the above property can be specified as follows: choose a k-basis B of U, a k-basis C of V, and then identify $B \times C$ to a k-basis, say D, of W via some bijection $\beta : B \times C \cong D$. Then any bilinear map $\lambda : U \times V \to X$ extends to the unique linear map $\mu : W \to X$ defined by $\mu(\beta(b, c)) = \lambda(b, c)$ for all $(b, c) \in B \times C$. This characterises the tensor product as a solution of a universal problem. The ideas behind this construction extend to much more general situations where k is replaced by any algebra A over some commutative ring k, where U is a right A-module, V a left A-module and the resulting tensor product W, denoted by $U \otimes_A V$, is a k-module. Moreover, this construction has good functoriality properties. In this section k is an arbitrary commutative ring.

Definition B.1. Let A be a k-algebra, U a right A-module, V a left A-module and W a k-module. An *A-balanced map from $U \times V$ to W* is a k-bilinear map $\beta : U \times V \to W$ satisfying $\beta(ua, v) = \beta(u, av)$ for all $u \in U$, $v \in V$ and $a \in A$.

If $A = k$, then an A-balanced map is just a k-bilinear map.

Definition B.2. Let A be a k-algebra, U a right A-module and V a left A-module. A *tensor product of U and V over A* is a pair (W, β) consisting of a k-module W and an A-balanced map $\beta : U \times V \to W$ such that for any further pair (W', β') consisting of an k-module W' and an A-balanced map $\beta' : U \times V \to W'$ there is a unique k-linear map $\gamma : W \to W'$ such that $\beta' = \gamma \circ \beta$.

The next result establishes the existence of tensor products; we may then speak of "the" tensor product, because any solution of a universal problem, if it exists, is unique up to unique isomorphism.

Theorem B.3. *Let A be a k-algebra, U a right A-module and V a left A-module. There exists a tensor product (W, β) of U and V over A, and if (W', β') is another tensor product of U and V over A, there is a unique k-linear isomorphism $\gamma : W \to W'$ such that $\beta' = \gamma \circ \beta$.*

Proof. Let M be the free k-module having as basis a set of symbols $u \otimes v$ indexed by the elements $(u, v) \in U \times V$. Let I be the k-submodule of M generated by the set of all linear combintations of these symbols of the form $ua \otimes v - u \otimes av$, $(u + u') \otimes v - u \otimes v - u' \otimes v$, $u \otimes (v + v') - u \otimes v - u \otimes v'$, $r(u \otimes v) - (ru) \otimes v$, $r(u \otimes v) - u \otimes (rv)$, where $u, u' \in U$, $v, v' \in V$, $a \in A$ and $r \in k$. Set $W = M/I$ and define $\beta : U \times V \to W$ to be the unique map sending $(u, v) \in U \times V$ to the image of the symbol $u \otimes v$ in W. It follows from the definition of the submodule I of M that β is an A-balanced map. Given any further k-module W' together with an A-balanced map $\beta' : U \times V \to W'$ there is a unique map $M \to W'$ mapping the symbol $u \otimes v$ to $\beta'(u, v)$. Since β' is k-balanced, this map has I in its kernel and induces hence a unique map $\gamma : W \to W'$ mapping the image of $u \otimes v$ in W to $\beta'(u, v)$. Thus γ is the unique k-linear map from W to W' satisfying $\beta' = \gamma \circ \beta$. This proves the existence of a tensor product (W, β) of U and V over A. The uniqueness is a formal routine exercise: if (W', β') is another tensor product, there are unique k-linear maps $\gamma : W \to W'$ and $\delta : W' \to W$ such that $\beta' = \gamma \circ \beta$ and $\beta = \delta \circ \beta'$. Thus $\beta = \delta \circ \gamma \circ \beta$. But also $\beta = \mathrm{Id}_W \circ \beta$. Thus $\delta \circ \gamma = \mathrm{Id}_W$ by the universal property of (W, β). Similarly, $\gamma \circ \delta = \mathrm{Id}_{W'}$. Thus γ and δ are the uniquely determined isomorphisms between (W, β) and (W', β'). $\square$

With the notation of the previous theorem, we denote a tensor product (W, β) of U and V over A by $U \otimes_A V = W$, and $u \otimes v = \beta(u, v)$, for all $(u, v) \in U \times V$. The property that β is k-bilinear takes the following form: for $u, u' \in U$, $v, v' \in V$ and $r \in k$ we have $(u+u') \otimes v = (u \otimes v) + (u' \otimes v)$, we have $u \otimes (v + v') = (u \otimes v) + (u \otimes v')$, and we have $r(u \otimes v) = (ru) \otimes v = u \otimes (rv)$. Furthermore, the property β is A-balanced reads then $ua \otimes v = u \otimes av$, for all $a \in A$. An element in $U \otimes_A V$ of the form $u \otimes v$ is called an *elementary tensor*. Not all elements in $U \otimes_A V$ are elementary tensors, but they are finite k-linear combinations of elementary tensors.

Proposition B.4. *Let A be a k-algebra, U a right A-module and V a left A-module. The set of elementary tensors $\{u \otimes v \mid (u, v) \in U \times V\}$ generates $U \otimes_A V$ as a k-module.*

Proof. By the construction of $U \otimes_A V$ in the proof of B.3 the set of images $u \otimes v$ in $U \otimes_A V$ generates $U \otimes_A V$ as a k-module. One can see this also using the universal property: if we take for W the submodule of $U \otimes_A V$ generated by the set of elementary tensors then W, together with the map $U \times V \to W$ sending (u, v) to $u \otimes v$ is easily seen to be a tensor product of U and V over A. Thus the inclusion $W \subseteq U \otimes_A V$ must be an isomorphism. $\square$

When using the notation $u \otimes v$ for elementary tensors it is important to keep track of the algebra A over which the tensor product is taken - confusion could arise if B is a subalgebra of A, in which case the tensor products $U \otimes_A V$ and $U \otimes_B V$ are both defined, while the elementary tensors would be denoted by the same symbol $u \otimes v$. In those cases it is important to specify the meaning of $u \otimes v$, which could be done, for instance by naming the structural map $\beta : U \times V \to U \otimes_A V$ explicitly, as in the definition of the tensor product. The following string of results describes the basic formal properties of tensor products: compatibility with bimodule structures, with algebra structures, functoriality, associativity and additivity.

Proposition B.5. *Let A, B, C be k-algebras, let U be an A-B-bimodule and V a B-C-bimodule. Then the tensor product $U \otimes_B V$ has a unique structure of A-C-bimodule satisfying $a \cdot (u \otimes v) \cdot c = (au) \otimes (vc)$ for any $a \in A$, $c \in C$, $u \in U$ and $v \in V$.*

Proof. Let $a \in A$. The map $U \times V \to U \otimes_B V$ sending $(u, v) \in U \times V$ to $au \otimes v$ is clearly B-balanced. Thus there is a unique k-linear map $\varphi_a : U \otimes_B V \to U \otimes_B V$ such that $\varphi(u \otimes v) = au \otimes v$. If a' is another element in A we have $\varphi_{a'} \circ \varphi_a = \varphi_{a'a}$ because this is true on the tensors $u \otimes v$. Thus $a.(u \otimes v) = (au) \otimes v$ defines a unique left A-module structure on $U \otimes_B V$. In a similar way one sees that $(u \otimes v).c = u \otimes (vc)$ defines a unique right C-module structure on $U \otimes_B V$. For any $r \in k$ and $(u, v) \in U \times V$ we have $(ru) \otimes v = u \cdot (r1_B) \otimes v = u \otimes (r1_B) \cdot v = u \otimes (rv)$, and hence the left and right k-module structure of $U \otimes_B V$ coincide. $\square$

Proposition B.6. *Let A, B be k-algebras, let U be an A-module and V a B-module. There is a unique k-algebra structure on $A \otimes_k B$ satisfying $(a \otimes b)(a' \otimes b') = aa' \otimes bb'$ for all $a, a' \in A$, $b, b' \in B$, and there is a unique $A \otimes_k B$-module structure on $U \otimes_k V$ satisfying $(a \otimes b).(u \otimes v) = au \otimes bv$ for all $a \in A$, $b \in B$, $u \in U$ and $v \in V$.*

Proof. Let $a \in A$ and $b \in B$. The map sending $(u, v) \in U \times V$ to $au \otimes bv \in U \otimes_k V$ is k-balanced, hence extends uniquely to an k-endomorphism $\lambda_{a,b}$ of $U \otimes_k V$ mapping $u \otimes v$ to $au \otimes bv$. Then the map sending $(a, b) \in A \times B$ to $\lambda_{a,b} \in \mathrm{End}_k(U \otimes_k V)$ is k-balanced, hence extends uniquely to a map

$$\lambda : A \otimes_k B \longrightarrow \mathrm{End}_k(U \otimes_k V)$$

sending $a \otimes b$ to $\lambda_{a,b}$. Consider first the case where $U = A$ and $V = B$. We use in this case λ to define a multiplication μ on $A \otimes B$ as follows: for $x, y \in A \otimes_k B$, we set $\mu(x, y) = \lambda(x)(y)$. By construction, if $x = a \otimes b$ and $y = a' \otimes b'$ then $\mu(x, y) = aa' \otimes bb'$. This shows that μ defines a distributive and associative multiplication: as usual, it suffices to check this on tensors and there it is clear. Once we know that $A \otimes_k B$ has the algebra structure as claimed, we observe that for general U, V, the map λ is an k-algebra homomorphism; as before, one sees this by checking on tensors. Thus $U \otimes_k V$ gets in this way an $A \otimes_k B$-module structure, and this is exactly the structure as claimed, as follows from looking at tensors yet again. □

Proposition B.7. *Let A, B, C be k-algebras, let U, U' be A-B-bimodules, and let V, V' be B-C-bimodules. For any A-B-bimodule homomorphism $\varphi : U \to U'$ and any B-C-bimodule homomorphism $\psi : V \to V'$ there is a unique A-C-bimodule homomorphism $\varphi \otimes \psi : U \otimes_B V \to U' \otimes_B V'$ mapping $u \otimes v$ to $\varphi(u) \otimes \psi(v)$ for all $u \in U$ and $v \in V$.*

Proof. The map sending $(u, v) \in U \times V$ to $\varphi(u) \otimes \psi(v)$ is clearly B-balanced and extends hence uniquely to a map $\varphi \otimes \psi$ as stated. □

Proposition B.8. *Let A, B, C, D be k-algebras, let U be an A-B-bimodule, let V be a B-C-bimodule and let W be a C-D-bimodule. There is a unique isomorphism of A-D-bimodules*

$$U \otimes_B (V \otimes_C W) \cong (U \otimes_B V) \otimes_C W$$

mapping $u \otimes (v \otimes w)$ to $(u \otimes v) \otimes w$ for all $u \in U$, $v \in V$ and $w \in W$.

Proof. For any $u \in U$ the map $V \times W \to (U \otimes_B V) \otimes_C W$ sending (v, w) to $(u \otimes v) \otimes w$ is C-balanced, hence extends to a unique map $V \otimes_C W \to (U \otimes_B V) \otimes_C W$ sending $v \otimes w$ to $(u \otimes v) \otimes w$. This works for all $u \in U$, and hence we get a map $U \times (V \otimes_C W) \to (U \otimes_B V) \otimes_C W$ mapping $(u, v \otimes w)$ to $(u \otimes v) \otimes w$. This map now is B-balanced, and hence extends uniquely to a map $\Phi : U \otimes_B (V \otimes_C W) \to (U \otimes_B V) \otimes_C W$ sending $u \otimes (v \otimes w)$ to $(u \otimes v) \otimes w$. In a completely analogous way one shows that there is a unique map $\Psi : (U \otimes_B V) \otimes_C W \to U \otimes_B (V \otimes_C W)$ sending $(u \otimes v) \otimes w$ to $u \otimes (v \otimes w)$. Then Φ and Ψ are inverse to each other because they are so on tensors. Finally, both Φ, Ψ are A-D-bimodule homomorphisms because they are compatible with the A-D-bimodule structure on tensors. □

Proposition B.9. *Let A, B, C be k-algebras, let $\{U_i\}_{i \in I}$ be a family of A-B-bimodules indexed by some set I, and let V be a B-C-bimodule. We have a canonical isomorphism of A-C-bimodules*

$$(\oplus_{i \in I}\, U_i) \otimes_B V \cong \oplus_{i \in I}\, (U_i \otimes_B V)\ .$$

Proof. The proof consists of playing off against each other the universal properties of direct sums and the tensor product. In order to keep clumsy notation minimal, we write here $\oplus$ for the direct sum indexed by the set I. The direct sum $\oplus\, U_i$ is, by definition, an A-B-bimodule coming along with canonical homomorphisms $\iota_i : U_i \to \oplus\, U_i$ with the universal property that for any further A-B-bimodule M endowed with homomorphisms $\iota'_i : U_i \to M$ there is a unique homomorphism of A-B-bimodules $\alpha : \oplus\, U_i \to M$ such that $\iota'_i = \alpha \circ \iota_i$ for all $i \in I$. Similarly, the right side in the isomorphism of the statement is a direct sum, hence comes along with canonical A-C-bimodule homomorphisms $\sigma_i : U_i \otimes_B V \to \oplus\, U_i \otimes_B V$ fulfilling the analogous universal property. In order to show that the left side in the statement is isomorphic to the right side, we construct maps $\tau_i : U_i \otimes_B V \to (\oplus\, U_i) \otimes_B V$ and show that they fulfill the same universal property. For any $i \in I$ we have a map $U_i \times V \to (\oplus\, U_i) \otimes_B V$ mapping (u_i, v) to $\iota_i(u) \otimes v$, where $u_i \in U_i$ and $v \in V$. This map is B-balanced, hence extends uniquely to a map $\tau_i : U_i \otimes_B V \to (\oplus\, U_i) \otimes_B V$ sending $u_i \otimes v$ to $\iota_i(u_i) \otimes v$. Let now N be any further A-C-bimodule endowed with A-C-bimodule homomorphisms $\tau'_i : U_i \otimes_B V \to N$ for all $i \in I$. Given $v \in V$ we have a map $U_i \to N$ sending u_i to $\tau'_i(u_i \otimes v)$, thus a unique map $\oplus\, U_i \to M$ sending $\iota_i(u_i)$ to $\tau'_i(u_i \otimes v)$. Since this holds for all $v \in V$, we get a map $\oplus\, U_i \times V \to N$ sending $(\iota_i(u_i), v)$ to $\tau'_i(u_i \otimes v)$. This map is B-balanced and induces hence a unique map $\beta : (\oplus\, U_i) \otimes_B V \to N$ sending $\iota_i(u_i) \otimes v$ to $\tau'_i(u_i \otimes v)$. Thus the map β is the unique map satisfying $\beta \circ \tau_i = \tau'_i$ for all $i \in I$. This shows that the left side in the statement, endowed with the family of maps τ_i, is a direct sum of the module $U_i \otimes_B V$, hence canonically isomorphic to the right side. □

Of course, the obvious analogue of the above result holds, too: if U is an A-B-bimodule and $\{V_i\}_{i \in I}$ a family of B-C-bimodules, we have a canonical isomorphism of A-C-bimodules $U \otimes_B (\oplus_{i \in I}\, V_i) \cong \oplus_{i \in I}\, (U \otimes_B V_i)$; this is proved just in the same way. Combining the above statements shows that taking tensor products is a covariantly functorial construction, and just as for the functors using homomorphism spaces briefly discussed at the end of the last section, this functor has certain exactness properties - it is *right exact*:

Proposition B.10. *Let A, B be k-algebras and M an A-B-bimodule. There is a unique k-linear covariant functor $M \otimes_B - : \mathrm{Mod}(B) \to \mathrm{Mod}(A)$ sending any B-module V to the A-module $M \otimes_B V$ and sending any homomorphism of B-modules $\varphi : V \to V'$ to the homomorphism of A-modules $\mathrm{Id}_M \otimes \varphi : M \otimes_B V \to M \otimes_B V'$. Morover, for any exact sequence of B-bimodules of the form $W \to V \to U \to 0$, the induced sequence of A-modules $M \otimes_B W \to M \otimes_B V \to M \otimes_B U \to 0$ is exact.*

Proof. The fact that $M \otimes_B -$ is a covariant functor follows immediately from the preceding statements. For the exactness property observe first that the map $M \otimes_B V \to M \otimes_B U$ is surjective because its image contains all elementary tensors $m \otimes u$ thanks to the fact that the map $V \to U$ is surjective. We need to show the exactness at $M \otimes_B V$. Let $I \subseteq M \otimes_B V$ be the image of the map $M \otimes_B W \to M \otimes_B V$. This is contained in the kernel of the map $M \otimes_B V \to M \otimes_B U$, and hence induces a surjective map $\varphi : (M \otimes_B V)/I \to M \otimes_B U$. We need to show that φ is injective. For this it suffices to construct a map $\psi : M \otimes_B U \to (M \otimes_B V)/I$ such that $\psi \circ \varphi$ is the identity on $(M \otimes_B V)/I$. Let $m \in M$ and $u \in U$. Choose $v \in V$ in the preimage of u. Define a map $M \times U \to (M \otimes_B V)/I$ by sending (m, u) to the image $(m \otimes v) + I$. One checks that this does not depend on the choice of v, and that the resulting map is B-balanaced, hence induces a map $\psi : M \otimes_B U \to (M \otimes_B V)/I$. By construction the composition $\psi \circ \varphi$ is the identity map. □

The functor $M \otimes_B -$ need not be *exact*; that is, it need not preserve injective homomorphisms - see the example B.11 (e) below. A right B-module M is called *flat* if the functor $M \otimes_B -$ from $\mathrm{Mod}(B)$ to $\mathrm{Mod}(k)$ is exact. Again, there is an obvious analogue for right modules: there is a unique k-linear covariant functor $- \otimes_A M : \mathrm{Mod}(A^0) \to \mathrm{Mod}(B^0)$ sending a right A-module U to the right B-module $U \otimes_A M$ and sending a homomorphism of right A-modules $\varphi : U \to U'$ to the homomorphism of right B-modules $\varphi \otimes \mathrm{Id}_M : U \otimes_A M \to U' \otimes_A M$.

Examples B.11. (a) Let A be a k-algebra. Then A can be considered as A-A-bimodule via multiplication in A. For any left A-module U we have a canonical isomorphism of left A-modules $A \otimes_A U \cong U$ mapping $a \otimes u$ to au, where $a \in A$ and $u \in U$. The existence of such a map follows from the fact that the map $A \times U \to U$ sending (a, u) to au is trivially A-balanced. The inverse of this map sends $u \in U$ to $1_A \otimes u$. In conjunction with the above corollary this shows that the functor $A \otimes_A -$ on $\mathrm{Mod}(A)$ is isomorphic to the identity functor on $\mathrm{Mod}(A)$. Similarly, for any right A-module V we have a canonical isomorphism of right A-modules $V \otimes_A A \cong V$ sending $v \otimes a$ to va, where $a \in A$ and $v \in V$.

(b) The remarks at the beginning of this section show that if k is a field and U, V are finite-dimensional k-vector spaces, then $U \otimes_k V$ is a k-vector space of finite dimension $\dim_k(U) \cdot \dim_k(V)$.

(c) There is a canonical isomorphism of $\mathbb{Q}$-vector spaces $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z} \cong \mathbb{Q}$ mapping $q \otimes n$ to qn; the inverse maps q to $q \otimes 1$. In contrast, for any positive integer n we have $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} = \{0\}$ because if $q \in \mathbb{Q}$ and $c + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$ then $q \otimes (c + n\mathbb{Z}) = \frac{q}{n} \otimes (nc + nZ) = 0$ because $nc + n\mathbb{Z} = 0_{\mathbb{Z}/nZ}$. In other words, tensoring a finitely generated abelian group A with $\mathbb{Q}$ yields a vector space over $\mathbb{Q}$ whose dimension is the rank of the free part of A and which annihilites all torsion in A. This reasoning extends to the more general situation of an integral domain $\mathcal{O}$ with quotient field K: tensoring any torsion $\mathcal{O}$-module M by K yields zero, while tensoring a free $\mathcal{O}$-module of finite rank n yields a K-vector space of dimension n.

(d) If n, m are coprime positive integers then $\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} (\mathbb{Z}/n\mathbb{Z}) = \{0\}$. Indeed, there are integers a, b such that $am + bn = 1$. Thus for $c, d \in \mathbb{Z}$ we have $(c + m\mathbb{Z}) \otimes_{\mathbb{Z}} (d + n\mathbb{Z}) = (cam + cbn) + m\mathbb{Z}) \otimes (d + n\mathbb{Z}) = (cam + m\mathbb{Z}) \otimes (d + n\mathbb{Z}) \; + \; (c + m\mathbb{Z}) \otimes (bnd + n\mathbb{Z})$, which is zero because $cam + m\mathbb{Z}$ and $bnd + n\mathbb{Z}$ are zero in $\mathbb{Z}/m\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$, respectively.

(e) Let A be a k-algebra, U a right A-module and $\varphi : V \to V'$ a homomorphism of left A-modules. If φ is surjective then the induced map $\mathrm{Id}_U \otimes \varphi$ from $U \otimes_A V$ to $U \otimes_A V'$ is surjective as well by B.10. It is not true, in general, that if φ is injective then $\mathrm{Id}_U \otimes \varphi$ is injective. Here is a general source of examples for this phenomenon: let I be a non zero ideal in A whose square I^2 is zero. Denote by $\varphi : I \to A$ the inclusion map; this is in particular a homomorphism of left A-modules. Since I is an ideal, we may consider I also as right A-modules. Tensoring by $I \otimes_A -$ yields a map $\mathrm{Id}_I \otimes \varphi : I \otimes_A I \to I \otimes_A A$. This map is always zero: if $a, b \in I$ then the image of $a \otimes b$ in $I \otimes A$ can be written in the form $a \otimes b = a \otimes b \cdot 1_A = ab \otimes 1$, and this is zero as $ab \in I^2 = \{0\}$ by the assumptions. Simple examples of this format arise for $A = \mathbb{Z}/4\mathbb{Z}$ and $I = 2\mathbb{Z}/4\mathbb{Z}$, with $k = \mathbb{Z}$. One checks that $I \otimes_A I \cong I \otimes_{\mathbb{Z}} I$ is non zero, with exactly two elements.

The tensor product is closely related to functors obtained from taking homomorphism spaces. Let A, B be k-algebras, M an A-B-bimodule and U an A-module. Then $\mathrm{Hom}_A(M, U)$ becomes a B-module via $(b \cdot \mu)(m) = \mu(mb)$, where $m \in M$, $b \in B$ and $\mu \in \mathrm{Hom}_A(M, U)$. This construction is covariant functorial: if $\alpha : U \to V$ is a homomorphism of A-modules, then the induced map $\mathrm{Hom}_A(M, U) \to \mathrm{Hom}_A(M, V)$ sending $\mu \in \mathrm{Hom}_A(M, U)$ to $\alpha \circ \mu$ is easily seen to be a B-homomorphism. We denote by $\mathrm{Hom}_A(M, -)$ the functor from $\mathrm{Mod}(A)$ to $\mathrm{Mod}(B)$ obtained in this way. Similarly, $\mathrm{Hom}_A(U, M)$ becomes a right B-module via $(\nu.b)(u) = \nu(u)b$, where $u \in U$, $b \in B$ and $\nu \in \mathrm{Hom}_A(U, M)$. This construction is now contravariant functorial: if $\alpha : U \to V$ is a homomorphism of A-modules then the induced map $\mathrm{Hom}_A(V, M) \to \mathrm{Hom}_A(U, M)$ sending $\nu \in \mathrm{Hom}_A(V, M)$ to $\nu \circ \alpha$ is a homomorphism of right B-modules. We denote by $\mathrm{Hom}_A(-, M)$ the contravariant functor from $\mathrm{Mod}(A)$ to $\mathrm{Mod}(B^{\mathrm{op}})$ obtained in this way. These two functors have the following exactness properties:

Proposition B.12. *Let A, B be k-algebras and M be an A-B-bimodule.*

(i) If $0 \to U \to V \to W$ is an exact sequence of A-modules then the induced sequence of B-modules $0 \to \mathrm{Hom}_A(M, U) \to \mathrm{Hom}_A(M, V) \to \mathrm{Hom}_A(M, W)$ is exact.

(ii) If $W \to V \to U \to 0$ is an exact sequence of A-modules then the induces sequence of right B-modules $0 \to \mathrm{Hom}_A(U, M) \to \mathrm{Hom}_A(V, M) \to \mathrm{Hom}_A(W, M)$ is exact.

Proof. Straightforward verification. □

In other words, the functor $\mathrm{Hom}_A(M, -)$ is *left exact.* It is not exact, in general, because it need not preserve surjective homomorphisms. This leads to the consideration of *projective modules.* Similarly, the functor $\mathrm{Hom}_A(-, M)$ need not be exact - this leads to the consideration of *injective modules.* The single most important general statement in module theory is arguably the following theorem stating that the functor $M \otimes_B -$ is left adjoint to the functor $\mathrm{Hom}_A(M, -)$.

Theorem B.13. *Let A, B be k-algebras and let M be an A-B-bimodule. For any A-module U and any B-module V we have natural inverse isomorphisms of k-modules*

$$\begin{cases} \mathrm{Hom}_A(M \otimes_B V, U) & \cong & \mathrm{Hom}_B(V, \mathrm{Hom}_A(M, U)) \\ \varphi & \to & (v \mapsto (m \mapsto \varphi(m \otimes v))) \\ (m \otimes v \mapsto \psi(v)(m)) & \longleftarrow & \psi \end{cases}$$

Proof. This is a series of straightforward verifications: one checks that

(1) the map $m \mapsto \varphi(m \otimes v)$ is an A-homomorphism from M to U;

(2) the map $v \mapsto (m \mapsto \varphi(m \otimes v))$ is a B-homomorphism from V to $\mathrm{Hom}_A(M, U)$;

(3) the map $\varphi \mapsto (v \mapsto (m \mapsto \varphi(m \otimes v)))$ is k-linear;

(4) the map $m \otimes v \mapsto \psi(v)(m)$ is well-defined (that is, one needs to check that $mb \otimes v$ and $m \otimes bv$ have the same image, for $b \in B$);

(5) the map $m \otimes v \mapsto \psi(v)(m)$ is an A-homomorphism from $M \otimes_B V$ to U;

(6) the map $\psi \mapsto (m \otimes v \mapsto \psi(v)(m))$ is inverse to the map $\varphi \mapsto (v \mapsto (m \mapsto \varphi(m \otimes v)))$. □

The left exactness of $\mathrm{Hom}_A(M, -)$ and the right exactness of $M \otimes_B -$ are formal consequences of this adjunction.

References

[1] J. L. Alperin, *Local Representation Theory*, Cambridge studies in Advanced Mathematics **11**, Cambridge University Press (1986).

[2] J. L. Alperin, *Weights for finite groups*, Proc. Symp. Pure Math. **47** (1987), 369–379.

[3] M. Auslander, I. Reiten, and S. O. Smalø, *Representation Theory of Artin Algebras*, Cambridge studies in advanced mathematics **36**, Cambridge University Press (1995).

[4] D. J. Benson, *Representations and Cohomology, Vol. I: Cohomology of groups and modules*, Cambridge studies in advanced mathematics **30**, Cambridge University Press (1991).

[5] D. J. Benson, *Representations and Cohomology, Vol. II: Cohomology of groups and modules*, Cambridge studies in advanced mathematics **31**, Cambridge University Press (1991).

[6] H. Cartan and S. Eilenberg, Homological Algebra. Princeton University Press, Princeton, New Jersey (1956).

[7] P. Gabriel, *Unzerlegbare Darstellungen I*, Manuscripta Math. **6** (1972) 71–103.

[8] J. A. Green, *Some remarks on defect groups*, Math. Z. **107** (1968), 133–150.

[9] I. M. Isaacs, *Character theory of finite groups*, Dover (1994).

[10] M. Linckelmann, *Cohomology of block algebras of finite groups*, in: Representations of Algebras and Related Topics, ICRA XIV, Tokyo (eds: A. Skowroński and K. Yamagata), European Math. Soc. Series of Congress Reports(2011), 189–250.

[11] J.-P. Serre, *Linear Representations of Finite Groups*, Graduate Texts in Mathematics **42**, Springer-Verlag, New York (1982).

[12] J. Thévenaz, *G-Algebras and Modular Representation Theory*, Oxford Science Publications, Clarendon, Oxford (1995).

[13] C. A. Weibel, *An introduction to homological algebra*, Cambridge studies in advanced mathematics **38**, Cambridge University Press (1994).

Index