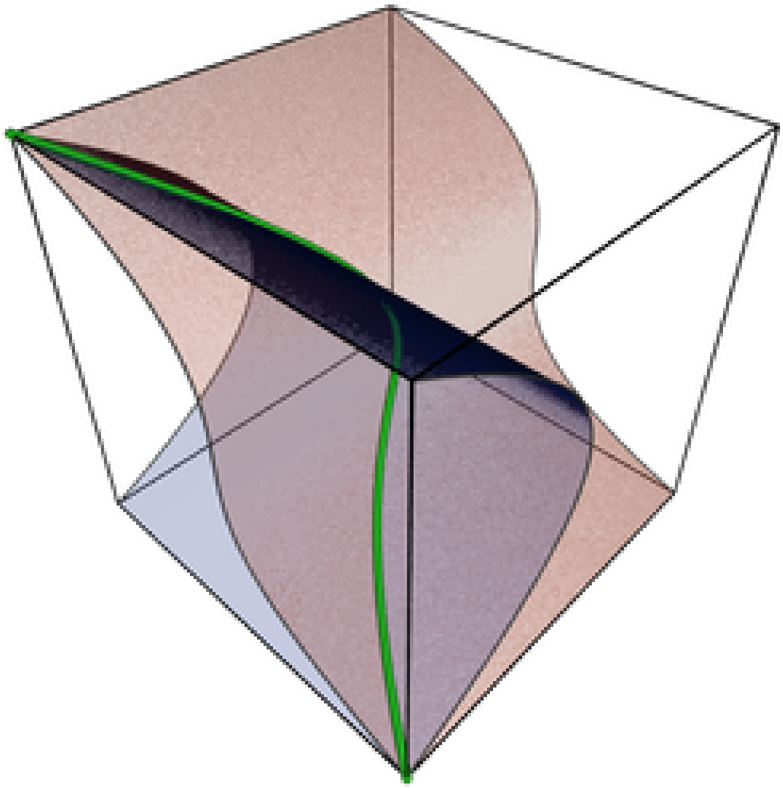
Non-commutative Algebra



Patrick Da Silva

Freie Universität Berlin

June 2, 2017

Table of Contents

Chapter 1

Introduction to unital rings

We assume the reader is familiar with a bit of algebra (at least elementary group theory). All our rings are assumed unital, namely multiplication admits a unique neutral element which will always be denoted by 1. This set of notes will serve as a reference to other sets of notes when proofs are necessary, and thus is not meant to be introductory. The set of non-negative integers $\mathbb{N}$ is equal to $\{0, 1, \cdots, n, \cdots\}$ (this has the advantage of turning it into a monoid).

1.1 Generalities

Definition 1.1. Let A be an abelian group denoted additively, i.e. via the symbol $+$ and with neutral element 0. We say that A is a (unital) **ring** when it is equipped with a multiplication (usually denoted by juxtaposition) $\cdot : A \times A \to A$ satisfying the following axioms :

- *Distributivity :* For all $a_1, a_2, a_3 \in A$,

$$a_1(a_2 + a_3) = a_1a_2 + a_1a_3, \quad (a_1 + a_2)a_3 = a_1a_3 + a_2a_3.$$

- *Associativity :* For all $a_1, a_2, a_3 \in A$,

$$a_1(a_2a_3) = (a_1a_2)a_3.$$

- *Neutral element :* There exists a unique element, call the **unit element** (or simply 1) and denoted by $1 \in A$, such that for all $a \in A$,

$$1a = a = a1.$$

A **subring** of A is a subset of A which contains 1 and is closed under addition and multiplication, and thus becomes a ring of its own.

Remark 1.2. If M is an abelian group, the collection of all abelian group endomorphisms of M, denoted by $\mathrm{End}_{\mathbb{Z}}(M)$, is a ring ; the identity endomorphism of M serves as unit element, addition is performed pointwise and multiplication is given by composition.

Definition 1.3. Let A, B be rings.

(i) A **morphism of rings** is a map $\varphi : A \to B$ such that for all $a_1, a_2 \in A$,

$$\varphi(a_1 + a_2) = \varphi(a_1) + \varphi(a_2), \quad \varphi(a_1a_2) = \varphi(a_1)\varphi(a_2), \quad \varphi(1) = 1.$$

It is clear under this definition that the image $\mathrm{im}\,\varphi \overset{\text{def}}{=} \varphi(A)$ is a subring of B.

(ii) A **left** A**-module** is an abelian group M together with a morphism of rings $\varphi : A \to \mathrm{End}_{\mathbb{Z}}(M)$. This morphism defines a left action of A on M, namely a map $A \times M \to M$, whose output is usually denoted by juxtaposition, and is given by $am \overset{\mathrm{def}}{=} \varphi_a(m)$, where $\varphi_a \overset{\mathrm{def}}{=} \varphi(a)$. The assumptions on a morphism of rings shows that $\varphi_1 = \mathrm{id}_M$, φ_a is an endomorphism of abelian groups and $\varphi_{a_1 a_2} = \varphi_{a_1} \circ \varphi_{a_2}$.

(iii) Given a ring A, the **opposite ring** A^{opp} is a ring whose underlying abelian group is equal to A but if we denote multiplication in A^{opp} by $\cdot$ and that of A by juxtaposition, for $a_1, a_2 \in A^{\mathrm{opp}}$, we set

$$a_1 \cdot a_2 \overset{\mathrm{def}}{=} a_2 a_1.$$

Reading the axioms of a ring in the multiplicatively reversed order shows that A^{opp} is a ring and has the same unit element as A.

(iv) A **right** A**-module** is an abelian group N together with a morphism of rings $\psi : A \to \mathrm{End}_{\mathbb{Z}}(M)^{\mathrm{opp}}$. To make notation more natural, an element $\varphi \in \mathrm{End}_{\mathbb{Z}}(M)^{\mathrm{opp}}$ acts on $m \in M$ by setting the endomorphism on the right, not on the left ; in other words, for all $m \in M$,

$$\varphi \in \mathrm{End}_{\mathbb{Z}}(M) \longrightarrow \varphi(m),$$
$$\varphi \in \mathrm{End}_{\mathbb{Z}}(M)^{\mathrm{opp}} \longrightarrow (m)\varphi.$$

This morphism defines a right action of A on M, namely a map $M \times A \to M$, whose output is also denoted by juxtaposition and is given by $ma \overset{\mathrm{def}}{=} \varphi_a(m)$. This is indeed a right action of A on M :

$$m(a_1 a_2) \overset{\mathrm{def}}{=} (m)\varphi_{a_1 a_2} = ((m)\varphi_{a_1})\varphi_{a_2}.$$

The order has indeed been reversed, since in $\mathrm{End}_{\mathbb{Z}}(M)$, the composition $\varphi_{a_1} \circ \varphi_{a_2}$ applied to $m \in M$ is equal to $\varphi_{a_1}(\varphi_{a_2}(m))$, where as in $\mathrm{End}_{\mathbb{Z}}(M)^{\mathrm{opp}}$, the composition $\varphi_{a_1} \circ \varphi_{a_2}$ applied to m equals $\varphi_{a_2}(\varphi_{a_1}(m))$; to emphasize the right action and hopefully minimize confusion, we chose the above notation.

(v) An (A, B)**-bimodule** is an abelian group M together with two morphisms of rings, namely $\varphi^L : A \to \mathrm{End}_{\mathbb{Z}}(M)$ and $\varphi^R : B \to \mathrm{End}_{\mathbb{Z}}(M)^{\mathrm{opp}}$, corresponding to left and right multiplication. The maps φ^L and φ^R are required to turn M into a left A-module and a right B-module respectively, together with the additional property that for all $a \in A$, $b \in B$ and $m \in M$,

$$(\varphi^L_a(m))\varphi^R_b = \varphi^L_a((m)\varphi^R_b).$$

Note that for left and right A-modules M, we usually denote the action of $a \in A$ on $m \in M$ by juxtaposition, namely $am \overset{\mathrm{def}}{=} \varphi_a(m)$. The axioms of an (A, B)-bimodule becomes essentially "associativity", namely $a(mb) = (am)b$. When $A = B$, we call an (A, A)-bimodule simply an A-**bimodule**.

(vi) If M is an abelian group which is a left A-module and a left B-module, we can canonically turn M into a right B^{opp}-module. We say that the two module structures on M are **compatible** if they make M a (A, B^{opp})-module. This is equivalent to asking that

$$\forall m \in M, a \in A, b \in B, \quad a(bm) = b(am).$$

Similarly, if M is a right A-module and a right B-module, we say that these are compatible if it makes M a (A^{opp}, B)-bimodule, which is equivalent to asking that

$$\forall m \in M, a \in A, b \in B, \quad (ma)b = (mb)a.$$

More generally, if $\{A_i\}_{i\in I}$ and $\{B_j\}_{j\in J}$ are two families of rings and M is an (A_i, B_j)-bimodule for each $i \in I, j \in J$, we say that these structures are **compatible** if the module structures given by $A_i, A_{i'}$ are compatible for all $i, i' \in I$ and the module structures iven by $B_j, B_{j'}$ are compatible for all $j, j' \in J$.

(vii) A **morphism** of left A-modules/right A-modules/(A, B)-bimodules is a morphism of abelian groups between two left A-modules/right A-modules/(A, B)-bimodules which commutes with the action of A on M. For instance, if $\varphi : M \to N$ is a morphism of abelian groups between two left A-modules, it is a morphism of left A-modules precisely when

$$\forall a \in A, \quad \forall m \in M, \quad \varphi(am) = a\varphi(m).$$

Remark 1.4. The collection of (small) left A-modules together with their morphisms form a category, which we denote by A-$\mathbf{Mod}$. Similarly, right A-modules and (A, B)-bimodules form categories ; we denote them by $\mathbf{Mod}$-A and A-$\mathbf{Mod}$-B, respectively. Therefore, left and right A-modules inherit notions of endomorphism, automorphism, monomorphism, epimorphism, isomorphism, etc. The composition of two maps (which are morphisms of some type, most of the time) is denoted by $\circ$ (for example, $\varphi \circ \psi$), except when the maps composed belong to some ring, in which case we might adopt juxtaposition as the symbol for composition.

Definition 1.5. Let A be a ring and M be a left A-module. The **endomorphism ring of** M is the ring $\mathrm{End}_A(M)$ consisting of all endomorphisms of M, i.e. morphisms of left A-modules $\varphi : M \to M$. Addition is done element-wise and multiplication is given by composition. If M is a right A-module, we also denote its endomorphism ring by $\mathrm{End}_A(M)$. When M is an (A, B)-bimodule, we denote the ring of all (A, B)-module endomorphisms of M by $\mathrm{End}_{(A,B)}(M)$.

Remark 1.6. A morphism of rings $\varphi : A \to B$ is equivalent to a morphism of rings $\varphi^{\mathrm{opp}} : A^{\mathrm{opp}} \to B^{\mathrm{opp}}$; the underlying set maps φ and φ^{opp} are equal, but the requirement that φ^{opp} respects multiplication is the multiplicative axiom of φ read in reverse. It follows that a right A-module is nothing more but a left A^{opp}-module, so anything proven about all left A-modules for any ring A is also proven for right A-modules, when the statement is read appropriately.

To prevent ourselves from dealing with left and right A-modules all the time, unless we specifically need both notions, we will stick to left A-modules. Given a left A-module M, the right A^{opp}-module structure on M corresponding to its left A-module structure will be denoted by M^{opp} (i.e. the morphism of rings $\varphi : A \to \mathrm{End}_{\mathbb{Z}}(M)$ corresponds to $\varphi : A^{\mathrm{opp}} \to \mathrm{End}_{\mathbb{Z}}(M)^{\mathrm{opp}}$, so it is given by the same data but in a different notation).

Definition 1.7. Let A be a ring and M a left A-module. A subset $N \subseteq M$ is called a **left A-submodule** of M (or simply an A-submodule) if it is an abelian subgroup of M which is stable under the action of A, i.e. for all $a \in A$ and $n \in N$, $an \in N$. We also say that N is **stable under** A to say that it is an A-submodule of M. In this case, we write $N \leq M$ to indicate that N is a submodule of M. Given a family of submodules $\{N_i\}_{i\in I}$, we can define their **sum** as

$$\sum_{i\in I} N_i \overset{\mathrm{def}}{=} \left\{ \sum_{i\in I}^{*} n_i \,\middle|\, n_i \in N_i \right\}$$

where the superscript * indicates that only finitely many of the n_i's are non-zero. A family of submodules $\{N_i\}_{i\in I}$ of M is said to be in a **direct sum** if they are in a direct sum as abelian groups, namely every $m \in \sum_{i\in I} N_i$ can be written uniquely as a sum $m = \sum_{i\in I}^{*} n_i, \quad n_i \in N_i$. When $\sum_{i\in I} N_i = M$, we write $M = \bigoplus_{i\in I} N_i$ and we say that M is the **direct sum of the N_i's**.

Remark 1.8. To check if M is a direct sum of two of its submodules N_1, N_2, it suffices to check if $N_1 + N_2 = M$ and $N_1 \cap N_2 = 0$, where 0 denotes the trivial submodule consisting only of the zero element of M. One needs to be careful when trying to check that M is the direct sum of k submodules, $k \in \mathbb{N}$; in this case, one must verify that

$$\sum_{i=1}^{k} N_i = M, \quad \forall 1 \leq i \leq k, \quad N_i \cap \left(\sum_{\substack{j=1 \\ j \neq i}}^{k} N_j \right) = 0.$$

Proposition 1.9. (Isomorphism theorems) Let A be a ring and $\varphi : M \to N$ be a morphism of left A-modules.

(i) If $N \leq M$, the **quotient module** M/N is defined as the quotient abelian group. Its A-module structure is given by

$$a(m+N) \stackrel{\text{def}}{=} am + N.$$

It is indeed a left A-module.

(ii) The **kernel** and the **image** of φ is defined as its kernel and image as abelian groups. We denote them by $\ker \varphi \leq M$ and $\operatorname{im} \varphi \leq N$. It induces a natural morphism $\widetilde{\varphi} : M/\ker \varphi \to N$ which is onto $\operatorname{im} \varphi$, thus giving the first isomorphism theorem :

$$M/\ker \varphi \simeq \operatorname{im} \varphi.$$

(iii) If $N_1, N_2 \leq M$ are two left A-submodules, then $N_1 + N_2, N_1 \cap N_2 \leq M$ and we have the second isomorphism theorem

$$(N_1 + N_2)/N_1 \simeq N_1/(N_1 \cap N_2).$$

(iv) If $N_1 \leq N_2 \leq M$, then N_1 is a submodule of M and

$$(M/N_1)/(N_2/N_1) \simeq M/N_2.$$

Proof. This is the same proof as in the commutative case, hence is omitted.

Definition 1.10. Let A be a ring. One can see A as an A-bimodule over itself by using multiplication, i.e. $\varphi^L_{a_1}(a_2) = a_1 a_2 = (a_1)\varphi^R_{a_2}$. A **left ideal** (resp. **right ideal**, **two-sided ideal**) of A is a left A-submodule (resp. right A-submodule, A-bisubmodule) of A when seen as an A-bimodule over itself.

Given a left A-module M and a subset $S \subseteq M$, we can define the **left A-submodule of M generated by** S, written ${}_A\langle S \rangle$, as the smallest A-submodule of M containing S ; it can be constructed as the intersection of all A-submodules of M which contain S, since this collection is non-empty because M is in it. Similarly, one defines the **right A-submodule of M generated by** S as $\langle S \rangle_A$ when M is a right A-module. If B is a ring and M is an (A,B)-bimodule, then the **(A,B)-bisubmodule of M generated by** S is defined the same way and is written ${}_A\langle S \rangle_B$.

When A is seen as an A-bimodule over itself, we use a different notation. For $S \subseteq A$, the left ideal, right ideal and two-sided ideal generated by S are denoted respectively by ${}_A(S)\,, (S)_A$ and ${}_A(S)_A$.

If $S = \{m_1, \cdots, m_n\}$ is a finite subset of M, we write ${}_A\langle m_1, \cdots, m_n \rangle$ instead (similar notations when M is a right A-module or an (A,B)-bimodule, or when $A = M$ is an A-bimodule over itself and we speak of ideals). If $S = \{m\}$ is a singleton, we may write $Am \stackrel{\text{def}}{=} {}_A\langle m \rangle$, $mA \stackrel{\text{def}}{=} \langle m \rangle_A$ and $AmB \stackrel{\text{def}}{=} {}_A\langle m \rangle_B$, so that

$${}_A\langle m_1, \cdots, m_n \rangle = \sum_{i=1}^{n} Am_i, \quad \langle m_1, \cdots, m_n \rangle_A = \sum_{i=1}^{n} m_i A, \quad {}_A\langle m_1, \cdots, m_n \rangle_B = \sum_{i=1}^{n} Am_i B.$$

Remark 1.11. When $\varphi : A \to B$ is a morphism of rings, $\operatorname{im}\varphi$ is a subring of B and $\ker\varphi$ is a two-sided ideal of A, which allows to turn the quotient $A/\ker\varphi$ into an A-bimodule. This A-bimodule structure turns $A/\ker\varphi$ into a ring of its own and $A/\ker\varphi \simeq \operatorname{im}\varphi$.

Proposition 1.12. Let A be a ring and M a left A-module. An element $\pi \in \operatorname{End}_A(M)$ is called a **projection** if $\pi^2 = \pi$.

(i) If π is a projection, then we have $M = \ker\pi \oplus \operatorname{im}\pi$.

(ii) If π is a projection, then so is $1-\pi$ (recall that $1 \in \operatorname{End}_A(M)$ is the identity map of M).

(iii) Whenever $m \in M$ is written as $m = m_1 + m_2$ where $m_1 \in \operatorname{im}\pi$ and $m_2 \in \ker\pi$, we have $m_1 = \pi(m)$ and $m_2 = (1-\pi)(m)$.

(iv) We have $\ker\pi = \operatorname{im}(1-\pi)$ and $\operatorname{im}\pi = \ker(1-\pi)$.

(v) Let $\pi \in \operatorname{End}_A(M)$ be a projection. We have the identities

$$\operatorname{End}_A(M)\pi = \{\varphi \in \operatorname{End}_A(M) \mid \ker\varphi \supseteq \ker\pi\}, \quad \pi\operatorname{End}_A(M) = \{\varphi \in \operatorname{End}_A(M) \mid \operatorname{im}\varphi \subseteq \operatorname{im}\pi\}.$$

(vi) If $M = N_1 \oplus N_2$ is the direct sum of two left A-submodules, let $\pi \in \operatorname{End}_A(M)$ be the endomorphism defined by $\pi(n_1+n_2) \stackrel{\text{def}}{=} n_1$. Then π is the unique projection in $\operatorname{End}_A(M)$ which satisfies $\ker\pi = N_2$ and $\operatorname{im}\pi = N_1$; we call it the **projection onto** N_1 and denote it by π_{N_1} or simply π_1 if the context allows it. More generally, if $M = \bigoplus_{i\in I} N_i$, there is a unique projection $\pi \in \operatorname{End}_A(M)$ satisfying $\operatorname{im}\pi = N_i$ and $\ker\pi = \bigoplus_{j\in I\setminus\{i\}} N_j$.

Proof. For $m \in M$, write $m = (m - \pi(m)) + \pi(m)$, so that $M = \ker\pi + \operatorname{im}\pi$. If $m \in \ker\pi \cap \operatorname{im}\pi$, then $m = \pi(m') = \pi^2(m') = \pi(m) = 0$, which proves (i). Note that $\pi = (1-(1-\pi))$, which proves (ii), (iii) and (iv) because $m = (m-\pi(m)) + \pi(m)$.

To prove (v), we proceed with the first equality. If $\varphi = \psi\pi$, then $\pi(m) = 0$ implies $\psi(\pi(m)) = 0$, hence the inclusion $(\supseteq)$ holds. For the reverse, if $\varphi : M \to M$ satisfies $\ker\varphi \supseteq \ker\pi$, then φ is entirely determined by the values it takes on $\operatorname{im}\pi$. But for $m \in \operatorname{im}\pi$, we have $\varphi(m) = \varphi(\pi(m))$, hence $\varphi = \varphi\pi \in \operatorname{End}_A(M)\pi$.

As for the second equality, it is clear that $\operatorname{im}\pi\varphi \subseteq \operatorname{im}\pi$, which gives $(\subseteq)$. For the reverse inclusion, suppose $\varphi \in \operatorname{End}_A(M)$ satisfies $\operatorname{im}\varphi \subseteq \operatorname{im}\pi$. Then $\varphi(m) \in \operatorname{im}\pi$ for all $m \in M$, hence $\pi(\varphi(m)) = \varphi(m)$, which means $\varphi = \pi\varphi \in \pi\operatorname{End}_A(M)$, as desired.

Finally, the endomorphism defined in (vi) is clearly a projection. Its unicity comes from part (iii).

Definition 1.13. Let A be a ring, M a left A-module and $N \leq M$ an A-submodule. We say that N is a **direct summand** if there exists a projection on M onto N. In other words, N is a direct summand if there exists an A-submodule $N' \leq M$ such that $M = N \oplus N'$.

Definition 1.14. Let A be a ring and M, N be two left A-modules. The set $\operatorname{Hom}_A(M,N)$ is defined as the set of all morphisms of left A-modules $\varphi : M \to N$. It is obviously an abelian group, and it is turned into a left A-module by

$$(a\varphi)(m) \stackrel{\text{def}}{=} a\varphi(m) = \varphi(am).$$

This construction is functorial in the following sense. Given morphisms $\varphi : M_2 \to M_1$ and $\psi : N_1 \to N_2$, we obtain a morphism $\operatorname{Hom}_A(\varphi,\psi) : \operatorname{Hom}_A(M_1,N_1) \to \operatorname{Hom}_A(M_2,N_2)$ by sending α to $\psi \circ \alpha \circ \varphi$. The following diagram commutes :

$$\begin{array}{ccc} \mathrm{Hom}_A(M_1,N_1) & \xrightarrow{\mathrm{Hom}_A(\varphi,\mathrm{id}_{N_1})} & \mathrm{Hom}_A(M_2,N_1) \\ \downarrow{\scriptstyle \mathrm{Hom}_A(\mathrm{id}_{M_1},\psi)} & \searrow{\scriptstyle \mathrm{Hom}_A(\varphi,\psi)} & \downarrow{\scriptstyle \mathrm{Hom}_A(\mathrm{id}_{M_2},\psi)} \\ \mathrm{Hom}_A(M_1,N_2) & \xrightarrow{\mathrm{Hom}_A(\varphi,\mathrm{id}_{N_2})} & \mathrm{Hom}_A(M_2,N_2) \end{array}$$

We sometimes write $\mathrm{Hom}_A(M,\psi)$ instead of $\mathrm{Hom}_A(\mathrm{id}_M,\psi) : \mathrm{Hom}_A(M,N_1) \to \mathrm{Hom}_A(M,N_2)$ when $\psi : N_1 \to N_2$ is a morphism ; similarly for $\mathrm{Hom}_A(\varphi,N) : \mathrm{Hom}_A(M_1,N) \to \mathrm{Hom}_A(M_2,N)$.

Remark 1.15. As in the case of abelian groups, we have a notion of short exact sequences

$$0 \longrightarrow M_1 \xrightarrow{\varphi} M_2 \xrightarrow{\psi} M_3 \longrightarrow 0.$$

This sequence is said to be exact at M_2 when $\ker\psi = \operatorname{im}\varphi$, and more generally, it is called a short exact sequence when φ is injective, ψ is surjective and $\ker\psi = \operatorname{im}\varphi$, in which case $M_2/\varphi(M_1) \simeq M_3$ (this is equivalent to asking the sequence to be exact at M_1, M_2 and M_3). Applying $\mathrm{Hom}_A(N,-)$ on this sequence, we obtain the **left-exact sequence**

$$0 \longrightarrow \mathrm{Hom}_A(N,M_1) \xrightarrow{\mathrm{Hom}_A(N,\varphi)} \mathrm{Hom}_A(N,M_2) \xrightarrow{\mathrm{Hom}_A(N,\psi)} \mathrm{Hom}_A(N,M_3)$$

Left-exactness means that the sequence is exact at $\mathrm{Hom}_A(N,M_1)$ and $\mathrm{Hom}_A(N,M_2)$ but not necessarily at $\mathrm{Hom}_A(N,M_3)$. Applying $\mathrm{Hom}_A(-,N)$ on this sequence, we obtain the left-exact sequence

$$0 \longrightarrow \mathrm{Hom}_A(M_3,N) \xrightarrow{\mathrm{Hom}_A(\psi,N)} \mathrm{Hom}_A(M_2,N) \xrightarrow{\mathrm{Hom}_A(\varphi,N)} \mathrm{Hom}_A(M_1,N)$$

(note the order inversion ; this is because $\mathrm{Hom}_A(-,N)$ is a **contravariant** functor, i.e. it reverses the order in which morphisms are composed). See Proposition 1.16 for proofs.

When ψ is a projection, we say that the above exact sequence **splits**. When applying $\mathrm{Hom}_A(N,-)$ or $\mathrm{Hom}_A(-,N)$ to split exact sequences, the resulting exact sequence is also split. One easily sees that when $N \le M$, N is a direct summand of M if and only if the identity map of M extends to a endomorphism $\pi \in \mathrm{End}_A(M)$ with $\operatorname{im}\pi = N$, in which case $M = N \oplus \ker\pi$.

Proposition 1.16. Let

$$0 \longrightarrow M_1 \xrightarrow{\varphi} M_2 \xrightarrow{\psi} M_3 \longrightarrow 0$$

be a sequence of left A-modules (not necessarily exact). The following are equivalent :

(i) The sequence above is right-exact

(ii) For all left A-modules N, the following sequence is exact :

$$0 \longrightarrow \mathrm{Hom}_A(M_3,N) \xrightarrow{\mathrm{Hom}_A(\varphi,N)} \mathrm{Hom}_A(M_2,N) \xrightarrow{\mathrm{Hom}_A(\psi,N)} \mathrm{Hom}_A(M_1,N)$$

Also, the following are equivalent :

(i) The above sequence is left-exact

(ii) For all left A-modules N, the following sequence is exact :

$$0 \longrightarrow \mathrm{Hom}_A(N,M_1) \xrightarrow{\mathrm{Hom}_A(N,\varphi)} \mathrm{Hom}_A(N,M_2) \xrightarrow{\mathrm{Hom}_A(N,\psi)} \mathrm{Hom}_A(N,M_3)$$

Proof. The fact that (i) implies (ii) is a consequence of the left-exactness of Hom and is proved in the same way as in the case of abelian groups, so is left as an exercise. Conversely, in the second case, we can take $N = A$ and notice that we have the natural isomorphism $\mathrm{Hom}_A(A, M_i) \simeq M_i$, so we recover the exactness required in (i).

In the first case, we have to work a bit more. Let $N \stackrel{\text{def}}{=} M_3/\mathrm{im}\,\psi$. The projection map $\pi : M_3 \to M_3/\mathrm{im}\,\psi$ is such that $\pi \circ \psi = 0$ by definition, but since $\pi \circ \psi = \mathrm{Hom}_A(\psi, N)(\pi) = 0$ and $\mathrm{Hom}_A(\psi, N)$ is injective, we get $\pi = 0$, i.e. $\mathrm{im}\,\psi = M_3$, which means ψ is surjective. Let $N = M_3$ and consider $\psi \in \mathrm{Hom}_A(M_2, N)$. Since $\mathrm{Hom}_A(\psi \circ \varphi, N) = \mathrm{Hom}_A(\psi, N) \circ \mathrm{Hom}_A(\varphi, N) = 0$ for all left A-modules N, we have $\psi \circ \varphi = 0$ (take $N = M_3$ and apply $\mathrm{Hom}_A(\psi \circ \varphi, N)$ to id_{M_3}), which implies $\mathrm{im}\,\varphi \subseteq \ker \psi$. Next, take $N \stackrel{\text{def}}{=} M_2/\mathrm{im}\,\varphi$. Since $\pi : M_2 \to M_2/\mathrm{im}\,\varphi$ lies in $\ker \mathrm{Hom}_A(\varphi, N) = \mathrm{im}\,\mathrm{Hom}_A(\psi, N)$, there exists $\nu : M_3 \to M_2/\mathrm{im}\,\varphi$ such that $\pi = \mathrm{Hom}_A(\psi, N)(\nu) = \nu \circ \psi$. Therefore, $\ker \psi \subseteq \ker(\nu \circ \psi) = \ker \pi = \mathrm{im}\,\varphi$, completing the proof.

Definition 1.17. Let A be a ring.

(i) An element $e \in A$ is called an **idempotent** if $e^2 = e$.

(ii) A family of idempotents $\{e_i\}_{i\in I}$ of A is called **orthogonal** if for any $i, j \in I$ distinct, we have $e_i e_j = 0$.

Corollary 1.18. Let A be a ring and M a left A-module. Consider a family of submodules $\{M_i\}_{i\in I}$ such that $\sum_{i\in I} M_i = M$. Then the following are equivalent :

(i) We have $M = \bigoplus_{i\in I} M_i$

(ii) Each M_i is a direct summand and the family of idempotents $\{\pi_i\}_{i\in I} \subseteq \mathrm{End}_A(M)$ is orthogonal.

Proof. Obvious.

Remark 1.19. The assumption that $\sum_{i\in I} M_i = M$ is not vital ; we can always add an element $*$ to the set I such that $M_* = \bigcap_{i\in I} \ker \pi_i$ and it follows that $M = \sum_{i\in I\cup\{*\}} M_i$. If M was already the direct sum of the M_i's, this does not change anything to the statement ; if it isn't, we have to replace (i) by the equality $M' \stackrel{\text{def}}{=} \sum_{i\in I} M_i = \bigoplus_{i\in I} M_i$ and the π_i by $\pi_i|_{M'}$, which shows that the $\pi_i|_{M'}$ form a family of orthogonal idempotents.

1.2 Centralizers and bicentralizers

Definition 1.20. Let A be a ring and $S \subseteq A$ be a subset. The **centralizer** of S in A is denoted by $C_A(S)$ and is defined as

$$C_A(S) \stackrel{\text{def}}{=} \{a \in A \mid \forall s \in S, \quad as = sa\}.$$

Note that by definition, $C_A(S)$ is a subring of A, so we can consider its **bicentralizer** $C_A^2(S) \stackrel{\text{def}}{=} C_A(C_A(S))$. The **center** of A is equal to its own centralizer and is denoted by

$$Z(A) \stackrel{\text{def}}{=} C_A(A) = \{z \in A \mid \forall a \in A, az = za\}.$$

We say that B is **commutative** if $B = Z(B)$ (in which case we resolve to the theory of commutative rings).

Remark 1.21. It might be tempting to define recursively the k^{th} centralizer by $C_A^k(S) \stackrel{\text{def}}{=} C_A(C_A^{k-1}(S))$, but this notion is pointless, as we can see right away. It is clear that $S \subseteq C_A^2(S)$ by definition (the elements of the centralizer commute with all elements of S, so the elements of S commute with the elements of the centralizer). Letting $C_A(S)$ play the role of S in the latter inclusion gives $C_A(S) \subseteq C_A^3(S)$. When $S \subseteq T \subseteq A$, we have $C_A(S) \supseteq C_A(T)$ (elements which commute with every element of T also commute with every element of S), therefore $S \subseteq C_A^2(S)$ implies $C_A(S) \supseteq C_A^3(S)$, which gives $C_A(S) = C_A^3(S)$. Therefore, the centralizer of the bicentralizer is the centralizer itself.

If $B \subseteq A$ is a subring, then $Z(B) = C_A(B) \cap B$. In particular, if B is commutative, then $B \subseteq C_A(B)$, thus $C_A^2(B) \subseteq C_A(B)$. It follows that

$$Z(C_A(B)) = C_{C_A(B)}(C_A(B)) = C_A(C_A(B)) \cap C_A(B) = C_A^2(B) \cap C_A(B).$$

One also sees that $C_A^2(A) = C_A(Z(A)) = A$ follows from the definition.

Definition 1.22. Let A be a commutative ring. An **associative A-algebra** is a ring B equipped with a morphism $\varphi : A \to B$, called the **structure map** of the algebra, such that $\operatorname{im} A \subseteq Z(B)$.

More generally, an A-algebra is defined as an A-bimodule B equipped with an A-bilinear map $(-,-) : B \times B \to B$; when this bilinear map satisfies $(a,1) = (1,a) = a$ and is associative (meaning that $(b_1,(b_2,b_3)) = ((b_1,b_2),b_3)$ for all $b_1,b_2,b_3 \in B$), we recover the notion of an associative A-algebra. In this document, all our A-algebras are associative unless otherwise mentioned, so we will call them A-algebras.

If B_1, B_2 are two A-algebras, since A is commutative, we can consider the tensor product $B_1 \otimes_A B_2$ which becomes a ring via the definition

$$(b_1 \otimes b_2)(b_1' \otimes b_2') \overset{\text{def}}{=} (b_1 b_1') \otimes (b_2 b_2')$$

which is extended by A-bilinearity to all of $B_1 \otimes_A B_2$. It canonically becomes an A-algebra via the morphism $A \to B_1 \otimes_A B_2$ defined by $a \mapsto a \otimes 1 = 1 \otimes a$.

An **A-subalgebra** of a A-algebra B is a subring $C \subseteq B$ such that the structure map $\varphi : A \to B$ of A satisfies $\varphi(A) \subseteq C$, in which case C becomes an A-algebra using the same structure map with codomain restricted to C since $\varphi(A) \subseteq Z(B) \cap C \subseteq Z(C)$.

Definition 1.23. A ring K in which for every $a \in A$, there exists a unique element $a^{-1} \in A$ satisfying $aa^{-1} = a^{-1}a = 1$, is called a **skew field** or a **division ring**. If K is commutative, we call K a **field**. When K is a field and A is a K-algebra, A is in particular a K-vector space and thus we can apply the techniques of linear algebra. One remark : since K has no nonzero ideals, a K-algebra always contains an isomorphic copy of K as a K-subalgebra, so we usually write $K \subseteq A$ with no regards to the structure map.

Proposition 1.24. Let K be a field and A, B be two K-algebras. If $A' \subseteq A$ and $B' \subseteq B$ are K-subalgebras, then $C_A(A')$ is a K-subalgebra of A, $C_B(B')$ is a K-subalgebra of B and

$$C_{A \otimes_K B}(A' \otimes_K B') = C_A(A') \otimes_K C_B(B').$$

As a corollary, $Z(A \otimes_K B) = Z(A) \otimes_K Z(B)$.

Proof. Since $A' \subseteq A$, we have $K \subseteq Z(A) = C_A(A) \subseteq C_A(A')$. Since $K \subseteq A' \subseteq C_A^2(A')$, we have $K \subseteq C_A(A') \cap C_A^2(A') = Z(C_A(A'))$ by Remark 1.21, hence $C_A(A')$ (and similarly $C_B(B')$) are K-subalgebras.

As for the equality, note that the inclusion ($\supseteq$) is clear. Consider the following direct sum decompositions

$$A = C_A(A') \oplus A'', \quad B = C_B(B') \oplus B''$$
$$\implies \quad A \otimes_K B = \Big(C_A(A') \otimes_K C_B(B') \Big) \oplus \Big((A'' \otimes_K C_B(B')) \oplus (C_A(A') \otimes_K B'') \oplus (A'' \otimes_K B'') \Big),$$

which shows that $C_A(A') \otimes_K C_B(B')$ is a direct summand of the K-vector space $A \otimes_K B$ and

$$C_A(A') \otimes_K C_B(B') = \Big(\big(A \otimes_K C_B(B')\big) \cap \big(C_A(A') \otimes_K B\big) \Big).$$

By the symmetry of our argument, it will suffice to show that $C_{A\otimes_K B}(A' \otimes_K B') \subseteq C_A(A') \otimes_K B$. Let $z = \sum_{i\in I}^{*} a_i \otimes b_i \in C_{A\otimes_K B}(A' \otimes_K B')$ where $a_i \in A$, $b_i \in B$. Without loss of generality, we can suppose that the b_i are linearly independent over K. For any $a \in A'$, we have

$$z(a \otimes 1) = (a \otimes 1)z \quad \implies \quad \sum_{i\in I} (a_i a - a a_i) \otimes b_i = 0.$$

Since the b_i are linearly independent, this means that $a_i a - a a_i = 0$ for all i, which means $a_i \in C_A(A')$, as desired.

Definition 1.25. Let A be a ring and M an A-module. The structure map $\varphi : A \to \mathrm{End}_{\mathbb{Z}}(M)$ is a morphism of rings, so let $A_M \overset{\text{def}}{=} \varphi(A)$, which is a subring of $\mathrm{End}_{\mathbb{Z}}(M)$. For each $a \in A$, we use the notation $a_M \overset{\text{def}}{=} \varphi_a \in A_M$. The map $\varphi : A \to A_M$ defined by $a \mapsto A_M$ is onto and A_M is called the **ring of homotheties of** M (its elements are called homotheties of M).

The **centralizer** and **bicentralizer** of M are defined as the centralizer/bicentralizer of A_M in $\mathrm{End}_{\mathbb{Z}}(M)$:

$$C_A(M) \overset{\text{def}}{=} C_{\mathrm{End}_{\mathbb{Z}}(M)}(A_M), \quad C_A^2(M) \overset{\text{def}}{=} C^2_{\mathrm{End}_{\mathbb{Z}}(M)}(A_M).$$

By definition, the centralizer of M is the endomorphism ring of the A-module M since

$$C_A(M) = \{\varphi \in \mathrm{End}_{\mathbb{Z}}(M) \mid \forall a \in A, \varphi a_M = a_M \varphi\} = \mathrm{End}_A(M).$$

The **countermodule**[1] of M, denoted by $M^{\triangleleft}$ is the abelian group M seen as a module over its centralizer, namely, the endomorphism ring $\mathrm{End}_A(M)$. Multiplication is defined the obvious way, namely if $\varphi \in \mathrm{End}_A(M)$ and $m \in M^{\triangleleft}$, we define $\varphi m \overset{\text{def}}{=} \varphi(m)$. Note that the A-module and $\mathrm{End}_A(M)$-module structures of M are compatible since $\varphi(am) = a\varphi(m)$ for all $a \in A$, $\varphi \in \mathrm{End}_A(M)$ and $m \in M$. We define the **double countermodule** of M, denoted by $M^{\triangleleft\triangleleft}$, as the countermodule of its countermodule, namely $M^{\triangleleft\triangleleft} \overset{\text{def}}{=} (M^{\triangleleft})^{\triangleleft}$.

Remark 1.26. Even when A is commutative, $C_A(M) = \mathrm{End}_A(M)$ is, in general, a noncommutative ring. Therefore, results that we build in this document here can also be useful for the theory of commutative rings, since considering only commutative rings prevents the study of noncommutative rings such as $\mathrm{End}_A(M)$.

Note that compatibility of module structures is not a transitive notion, i.e. if M is a left module over the three rings A, B, C, the module structures of A and B are compatible and the module structures of B and C are compatible, this does not mean that the structures of A and C are compatible. A particularly relevant example is that of the A-module, $C_A(M)$-module and $C_A^2(M)$-module structures on the A-module M. The first two and last two are compatible, but A and $C_A^2(M)$ give compatible structures on M if and only if $C_A^2(M) \subseteq C_A(M)$, which is not always the case (see Example 1.34).

[1]The French term for this is **contre-module**, but we have not found an English translation which is commonly used.

Definition 1.27. Let A be a ring. We have already seen that A can be interpreted as an A-bimodule over itself, but we can relax these assumptions and only consider the left A-module A, which we denote by A_ℓ. Equivalently, we can consider the right A-module A, which we denote by A_r.

Proposition 1.28. Let A be a ring.

(i) The centralizer of the left A-module A_ℓ is the opposite ring of homotheties of the right A-module A_r. In symbols,
$$C_A(A_\ell) = (A_{A_r})^{\text{opp}} = (A^{\text{opp}})_{(A^{\text{opp}})_\ell} \simeq A^{\text{opp}}.$$
This means that ${A_\ell}^\triangleleft$ is canonically a left A^{opp}-module. Namely, as left A^{opp}-modules, ${A_\ell}^\triangleleft \simeq (A^{\text{opp}})_\ell$.

(ii) The centralizer of the right A-module A_r is the opposite ring of homotheties of the left A-module A_ℓ. In symbols,
$$C_A(A_r) = (A_{A_\ell})^{\text{opp}} = (A^{\text{opp}})_{(A^{\text{opp}})_r} \simeq A^{\text{opp}}.$$
The same comments as in part (i) apply, i.e. ${A_r}^\triangleleft$ is a right A^{opp}-module satisfying ${A_r}^\triangleleft \simeq (A^{\text{opp}})_r$.

Proof. We begin by proving (i). If $\varphi \in \operatorname{End}_{\mathbb{Z}}(A_\ell) = \operatorname{End}_{\mathbb{Z}}((A^{\text{opp}})_r)$ commutes with a_{A_ℓ} for each $a \in A$, then
$$\varphi(a) = \varphi(a1) = (\varphi \circ a_{A_\ell})(1) = (a_{A_\ell} \circ \varphi)(1) = a\varphi(1),$$
so that φ corresponds to multiplication on the right by the element $\varphi(1)$. Conversely, any such endomorphism (of the form $a_{A_r^{\text{opp}}}$) belongs to $C_A(A_\ell)$ since multiplication on the left commutes with multiplication on the right ; this is associativity of multiplication. Therefore, $C_A(A_\ell)$ and $(A_{A_r})^{\text{opp}}$ are identified as abelian groups. As for multiplication, if $\psi, \varphi \in C_A(A_\ell)$, then
$$(\psi \circ \varphi)(a) = \psi(\varphi(a)) = \psi(a\varphi(1)) = a\varphi(1)\psi(1) = a(\psi(1)_{A_r} * \varphi(1)_{A_r}).$$
where $*$ stands for multiplication in $(A_{A_r})^{\text{opp}}$. Finally, we show that the identity map of A induces the isomorphism ${A_\ell}^\triangleleft \simeq (A^{\text{opp}})_\ell$. For $\varphi, \psi \in C_A(A_\ell)$, we have
$$(\psi \circ \varphi)(a) = a(\psi(1) * \varphi(1)) = \psi(1) * \varphi(1) * a.$$
The left-most term is the left $C_A(A_\ell)$-action on ${A_\ell}^\triangleleft$, and identifying the action of $C_A(A_\ell)$ with that of A^{opp} via the map $\varphi \mapsto \varphi(1)_{(A^{\text{opp}})_\ell}$, this completes the proof. (Note that $C_A(A_\ell)$ and $(A_{A_\ell})^{\text{opp}}$ are not just isomorphic, they are **equal** ; this is because they are defined as the same subsets of $\operatorname{End}_{\mathbb{Z}}(A)$.)

The statement of (ii) is proved along the lines of the proof of part (i), everything being written in reverse order.

Remark 1.29. The centralizer of a left A-module M is equal to the ring of homotheties of $M^\triangleleft$ (in symbols, $C_A(M) = C_A(M)_{M^\triangleleft}$). Since it is clear that $C_A(M)_{M^\triangleleft} \subseteq C_A(M)$, this is the statement that for $\varphi \in C_A(M) = C_{\operatorname{End}_{\mathbb{Z}}(M)}(A_M)$, as endomorphisms of M, we have $\varphi_{M^\triangleleft} = \varphi$. In other words, the map $\varphi \mapsto \varphi_M$ from $C_A(M)$ to $\operatorname{End}_{\mathbb{Z}}(M)$ is an injective morphism of rings. This is clear because the endomorphism of $M^\triangleleft$ which multiplies by φ_M is exactly φ. It follows that $C_A(M)_{M^\triangleleft} = C_A(M)$ and
$$C_A^2(M) = C^2_{\operatorname{End}_{\mathbb{Z}}(M)}(A_M) = C_{\operatorname{End}_{\mathbb{Z}}(M)}(C_{\operatorname{End}_{\mathbb{Z}}(M)}(A_M)) = C_{\operatorname{End}_{\mathbb{Z}}(M)}(C_A(M)_{M^\triangleleft}) = C_{C_A(M)}(M^\triangleleft),$$
thus
$$C_A^2(M) = C_{C_A(M)}(M^\triangleleft) = C_{C_A(M)}(M^\triangleleft)_{M^{\triangleleft\triangleleft}} = C_A^2(M)_{M^{\triangleleft\triangleleft}}.$$
This means that $C_A^2(M)$ is the ring of homotheties of the double countermodule $M^{\triangleleft\triangleleft}$ and the centralizer of $M^\triangleleft$. The latter can be re-written as $C_A^2(M) = \operatorname{End}_{\operatorname{End}_A(M)}(M^\triangleleft)$, but since for any $a \in A$, the endomorphism a_M is an $\operatorname{End}_A(M)$-linear map on $M^\triangleleft$ by definition of $\operatorname{End}_A(M)$, we obtain $A_M \subseteq C_A^2(M) = A_{M^{\triangleleft\triangleleft}}$. Also note that since $C_{\operatorname{End}_{\mathbb{Z}}(M)}(A_M) = C^3_{\operatorname{End}_{\mathbb{Z}}(M)}(A_M)$, the centralizer of $M^{\triangleleft\triangleleft}$ is just the centralizer of M, so that we do not speak of $M^{\triangleleft\triangleleft\triangleleft}$.

Corollary 1.30. Let A be a ring. We have

$$C_A^2(A_l) = A_{A_\ell}, \quad C_A^2(A_r) = A_{A_r}.$$

Proof. It suffices to prove that the first equality holds. By using Proposition 1.28 and Remark 1.29, we see that

$$C_A^2(A_\ell) = C_{A^{\mathrm{opp}}}(A_\ell{}^{\triangleleft}) = C_{A^{\mathrm{opp}}}((A^{\mathrm{opp}})_r) = A_{A_\ell}.$$

The proof of the second equality is done analogously.

Proposition 1.31. Let A be a ring and M a left A-module. Suppose $N \leq M$ is an A-submodule which is a direct summand.

(i) N is stable under $C_A^2(M)$, i.e. is also a submodule of $M^{\triangleleft\triangleleft}$. Letting N' be a complement for N, since N' is also a direct summand, it is also stable under $C_A^2(M)$, so N is also a direct summand of $M^{\triangleleft\triangleleft}$.

(ii) If N' is another direct summand of M, any A-linear map $\varphi : N \to N'$ is also $C_A^2(M)$-linear.

(iii) For every $\psi \in C_A^2(M)$, the restriction of ψ to N lies in $C_A^2(N)$, i.e. $\psi_M|_N = (\psi|_N)_N$. This implies that restriction to N is a morphism of rings $(-)|_N : C_A^2(M) \to C_A^2(N)$.

Proof. Let $\pi_N \in \mathrm{End}_A(M)$ be the projection of M onto N.

(i) For $\psi \in C_A^2(M)$, since elements of $C_A^2(M)$ commute with elements of $C_A(M) = \mathrm{End}_A(M)$ by definition, we see that

$$\psi(N) = \psi(\pi(M)) = \pi(\psi(M)) \subseteq \pi(M) = N.$$

(ii) Let $\varphi : N \to N'$ be an A-linear map. Then $\varphi \circ \pi_N \in \mathrm{End}_A(M) = C_A(M)$, so for $\psi \in C_A^2(M)$ and $n \in N$, we have

$$\varphi(\psi n) = ((\varphi \circ \pi_N) \circ \psi)(n) = (\psi \circ (\varphi \circ \pi_N))(n) = \psi(\varphi(n)).$$

(iii) Let $\psi \in C_A^2(M)$ and $\varphi \in C_A(N) = \mathrm{End}_A(N)$. By part (ii), if we set $N' = N$, we see that $\varphi \in \mathrm{End}_{C_A^2(M)}(N)$, which means that $\psi|_N \circ \varphi = \varphi \circ \psi|_N$ because ψ acts on N via $\psi|_N$. This implies $\psi|_N \in C_A^2(N)$, so we are done.

Definition 1.32. Let $\{A_i\}_{i\in I}$ be a family of rings. Their **product** is the ring $A \overset{\mathrm{def}}{=} \prod_{i\in I} A_i$ with addition and multiplication defined pointwise, so that its unit element is equal to $(1)_{i\in I}$. Given a family $\{M_i\}_{i\in I}$ where each M_i is a left A_i-module, the abelian group $\prod_{i\in I} M_i$ is a left $\prod_{i\in I} A_i$-module via

$$(a_i)_{i\in I}(m_i)_{i\in I} \overset{\mathrm{def}}{=} (a_i m_i)_{i\in I}.$$

Proposition 1.33. Let A_1, A_2 be rings and M_i be a left A_i-module, $i = 1, 2$. Then

$$C_{A_1\times A_2}(M_1 \times M_2) = C_{A_1}(M_1) \times C_{A_2}(M_2), \quad C^2_{A_1\times A_2}(M_1 \times M_2) = C^2_{A_1}(M_1) \times C^2_{A_2}(M_2).$$

Proof. The second equality follows from the first since the bicentralizer is the centralizer of the countermodule, hence

$$\begin{aligned} C^2_{A_1\times A_2}(M_1\times M_2) &= C_{C_{A_1\times A_2}(M_1\times M_2)}(M_1\times M_2) \\ &= C_{C_{A_1}(M_1)\times C_{A_2}(M_2)}(M_1\times M_2) \\ &= C_{C_{A_1}(M_1)}(M_1)\times C_{C_{A_2}(M_2)}(M_2) \\ &= C^2_{A_1}(M_1)\times C^2_{A_2}(M_2). \end{aligned}$$

For the first, note that

$$M_1\times M_2 = \underbrace{(M_1\times\{0\})}_{\overset{\text{def}}{=}M_1}\oplus\underbrace{(\{0\}\times M_2)}_{\overset{\text{def}}{=}M_2}.$$

The element $\varphi\in\operatorname{End}_{\mathbb{Z}}(M_1\times M_2)$ belongs in the set $C_{A_1\times A_2}(M_1\times M_2)$ if and only if for all $(a_1,a_2)\in A_1\times A_2$, we have $\varphi(a_1,a_2)_M=(a_1,a_2)_M\varphi$. Letting π_i be the projection onto M_i, $\varphi\in C_{A_1\times A_2}(M_1\times M_2)$ implies that $\pi_i\varphi\in C_{A_i}(M_i)$, so $\varphi=\pi_1\varphi+\pi_2\varphi\in C_{A_1}(M_1)\times C_{A_2}(M_2)$. The reverse inclusion is obvious, which proves equality.

Example 1.34. We give an example where the restriction morphism $(-)|_N : C^2_A(M)\to C^2_A(N)$ is neither injective or surjective. Consider a field K and the K-algebra $\operatorname{End}_K(K^3)$. After fixing the standard basis $\{e_1,e_2,e_3\}$, this is canonically isomorphic to the ring of 3×3 matrices with coefficients in K, which we denote by $\operatorname{Mat}_{3\times 3}(K)$. Consider the K-subalgebra A of matrices of the form

$$\begin{bmatrix} a & 0 & 0 \\ b & c & 0 \\ 0 & 0 & a \end{bmatrix}, \quad a,b,c\in K.$$

Considered as a left A-module, $M\overset{\text{def}}{=}K^3$ is the direct sum of the A-submodules $N\overset{\text{def}}{=}{}_K\langle e_1,e_2\rangle$ and $N'\overset{\text{def}}{=}{}_K\langle e_3\rangle$. Note that elements of $C_A(M)$ have to be K-linear maps since they have to commute with elements of the form λ_M for $\lambda\in K$. The condition that $\varphi\in\operatorname{End}_{\mathbb{Z}}(M)$ commutes with all matrices of the above form gives linear conditions on the coefficients of the matrix form, so solving for it tells us that the matrix form of φ over the basis $\{e_1,e_2,e_3\}$ is of the form

$$\begin{bmatrix} \alpha & 0 & 0 \\ 0 & \alpha & 0 \\ \beta & 0 & \gamma \end{bmatrix}$$

One sees that this ring is of the same form as A, where the roles of e_2 and e_3 have been permuted. It follows that $A=C^2_A(M)$. The map $(-)|_N : C^2_A(M)\to C^2_A(N)$ is injective since it can be written as

$$\begin{bmatrix} a & 0 & 0 \\ b & c & 0 \\ 0 & 0 & a \end{bmatrix}\longmapsto\begin{bmatrix} a & 0 \\ b & c \end{bmatrix}$$

However, one sees that $C_A(N)$ is the set of 2×2 scalar matrices, so $C^2_A(N)$ is the full ring of 2×2 matrices, which means that $(-)|_N$ is not surjective. Similarly, $C_A(N')=C^2_A(N')\simeq K$, so $(-)|_{N'}$ is surjective but not injective.

Note that $A\times A$ is a ring (its unit element is $(1,1)$). Consider the left $A\times A$-module $M\times M$ with action given by $(a_1,a_2)(m_1,m_2)\overset{\text{def}}{=}(a_1m_1,a_2m_2)$. The subset $N\times N'$ is a direct summand and by Proposition 1.33, we see that $C^2_{A\times A}(M\times M)=A\times A$ and $C_{A\times A}(N\times N')=C_A(N)\times C_A(N')$. The restriction map $(-)|_{N\times N'} : C^2_A(M)\times C^2_A(M)\to C^2_A(N)\times C^2_A(N')$ is neither injective or surjective since it is the product of the restriction maps $(-)|_N\times(-)|_{N'}$ on each component, the first not being surjective and the second not being injective.

Lemma 1.35. Let A be a ring, M a left A-module and N, P two A-submodules such that $M = N \oplus P$. Suppose that there exists two families of A-submodules $\{P_i\}_{i\in I}$ and $\{N_i\}_{i\in I}$ of P and N respectively, such that $P = \sum_{i\in I} P_i$ and $P_i \simeq N/N_i$.

(i) We have ${}_{C_A(M)}\langle N\rangle = M$.

(ii) The restriction morphism $(-)|_N : C_A^2(M) \to C_A^2(N)$ is injective.

(iii) If $A_N = C_A^2(N)$, then $A_M = C_A^2(M)$.

Proof. (i) This is clear since ${}_{C_A(M)}\langle N\rangle$ contains P_i by assumption ; just take the surjective map $N \to N/N_i \simeq P_i$ and lift it to an endomorphism of M to see that ${}_{C_A(M)}\langle N\rangle \supseteq P_i$, so that ${}_{C_A(M)}\langle N\rangle \supseteq P$.

(ii) Assume $\varphi \in C_A^2(M)$ satisfies $\varphi|_N = 0$. The composition

$$N \to N/N_i \simeq P_i \to P$$

is A-linear, thus $C_A^2(M)$-linear by Proposition 1.31 (ii). If $\varphi|_N = 0$, then $\varphi(P_i) = \varphi(N/N_i) = 0$, which means $\varphi(P) = \sum_{i\in I}\varphi(P_i) = 0$. This means $\varphi(M) = \varphi(N) + \varphi(P) = 0$, i.e. $\varphi = 0$, so $(-)|_N$ is injective.

(iii) Let $\varphi \in C_2^A(M)$. Since $A_N = C_A^2(N)$, there exists $a \in A$ such that $\varphi|_N = a_N$, i.e. $(\varphi - a_M)|_N = 0$. Since restriction to N is injective by part (ii), we see that $\varphi = a_M \in A_M$. Since $A_M \subseteq C_2^A(M)$, we are done.

Proposition 1.36. Let A be a ring and M a left A-module with an A-submodule such that $M \simeq A_\ell \oplus N$ (in other words, we assume that M admits a direct summand isomorphic to A_ℓ). Then $A_M = C_A^2(M)$.

Proof. Consider the restriction map $(-)_{A_\ell} : C_A^2(M) \to C_A^2(A_\ell)$. By Corollary 1.30, we have $C_A^2(A_\ell) = A_\ell$, so for any $\varphi \in C_A^2(M)$, we have $\varphi|_{A_\ell} = a_{A_\ell}$ for some $a \in A$. Each element $n \in N$ generates a left A-module ${}_A\langle n\rangle \simeq A_\ell/\mathfrak{a}_n$ where $\mathfrak{a}_n$ is some left ideal of A (namely, the ideal of all those $a \in A$ such that $an = 0$). It follows that the pair (A_ℓ, N) satisfies the hypotheses of Lemma 1.35, so $(-)|_{A_\ell}$ is injective, This means $\varphi = a_M$, so we're done.

Definition 1.37. Let A be a ring. A left (resp. right) A-module is said to be **free** if there exists an isomorphism $M \simeq \bigoplus_{i\in I} A_\ell$ (resp. $M \simeq \bigoplus_{i\in I} A_r$). When I is finite, we write $A_\ell^{\oplus n} \overset{\text{def}}{=} \bigoplus_{i\in I} A_\ell$ where $|I| = n$.

Corollary 1.38. Let A be a ring and M be a left A-module which admits a direct summand isomorphic to A_ℓ. Then $A_M = C_A^2(M)$ and

$$Z(\mathrm{End}_A(M)) = Z(A_M),$$

i.e. an element of the center of $\mathrm{End}_A(M)$ is equal to multiplication by some element of $Z(A_M)$. This holds in particular if M is a free left A-module. Furthermore, if A is commutative, $Z(\mathrm{End}_A(M)) = A_M$.

Proof. We have

$$\begin{aligned}
Z(\mathrm{End}_A(M)) &= C_{\mathrm{End}_{\mathbb{Z}}(M)}(\mathrm{End}_A(M)) \cap \mathrm{End}_A(M) \\
&= C_{\mathrm{End}_{\mathbb{Z}}(M)}(C_A(M)) \cap \mathrm{End}_A(M) \\
&= C_A^2(M) \cap \mathrm{End}_A(M) \\
&= A_M \cap \mathrm{End}_A(M) \\
&= Z(A_M).
\end{aligned}$$

The last equality is clear since saying that a_M is an A-linear map is exactly saying that it commutes with all other b_M for $b \in A$, i.e. lies in $Z(A_M)$.

Remark 1.39. We have $Z(A)_M \subseteq Z(A_M)$, but we don't have equality in general. The point is, two endomorphisms a_M and b_M may commute without a and b commuting in A.

Definition 1.40. Let A be a ring and M a left A-module. We say that M is **finitely generated** or is a **finite A-module** if there exists a surjective map $A_\ell^{\oplus n} \to M$ of left A-modules for some $n \geq 1$.

Corollary 1.41. Let A be a PID (note that principal ideal domains are assumed commutative by definition!) and M be a finitely generated left A-module. Then $A_M = C_A^2(M)$ and $Z(\mathrm{End}_A(M)) \simeq A/\mathrm{Ann}_A(M)$ (recall that $\mathrm{Ann}_A(M) = \ker(a \mapsto a_M)$).

Proof. By the classification of finitely generated modules over a PID, we have an isomorphism $M \simeq \bigoplus_{i=1}^n A/\mathfrak{a}_i$ where we can choose the ideals such that $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots \subseteq \mathfrak{a}_n$. It follows that $\mathrm{Ann}_A(M) = \mathfrak{a}_1$, so we can interpret M as an $A/\mathfrak{a}_1$-module. Without loss of generality, assume $\mathfrak{a}_1 = 0$. We can then apply Proposition 1.36 and Corollary 1.38.

Corollary 1.42. Let V be a finite-dimensional vector space over a field K and $\varphi_1, \varphi_2 \in \mathrm{End}_K(V)$. The following are equivalent :

(i) There exists a polynomial $p \in K[T]$ such that $p(\varphi_1) = \varphi_2$

(ii) For all $\psi \in \mathrm{End}_K(V)$ which commutes with φ_1, ψ commutes with φ_2.

Proof. Turn V into a $K[T]$-module V_{φ_1} by setting $pv \stackrel{\mathrm{def}}{=} p(\varphi_1)(v)$. The ring $\mathrm{End}_{K[T]}(V)$ equals the set of K-linear endomorphisms of V which commute with polynomials in φ_1 ; this is equivalent to commuting with φ_1. By Corollary 1.41, we have $K[T]_V/\mathrm{Ann}_{K[T]}(V) \simeq Z(\mathrm{End}_{K[T]}(V))$, so after translating both sides of this equality into the statements (i) and (ii), we are done.

1.3 Tensor products and Hom

For the rest of this chapter, A denotes a ring.

Definition 1.43. Let M be a right A-module and N be a left A-module. If L is an abelian group, a map $\varphi : M \times N \to L$ is called A-**balanced** if for any $m_1, m_2 \in M, n_1, n_2 \in N$ and $a \in A$, the following holds :

$$\begin{aligned}
\varphi(m_1 + m_2, n_1) &= \varphi(m_1, n_1) + \varphi(m_2, n_1) \\
\varphi(m_1, n_1 + n_2) &= \varphi(m_1, n_1) + \varphi(m_1, n_2) \\
\varphi(m_1 a, n_1) &= \varphi(m_1, a n_1).
\end{aligned}$$

In other words, it is a $\mathbb{Z}$-bilinear map for which the action of $a \in A$ can be done either on M or on N without changing the result of the application of φ.

The **tensor product** of M and N over A is the abelian group $M \otimes_A N$ defined as the quotient of the free abelian group $\mathbb{Z}^{\oplus(M \times N)}$ modulo the subgroup generated by the relations

$$\begin{gathered}(m_1 + m_2, n_1) - (m_1, n_1) - (m_2, n_1) \\ (m_1, n_1 + n_2) - (m_1, n_1) - (m_1, n_2) \\ (m_1 a, n_1) - (m_1, a n_1).\end{gathered}$$

The coset of the $\mathbb{Z}$-module basis element $(m, n) \in M \times N$ in $M \otimes_A N$ is denoted by $m \otimes n$. It comes with a canonical A-balanced map $\iota : M \times N \to M \otimes N$ given by $(m, n) \mapsto m \otimes n$.

Proposition 1.44. (Universal property of the tensor product) Let M be a right A-module, N a left A-module and L an abelian group. There is a canonical bijection

$$\{\varphi : M \times N \to L \mid \varphi \text{ is } A\text{-balanced}\} \longleftrightarrow \operatorname{Hom}_{\mathbb{Z}}(M \otimes_A N, L)$$

sending φ to $\widetilde{\varphi}$ in such a way that the following diagram commutes :

$$\begin{array}{ccc} M \times N & \xrightarrow{\ \iota\ } & M \otimes_A N \\ & \searrow^{\varphi} & \downarrow \widetilde{\varphi} \\ & & L \end{array}$$

| ***Proof.*** Obvious from our definition of $M \otimes_A N$. Details are left to the reader.

Remark 1.45. Since we have shown that $M \otimes_A N$ satisfies the above universal property, the pair $(M \otimes_A N, \iota)$ is unique up to a unique isomorphism making a commutative triangle with $M \times N$ as above.

More generally, if we assume additionally that we have rings B, C, that M is a left B-module, N a right C-module and L a (B, C)-bimodule, then $M \otimes_A N$ is a (B, C)-bimodule via

$$\forall b \in B, c \in C, m \in M, n \in N, \quad b(m \otimes n)c \overset{\text{def}}{=} bm \otimes nc$$

and the set of A-balanced maps $\varphi : M \times N \to L$ satisfying

$$\varphi(bm, nc) = b\varphi(m, n)c$$

are in bijection with $\operatorname{Hom}_{(B,C)}(M \otimes_A N, L)$. Even more generally, the module structures on M and N which are compatible with their respective A-module structures induce module structures on $M \otimes_A N$ (if the module structure on M is on the right or the structure on N is on the left, just replace it by the corresponding structure on the opposite ring and use the same construction).

Furthermore, the construction $(M, N) \mapsto M \otimes_A N$ gives a bifunctor $\otimes : \mathbf{Mod}\text{-}A \times A\text{-}\mathbf{Mod} \to \mathbf{Ab}$. If any of M or N admits module structures compatible with their A-module structure, $\otimes$ will also be functorial in the category of pairs of A-modules admitting those structures. Note that $\otimes$ is an additive functor in both of its arguments, meaning that if $f, f' \in \operatorname{End}_A(M)$ and $g, g' \in \operatorname{End}_A(N)$, then

$$(f + f') \otimes g = f \otimes g + f' \otimes g, \quad f \otimes (g + g') = f \otimes g + f \otimes g'.$$

Definition 1.46. Let A, B be rings and M, N be (A, B)-modules. The abelian group $\operatorname{Hom}_{(A,B)}(M, N)$ automatically becomes an $(\operatorname{End}_{(A,B)}(N), \operatorname{End}_{(A,B)}(M))$-bimodule via post-/pre-composition : for $(\varphi_B, \varphi_A) \in \operatorname{End}_B(N) \times \operatorname{End}_A(M)$, $f \in \operatorname{Hom}_{(A,B)}(M, N)$

$$\varphi_B f \varphi_A \overset{\text{def}}{=} \varphi_B \circ f \circ \varphi_A.$$

One easily checks that this is still a morphism of (A, B)-bimodules : for $(a, b) \in A \times B$ and $m \in M$,

$$(\varphi_B f \varphi_A)(amb) = (\varphi_B f)(a\varphi_A(m)b) = \varphi_B(a(f\varphi_A)(m)b) = a(\varphi_B f \varphi_A)(m)b.$$

Remark 1.47. When M, N are two left A-modules, we can define module structures on $\mathrm{Hom}_A(M,N)$ using module structures on M and N compatible with their A-module structures. For instance, if M is also a left C-module, N a left B-module and the structures are compatible, we can turn $\mathrm{Hom}_A(M,N)$ into a (B,C)-bimodule via

$$\forall m \in M, b \in B, c \in C, \quad (bfc)(m) \stackrel{\text{def}}{=} bf(cm).$$

This is possible because the compatibility condition is equivalent to asking that the endomorphisms c_M and b_N are A-linear, giving rise to morphisms of rings $C \to \mathrm{End}_A(M)$ and $B \to \mathrm{End}_A(N)$. The $(\mathrm{End}_A(N), \mathrm{End}_A(M))$-bimodule structure on $\mathrm{Hom}_A(M,N)$ can therefore be restricted to a (B,C)-bimodule structure.

We can also apply this technique if one of the module structures on M or N is a right module structure instead of a left one, as long as it is compatible with the left A-module structures on M or N ; it suffices to replace these right module structures by left module structures on the opposite ring. This is possible, in particular, when M is an (A,B)-bimodule and N a (A,C)-bimodule, making $\mathrm{Hom}_A(M,N)$ a (C,B)-bimodule via

$$\forall m \in M, b \in B, c \in C, \quad (cfb)(m) \stackrel{\text{def}}{=} f(mb)c.$$

Furthermore, the construction $(M,N) \mapsto \mathrm{Hom}_A(M,N)$ gives a bifunctor $\otimes : A\text{-}\mathbf{Mod}^{\mathrm{opp}} \times A\text{-}\mathbf{Mod} \to \mathbf{Ab}$. If any of M or N admits module structures compatible with their A-module structure, $\mathrm{Hom}_A(-,-)$ will also be functorial in the category of pairs of A-modules admitting those structures. By linearity of composition, $\mathrm{Hom}_A(-,-)$ is also additive in both of its arguments.

Lemma 1.48. Let $M, N, \{M_i\}_{i\in I}, \{N_i\}_{i\in I}$ be left A-modules. We have natural isomorphisms

$$\mathrm{Hom}_A(\bigoplus_{i\in I} M_i, N) \simeq \prod_{i\in I} \mathrm{Hom}_A(M_i, N), \quad \mathrm{Hom}_A(M, \prod_{i\in I} N_i) \simeq \prod_{i\in I} \mathrm{Hom}_A(M, N_i).$$

Proof. The first statement is equivalent to saying that a morphism of left A-modules $\varphi : M \to N$ is determined by its restrictions $\varphi|_{M_i} : M_i \to N$ since $\varphi = \bigoplus_{i\in I} \varphi|_{M_i}$. For the second one, letting $\pi_i : N \to N_i$ be the canonical projection, this is the fact that a morphism $\varphi : M \to N$ is determined by its components $\pi_i \circ \varphi : M \to N_i$.

Corollary 1.49. Let M, N be two left A-modules and assume $N = \bigoplus_{i\in I} N_i$ for a family $\{N_i\}_{i\in I}$ of submodules. If M is finitely generated, then the isomorphism

$$\mathrm{Hom}_A(M, \prod_{i\in I} N_i) \simeq \prod_{i\in I} \mathrm{Hom}_A(M, N_i)$$

restricts to the following isomorphism on the two following subsets :

$$\mathrm{Hom}_A(M, \bigoplus_{i\in I} N_i) \simeq \bigoplus_{i\in I} \mathrm{Hom}_A(M, N_i).$$

Proof. The isomorphism of Lemma 1.48 puts in correspondence a morphism $\varphi : M \to \bigoplus_{i\in I} N_i$ with its projections $\{\pi_i \circ \varphi\}_{i\in I}$. Since M is finitely generated, such a morphism φ is determined by the image of a subset $\{m_1, \cdots, m_k\}$. Because $\varphi(m_i) = \bigoplus_{i\in I} n_i$, only finitely many indices $i \in I$ contain non-zero components of the elements $\varphi(m_1), \cdots, \varphi(m_k)$. It follows that only finitely many of the maps $\pi_i \circ \varphi$ are non-zero. Conversely, if only $\pi_{i_1} \circ \varphi, \cdots, \pi_{i_s} \circ \varphi$ are non-zero, then the corresponding map $\varphi : M \to \prod_{i\in I} N_i$ satisfies $\varphi(M) \subseteq \sum_{j=1}^{s} N_{i_j}$, so $\varphi(M)$ lands inside N in a well-defined manner.

Theorem 1.50. (Tensor-hom adjunction) Let A, B be rings, M a right A-bimodule, N a (A, B)-bimodule and P a right B-bimodule. (It follows that $M \otimes_A N$ is a right B-module and $\mathrm{Hom}_B(N, P)$ is a right A-module.) There is a natural isomorphism of abelian groups

$$\mathrm{Hom}_B(M \otimes_A N, P) \simeq \mathrm{Hom}_A(M, \mathrm{Hom}_B(N, P)).$$

Moreover, this is an isomorphism of right $\mathrm{End}_A(M)$-modules, $\mathrm{End}_{(A,B)}(N)$-modules and $\mathrm{End}_B(P)$-modules. This implies that if C is a ring and any of M, N or P admit a C-module structure which is compatible with the module structures we already gave on that module, then both sides admit that corresponding C-module structure and the natural isomorphism above is an isomorphism of C-modules.

Proof. Working out the details is easy but long and pointless. Seeing the main idea is the most useful part. A morphism of right B-modules $\widetilde{\varphi} : M \otimes_A N \to P$ corresponds to an A-balanced map $\varphi : M \times N \to P$ for which the restriction $\varphi_m : N \to P$ given by $\varphi_m(n) = \varphi(m, n)$ is B-linear. The fact that it is A-balanced implies that for $a \in A$,

$$\varphi_{am}(n) = \varphi_m(an) = (\varphi_m a)(n)$$

by definition of the A-module structure on $\mathrm{Hom}_B(N, P)$, which means that the construction $m \mapsto \varphi_m$ is A-linear. This process can be reversed, thus gives the isomorphism. Naturality is obvious. The fact that this is an isomorphism of $\mathrm{End}_A(M)$-modules (resp. $\mathrm{End}_{(A,B)}(N)$, $\mathrm{End}_B(P)$) follows from the naturality of this isomorphism in all three arguments. Restricting this property to any subring of one of these three rings gives the statement about compatible module structures.

Theorem 1.51. Let M be a right A-module and N be a left A-module.

(i) The functor of left A-modules to abelian groups given by $N \mapsto M \otimes_A N$ is right-exact.

(ii) The functor of right A-modules to abelian groups $M \mapsto M \otimes_A N$ is right-exact.

Proof. Let P be a left A-module. Recall that $\mathrm{Hom}_A(N, P)$ is an (A, A)-bimodule since both N and P are left A-modules. Since M is a right A-module, the functor $\mathrm{Hom}_A(M, \mathrm{Hom}_A(-, P)) = \mathrm{Hom}_{\mathbb{Z}}(M, -) \circ \mathrm{Hom}_A(-, P)$ is a composition of left-exact functors, namely $\mathrm{Hom}_A(-, P) : A\text{-}\mathbf{Mod} \to A\text{-}\mathbf{Mod}\text{-}A$ and $\mathrm{Hom}_A(M, -)|_{A\text{-}\mathbf{Mod}\text{-}A} : A\text{-}\mathbf{Mod}\text{-}A \to A\text{-}\mathbf{Mod}\text{-}A$ (because both M and $\mathrm{Hom}_A(N, P)$ are right A-modules). The first functor sends a right-exact sequence to a left-exact one, and the second functor preserves left-exact sequences. Therefore, the composition is a contravariant functor mapping a right-exact sequence to a left-exact one and it is naturally isomorphic to $\mathrm{Hom}_A(M \otimes_A -, P)$ by Theorem 1.50. Since the latter is exact for all left A-modules P, it follows that the functor $M \otimes_A -$ is right-exact by Proposition 1.16 since the functor $\mathrm{Hom}_A(-, P)$ is contravariant. This proves part (i).

For part (ii), note that the functor $\mathrm{Hom}_A(-, \mathrm{Hom}_A(N, P))$ is contravariant left-exact for all left A-modules N,P and it is naturally isomorphic to $\mathrm{Hom}_A(- \otimes_A N, P)$. Since the latter is left-exact for all P, the functor $- \otimes_A N$ is right-exact.

Definition 1.52. Let $M_0, \cdots, M_n$ be abelian groups and $A_1, \cdots, A_n$ be rings with the following relations :

(i) M_0 is a right A_1-module

(ii) M_n is a left A_n-module

(iii) For each $1 \leq i \leq n-1$, M_i is a (A_i, A_{i+1})-bimodule.

Then we can form the abelian group

$$M_0 \otimes_{A_1} M_1 \otimes_{A_2} M_2 \otimes_{A_2} \cdots \otimes_{A_n} M_n$$

as follows. Consider the free abelian group $\mathbb{Z}^{\oplus \prod_{i=0}^n M_i}$ on the set $n+1$-tuples $(m_0, \cdots, m_n) \in \prod_{i=0}^n M_i$. Quotient out by the submodule generated by the relations

$$(m_0, \cdots, m_i, \cdots, m_n) + (m_0, \cdots, m_i', \cdots, m_n) - (m_0, \cdots, m_i + m_i', \cdots, m_n)$$
$$(m_0, \cdots, m_i a_i, m_{i+1}, \cdots, m_n) - (m_0, \cdots, m_i, a_i m_{i+1}, \cdots, m_n).$$

This gives us the abelian group. It is a bimodule for each ring A_i by allowing multiplication on the M_{i-1}-factor on the right and on the M_i-factor on the left. If A_0 (resp. A_{n+1}) is a ring and M_0 is a left A_0-module (resp. if M_n is a right A_{n+1}-module), then the corresponding tensor product also admits this structure.

Proposition 1.53. (Associativity of the tensor product) Let A_0, A_1, A_2, A_3 be rings, M_0 a (A_0, A_1)-bimodule, M_1 a (A_1, A_2)-bimodule and M_2 a (A_2, A_3)-bimodule. We have two isomorphism of abelian groups which is simultaneously an isomorphism of A_0, A_1, A_2 and A_3-bimodules :

$$M_0 \otimes_{A_1} (M_1 \otimes_{A_2} M_2) \simeq M_0 \otimes_{A_1} M_1 \otimes_{A_2} M_2 \simeq (M_0 \otimes_{A_1} M_1) \otimes_{A_2} M_2.$$

Proof. It suffices to see that the correspondences

$$m_0 \otimes (m_1 \otimes m_2) \longleftrightarrow m_0 \otimes m_1 \otimes m_2 \longleftrightarrow (m_0 \otimes m_1) \otimes m_2$$

produce well-defined maps in each direction and they are inverse to each other, as can be seen when applied on the generators of the respective modules given above.

Proposition 1.54. (Tensor product with respect to $^{\mathrm{opp}}$) Given a left (resp. right) A-module M, recall Remark 1.6 for the definition of the opposite module structure M^{opp} on its opposite ring A^{opp}. Let M_0 be an (A_0, A_1)-bimodule and M_1 be an (A_1, A_2)-bimodule. We have an isomorphism of $(A_2^{\mathrm{opp}}, A_0^{\mathrm{opp}})$-bimodules

$$(M_0 \otimes_{A_1} M_1)^{\mathrm{opp}} \simeq M_1^{\mathrm{opp}} \otimes_{A_1^{\mathrm{opp}}} M_0^{\mathrm{opp}}.$$

In particular, if A_0, A_1, A_2 are commutative rings, the tensor product is commutative up to the natural isomorphism given in the proof.

Proof. Given $m \in M_0$, write $m^{\mathrm{opp}} \in M_0^{\mathrm{opp}}$ for the same element but which gets affected by multiplication from the opposite side in the reversed order. It suffices to map $(m_0 \otimes m_1)^{\mathrm{opp}}$ to $m_1^{\mathrm{opp}} \otimes m_0^{\mathrm{opp}}$. The $(A_2^{\mathrm{opp}}, A_0^{\mathrm{opp}})$-linearity becomes obvious since for $a_2 \in A_2$, $m_0 \in M_0$ and $m_1 \in M_1$, denoting the opposite multiplication with the symbol $*$, we have

$$a_2 * (m_0 \otimes m_1)^{\mathrm{opp}} = (m_0 \otimes m_1 a_2)^{\mathrm{opp}} \mapsto (m_1 a_2)^{\mathrm{opp}} \otimes m_0^{\mathrm{opp}} = a_2 * m_1^{\mathrm{opp}} \otimes m_0^{\mathrm{opp}}.$$

The argument is similar for $a_0 \in A_0$.

1.4 Isotypical modules

Isotypical modules are to be seen as generalizations of free modules over a ring. We will see their importance in Theorem 1.59, where we establish a correspondence between the free modules over $\mathrm{End}_A(M) = C_A(M)$ and the isotypical modules of type M.

Definition 1.55. Let M, N be two left A-modules. We say that M is **isotypical of type** N if $M \simeq \bigoplus_{i \in I} N_i$ where $N_i \simeq N$. When this is the case, we write $M \simeq N^{\oplus I}$.

Proposition 1.56. Let M be an isotypical A-module of type N.

(i) The restriction map $(-)|_N : C_A^2(M) \to C_A^2(N)$ is an isomorphism.

(ii) The $C_A^2(M)$-module M is also isotypical of type N when N is seen as a $C_A^2(M)$-module via its $C_A^2(N)$-module structure and the isomorphism $(-)|_N : C_A^2(M) \simeq C_A^2(N)$ given in part (i).

Proof. By Proposition 1.31 (ii) and Lemma 1.35 (ii), we know that $(-)|_N$ is injective and that the direct summands isomorphic to N in (ii) are isomorphic as $C_A^2(M)$-modules. It only remains to show that $(-)|_N$ is surjective.

Let $\varphi \in C_A^2(N)$, and let $\psi \stackrel{\text{def}}{=} \varphi^{\oplus I} \in \operatorname{End}_{\mathbb{Z}}(M)$, so that whenever $m \in N_i = N$, we have $\psi(m) = \varphi(m) \subseteq N_i$. It is clear that $\psi|_N = \varphi$, so we only need to show that $\psi \in C_A^2(M)$. Let $\alpha \in C_A(M)$ and $m \in N_i$ for some $i \in I$. Denote the projection of M onto N_i by π_i. Note that $\pi_i\alpha$ is an A-linear endomorphism of N_i, thus commutes with φ. Therefore,

$$(\alpha\psi)(m) = \sum_{i\in I} (\pi_i\alpha\psi)(m) = \sum_{i\in I} (\pi_i\alpha)(\varphi(m)) = \sum_{i\in I} \varphi((\pi_i\alpha)(m)) = \psi\left(\sum_{i\in I} (\pi_i\alpha)(m)\right) = (\psi\alpha)(m).$$

By linearity, we obtain $\alpha\psi = \psi\alpha$, which completes the proof.

Remark 1.57. We had already proved Proposition 1.56 in the case where $F = A_\ell$, so this is a generalization from the case of free A-modules to the case of isotypical A-modules.

Theorem 1.58. Let M be a left A-module. Since the A-module structure and $C_A(M)$-module structures on M are compatible by definition, when V is a left A-module and W is a right $C_A(M)$-module, we can define

$$S(W) \stackrel{\text{def}}{=} W \otimes_{C_A(M)} M, \quad T(V) \stackrel{\text{def}}{=} \operatorname{Hom}_A(M, V).$$

By the constructions of Section 1.3, $S(W)$ is canonically a left A-module and $T(V)$ is canonically a right $C_A(M)$-module, which gives a canonical isomorphism

$$\operatorname{Hom}_A(S(W), V) \simeq \operatorname{Hom}_{C_A(M)}(W, T(V)).$$

The functors S and T are therefore adjoint functors. We can describe the unit and counit of this adjunction explicitly as follows :

$$\varepsilon_V : S(T(V)) = \operatorname{Hom}_A(M, V) \otimes_{C_A(M)} M \to V, \quad \varepsilon_V(\varphi \otimes m) \mapsto \varphi(m)$$

and

$$\eta_W : W \to T(S(W)) = \operatorname{Hom}_A(M, W \otimes_{C_A(M)} M), \quad \eta_W(w)(m) = w \otimes m.$$

The morphism ε_V is a morphism of A-modules and η_W is a morphism of $C_A(M)$-modules.

Proof. We can apply Theorem 1.50 directly. One needs to see M and W as right A^{opp}-modules instead of left A-modules so that the statement applies accordingly to the notation given there, but this makes literally no difference in the result.

Theorem 1.59. Let M be a finitely generated left A-module, V a left A-module isotypical of type M and W a free right $C_A(M)$-module.

(i) The left A-module $S(W)$ is isotypical of type M. More explicitly, for any $C_A(M)$-basis $\{w_i\}_{i\in I}$ of W, the submodules $S_i \stackrel{\text{def}}{=} \langle w_i \rangle_{C_A(M)} \otimes M$ satisfy $S(W) = \bigoplus_{i\in I} S_i$.

(ii) The morphism $\eta_W : W \to \mathrm{Hom}_A(M, W \otimes_{C_A(M)} M)$ is an isomorphism of $C_A(M)$-modules.

(iii) If W' is another right $C_A(M)$-module, the morphism of abelian groups

$$S : \mathrm{Hom}_{C_A(M)}(W', W) \to \mathrm{Hom}_A(S(W'), S(W))$$

is an isomorphism.

(iv) Write $V = \bigoplus_{i\in I} V_i$ where $\iota_i : M \to V$ is the isomorphism onto V_i. Then $T(V) = \mathrm{Hom}_A(M, V)$ is a free right $C_A(M)$-module with basis $\{\iota_i\}_{i\in I}$.

(v) The morphism $\varepsilon_V : S(T(V)) = \mathrm{Hom}_A(M, V) \otimes_{C_A(M)} M \to V$ is an isomorphism of A-modules.

(vi) If V' is another left A-module, the morphism of abelian groups

$$T : \mathrm{Hom}_A(V, V') \to \mathrm{Hom}_{C_A(M)}(T(V), T(V'))$$

is an isomorphism.

Proof. (i) Writing $W = C_A(M)^{\oplus I}$, we obtain

$$S(W) = W \otimes_{C_A(M)} M \simeq (C_A(M)^{\oplus I}) \otimes_{C_A(M)} M \simeq (C_A(M) \otimes_{C_A(M)} M)^{\oplus I} \simeq M^{\oplus I}.$$

A choice of basis corresponds to an isomorphism $W \simeq C_A(M)^{\oplus I}$, which explains the second statement.

(ii) The morphism η_W commutes with the following isomorphisms since $C_A(M) = \mathrm{Hom}_A(M, M)$:

$$W \simeq \mathrm{Hom}_A(M, M)^{\oplus I} \simeq \mathrm{Hom}_A(M, M^{\oplus I}) \simeq \mathrm{Hom}_A(M, W \otimes_{C_A(M)} M) = S(T(W)).$$

(iii) Because S and $\mathrm{Hom}_{C_A(M)}(W', -)$ commute with direct sums, it suffices to show that

$$\mathrm{Hom}_{C_A(M)}(W', \mathrm{Hom}_A(M, M)) = \mathrm{Hom}_{C_A(M)}(W', C_A(M)) \simeq \mathrm{Hom}_A(W' \otimes_{C_A(M)} M, M),$$

which is precisely the statement of the tensor-hom adjunction.

(iv) Without loss of generality, write $V = M^{\oplus I}$. It follows that

$$T(V) = \mathrm{Hom}_A(M, M^{\oplus I}) \simeq \mathrm{Hom}_A(M, M)^{\oplus I} \simeq C_A(M)^{\oplus I}$$

is a free right $C_A(M)$-module.

(v) Letting $V = M^{\oplus I}$, the morphism ε_V commutes with the isomorphism

$$\mathrm{Hom}_A(M, V) \otimes_{C_A(M)} M \simeq C_A(M)^{\oplus I} \otimes_{C_A(M)} M \simeq C_A(M)^{\oplus I} \otimes_{C_A(M)} M \simeq M^{\oplus I} = V.$$

(vi) Because T and $\mathrm{Hom}_A(-, V')$ commutes with direct sums, it suffces to show that

$$\mathrm{Hom}_A(M, V') \simeq \mathrm{Hom}_{C_A(M)}(\mathrm{Hom}_A(M, M), \mathrm{Hom}_A(M, V')) =\simeq \mathrm{Hom}_{C_A(M)}(C_A(M), \mathrm{Hom}_A(M, V')),$$

which is clear ; the isomorphism from right to left is given by evaluation of a $C_A(M)$-linear map $\varphi : C_A(M) \to \mathrm{Hom}_A(M, V')$ at $1 \in C_A(M)$, i.e. $\varphi \mapsto \varphi(1)$.

Corollary 1.60. Let M be a finitely generated left A-module, V a left A-module isotypical of type M and W a free right $C_A(M)$-module.

(i) The map $f \mapsto S(f)$ induces an isomorphism of rings

$$\mathrm{End}_{C_A(M)}(W) \simeq \mathrm{End}_A(S(W)) = \mathrm{End}_A(W \otimes_{C_A(M)} M).$$

(ii) The map $g \mapsto T(g)$ induces an isomorphism of rings

$$\mathrm{End}_A(V) \simeq \mathrm{End}_{C_A(M)}(T(V)) = \mathrm{End}_{C_A(M)}(\mathrm{Hom}_A(M, V)).$$

(iii) There is a one-to-one correspondence between the A-submodules $V' \leq V$ which are direct summands of V isotypical of type M and the free right $C_A(M)$-submodules $W' \leq W$ which are direct summands of W via the formulas

$$V' \mapsto T(V'), \quad W' \mapsto S(W').$$

Proof. Part (i) is obtained by setting $W' = W$ in Theorem 1.59 (iii) and part (ii) is obtained by setting $V' = V$ in Theorem 1.59 (vi). This argument makes them isomorphisms of abelian groups ; functoriality of this isomorphism in the general case makes it an isomorphism of rings. Part (iii) follows from parts (i) and (ii) since the ring isomorphisms given there map projections to projections.

Chapter 2

Finiteness conditions on rings and modules

In this chapter, A denotes a ring. The three conditions we will study are the properties of being artinian, noetherian and of finite length ; these apply to both modules and rings.

2.1 Artinian, noetherian and finite length modules

Definition 2.1. Let M be a left A-module.

(i) We say that M is **artinian** if it satisfies one of the following equivalent conditions :

- Every non-empty subset of submodules of M possesses a minimal element
- Every countable descending chain $M_1 \supseteq M_2 \supseteq \cdots \supseteq M_n \supseteq \cdots$ of submodules of M **stabilizes**, which means there exists $n \geq 1$ such that for all $n' \geq n$, $M_{n'} = M_n$.

(ii) We say that M is **noetherian** if it satisfies one of the following equivalent conditions :

- Every non-empty subset of submodules of M possesses a maximal element
- Every countable ascending chain $M_1 \subseteq M_2 \subseteq \cdots \subseteq M_n \subseteq \cdots$ of submodules of M **stabilizes**, which means there exists $n \geq 1$ such that for all $n' \geq n$, $M_{n'} = M_n$.

The equivalence between those two definitions is clear by using Zorn's Lemma. Note that M is an artinian (resp. a noetherian) left A-module if and only if it is artinian (resp. noetherian) as a left A_M-module.

Example 2.2. (i) If K is a field and V is a finite-dimensional vector space over K, then V is artinian and noetherian because given a chain of subspaces, the dimension of each member of the chain tells us when the chain stops.

(ii) Let $\{M_i\}_{i \in I}$ be an infinite family of non-zero left A-modules and consider $M \overset{\text{def}}{=} \bigoplus_{i \in I}$. Then M is neither artinian or noetherian. It suffices to give a total order on I and consider the chain of submodules $M_i' \overset{\text{def}}{=} \sum_{j \leq i} M_j$ (resp. $M_i'' \overset{\text{def}}{=} \sum_{j \geq i} M_j$).

Proposition 2.3. Let M be a noetherian left A-module. If $S \subseteq M$ is such that ${}_A\langle S \rangle = M$, there exists $n \geq 1$ and $s_1, \cdots, s_n \in S$ such that ${}_A\langle s_1, \cdots, s_n \rangle = M$. In particular, every noetherian left A-module is finitely generated.

Proof. Without loss of generality, assume S is infinite. Let $\{M_T\}_{T \subseteq S}$ be the set of submodules given by $M_T \overset{\text{def}}{=} {}_A\langle T \rangle$ where T is assumed finite. This collection is not empty, so let M_{T_0} be a maximal element.

For any $s \in S$, $M_{T_0 \cup \{s\}} \subseteq M_{T_0} \subseteq M_{T_0} + {}_A\langle s \rangle = M_{T_0 \cup \{s\}}$, which means $s \in M_{T_0}$. Therefore $S \subseteq M_{T_0}$, which implies $M_{T_0} = M$.

Since $S = M$ generates M, this implies M is finitely generated.

Proposition 2.4. Let M be a left A-module. The following are equivalent :

(i) M is noetherian

(ii) Every A-submodule $M' \leq M$ is finitely generated.

Since the condition (ii) is inherited from M to any of its submodules, it follows that every submodule of a noetherian A-module is noetherian.

Proof. ((i) $\Rightarrow$ (ii)) By definition, a chain of submodules of M' is also a chain of submodules of M, so M' is noetherian, hence finitely generated by Proposition 2.3.

((ii) $\Rightarrow$ (i)) Suppose we are given a chain $M_1 \subseteq M_2 \subseteq \cdots \subseteq M_n \subseteq \cdots$ of submodules of M. Let $M' \stackrel{\text{def}}{=} \bigcup_{n \geq 1} M_n$. Since M' is finitely generated, its generators all lie in M_n for some $n \geq 1$, meaning that $M_n = M_{n+1} = \cdots = M'$. It follows that M is noetherian.

Proposition 2.5. Consider the following exact sequence of left A-modules :

$$0 \longrightarrow N \xrightarrow{\iota_N} M \xrightarrow{\pi_N} M/N \longrightarrow 0$$

(i) M is artinian if and only if N and M/N are artinian.

(ii) M is noetherian if and only if N and M/N are noetherian.

Proof. We begin with (i).

($\Rightarrow$) If $\{N_i\}_{i \in \mathbb{N}}$ is a decreasing chain of submodules of N, then $\{\iota_N(N_i)\}_{i \in I}$ is a decreasing chain of submodules of M, so it stabilizes ; since ι_N is injective, our original chain stabilizes, so N is artinian. Similarly, if $\{P_i\}_{i \in \mathbb{N}}$ is a decreasing chain of submodules of M/N, then $\{\pi_N^{-1}(P_i)\}_{i \in I}$ is a decreasing chain of submodules of M, hence stabilizes ; since π_N is surjective, $P_i = \pi_N(\pi_N^{-1}(P_i))$, so our original chain stabilizes and M/N is artinian.

($\Leftarrow$) Let $\{M_i\}_{i \in I}$ be a decreasing chain of submodules of M/N. The projections $\{\pi_N(M_i)\}_{i \in I}$ form a chain in the artinian module M/N, thus stabilizes. Therefore, there exists $n_1 \geq 1$ such that $M_i + N = M_{n_1} + N$ for all $i \geq n_1$. The restrictions $\{\iota_N^{-1}(M_i)\}_{i \in \mathbb{N}}$ form a chain in the artinian module N, thus also stabilizes, which means there exists $n_2 \geq 1$ with $M_i \cap N = M_{n_2} \cap N$ for all $i \geq n_2$. Letting $n \stackrel{\text{def}}{=} \max\{n_1, n_2\}$, we see that $M_i + N = M_n + N$ and $M_i \cap N = M_n \cap N$. It follows that $M_i = M_n$ since $M_i \subseteq M_n + N$ but $m \in M_i \cap (M_n + N \setminus M_n)$ is impossible since then $m \in M_i \cap N$; this gives $M_i \subseteq M_n$, and the symmetry of the argument gives equality. In other words, M is artinian.

The proof in the noetherian case is the same ; just replace the words "artinian" by "noetherian" and the words "decreasing chain" by "increasing chain".

Corollary 2.6. A finite direct sum of artinian (resp. noetherian) left A-modules is artinian (resp. noetherian).

Proof. By induction on the number of modules considered. If $M_1, \cdots, M_n$ are artinian (resp. noetherian), let $M \stackrel{\text{def}}{=} \bigoplus_{i=1}^n M_i$ and $M' \stackrel{\text{def}}{=} \bigoplus_{i=1}^{n-1}$. By assumption, M' and M_n are artinian (resp. noetherian), hence so is M by considering the split exact sequence involving those three.

Definition 2.7. Let M be a left A-module.

(i) The module M is called **simple** if it is nonzero and its set of submodules equals $\{0, M\}$.

(ii) Given a left A-module M and a left ideal $\mathfrak{a} \trianglelefteq A$, we let

$$\mathfrak{a}M \stackrel{\text{def}}{=} \left\{ \sum_{i=1}^n a_i m_i \,\middle|\, n \geq 1, \quad a_i \in \mathfrak{a}, \quad m_i \in M \right\}.$$

The **annihilator of a module** M is the kernel of the map $A_M \to \mathrm{End}_A(M)$, i.e.

$$\mathrm{Ann}_A(N) \stackrel{\text{def}}{=} \{a \in A \mid a_M = 0\}.$$

If $m \in M$, we also define the **annihilator of** m as the annihilator of ${}_A\langle m \rangle$, namely the set of $a \in A$ such that $am = 0$. A left A-module M for which $\mathrm{Ann}_A(M) = 0$ is said to be **faithful**.

(iii) An element $a \in A$ is called **nilpotent** if $a^n = 0$ for some $n \geq 1$; the set of nilpotent elements in A is denoted by $\mathrm{Nil}(A)$. Note that in contrast with the case of commutative rings, $\mathrm{Nil}(A)$ is not an ideal since it is not even a subgroup of A in general! This can be seen by the example of the ring $\mathrm{Mat}_{2\times 2}(A)$ and the equation

$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$

where the two matrices we are adding square to zero but their sum squares to the identity matrix.

(iv) A left ideal $\mathfrak{a} \trianglelefteq A$ is called a **nilideal** if $\mathfrak{a} \subseteq \mathrm{Nil}(A)$.

(v) The (left)**Jacobson radical** is the intersection of all left maximal ideals of A. We denote it by $\mathrm{Jac}(A)$.

Proposition 2.8. Let A be a ring. The following conditions on $a \in A$ are equivalent :

(i) $a \in \mathrm{Jac}(A)$

(ii) $1 - xa$ admits a left inverse for all $x \in A$

(iii) For every simple left A-module M, we have $a \in \mathrm{Ann}_A(M)$, i.e. $am = 0$ for all $m \in M$.

Proof. ((i) $\Rightarrow$ (ii)) Let $a \in \mathrm{Jac}(A)$ and $x \in A$. Repeating the argument of Krull's theorem in the non-commutative case, if $1 - xa$ does not have a left inverse, the left ideal ${}_A\langle 1 - xa \rangle \trianglelefteq A$ is proper, hence Zorn's Lemma implies that ${}_A\langle 1 - xa \rangle$ is contained in some left maximal ideal $\mathfrak{m} \trianglelefteq A$. But then $1 - xa, xa \in \mathfrak{m}$, hence $1 = (1 - xa) + xa \in \mathfrak{m}$, a contradiction.

((ii) $\Rightarrow$ (iii)) Suppose M is a simple left A-module and there exists $m \in M$ with $am \neq 0$. Since M is simple, aM being a left A-submodule of M, we have $aM = M$. In particular, there exists $x \in A$ with $x(am) = m$, e.g. $(1-xa)m = 0$. Since $1-xa$ admits a left inverse z, we have $m = z((1-xa)m) = 0$.

((iii) $\Rightarrow$ (i)) Let $\mathfrak{m} \trianglelefteq A$ be a left maximal ideal. Then $A/\mathfrak{m}$ is a simple left A-module, hence $a \in \mathrm{Ann}_A(A/\mathfrak{m}) = \mathfrak{m}$. Taking the intersection over all left maximal ideals $\mathfrak{m}$, we obtain $a \in \mathrm{Jac}(A)$.

Theorem 2.9. (Nakayama's Lemma) Let M be a finitely generated left A-module. If $\mathrm{Jac}(A)M = M$, then $M = 0$.

Proof. Suppose $M \neq 0$ and let $\{m_1, \cdots, m_n\}$ be a set of generators where $n > 0$ is chosen minimal. Write

$$m_1 = a_1 m_1 + \cdots + a_n m_n, \quad a_i \in \mathrm{Jac}(A).$$

We can re-write this as

$$(1 - a_1)m_1 = a_2 m_2 + \cdots + a_n m_n.$$

Since $(1 - a_1)$ admits a left-inverse, we see that $m_1 \in \langle m_2, \cdots, m_n \rangle_A$, hence $\{m_2, \cdots, m_n\}$ is also a set of generators for M. This contradicts the minimality of n, therefore we must have $n = 0$, i.e. $M = 0$.

Proposition 2.10. Let A be a ring. If $\mathfrak{a} \trianglelefteq A$ is a nilideal, then $\mathfrak{a} \subseteq \mathrm{Jac}(A)$.

Proof. Let $\mathfrak{a} \trianglelefteq A$ be a nilideal and pick $a \in \mathfrak{a}$. For $x \in A$, since $xa \in \mathfrak{a}$ is nilpotent, we have $(xa)^n = 0$ for some $n \geq 1$. Therefore

$$\left(\sum_{i=0}^{n-1} (xa)^i \right) (1 - xa) = 1 - (xa)^n = 1,$$

showing that $1 - xa$ has a left-inverse for all $x \in A$. This means $a \in \mathrm{Jac}(A)$ by Proposition 2.8.

Proposition 2.11. Let K be a field and A a K-algebra. If A is a finite-dimensional K-vector space, then there exists $n \geq 1$ such that $\mathrm{Jac}(A)^n = 0$.

Proof. Since the sequence $\mathrm{Jac}(A) \supseteq \mathrm{Jac}(A)^2 \supseteq \cdots$ is a decreasing sequence of finite-dimensional K-vector subspaces of A, the sequence eventually becomes stationary, so there exists $n \geq 1$ such that $\mathrm{Jac}(A)^n = \mathrm{Jac}(A)^{n+1} = \mathrm{Jac}(A)\mathrm{Jac}(A)^n$. By Nakayama's Lemma, $\mathrm{Jac}(A)^n = 0$.

The next part of this preliminary section is needed to prove the existence of a Jordan-Hölder series of a left A-module of finite length, which is a necessary tool to work with simple subquotients of a module of finite length.

Lemma 2.12. Let M a left A-module and $F, E, U \subseteq M$ be A-submodules. Suppose $F \subseteq E$. Then $(E \cap U) + F = E \cap (U + F)$.

Proof. We have $(E \cap U) + F = (E \cap U) + (E \cap F) = E \cap (U + F)$.

We see that

$$F \subseteq (E \cap U) + F = E \cap (U + F) \subseteq E,$$

so that in some way we inserted U in between E and F. We call the module $(E \cap U) + F = E \cap (U + F)$ the **insertion** of U between E and F, and we denote it by $\mathrm{Ins}_{E,F}(U)$.

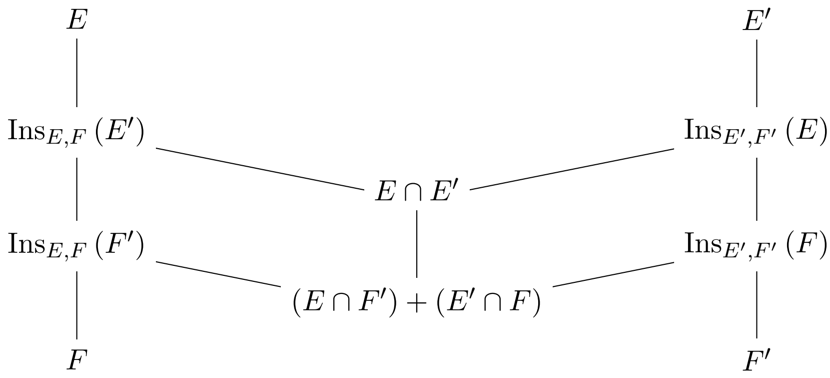
Theorem 2.13. (Zassenhaus' Lemma, a.k.a. the Butterfly Lemma) Let A be a ring, F, E, F' and E' be A-submodules of the left A-module M with the property that $F \subseteq E$ and $F' \subseteq E'$. We have a natural isomorphism of left A-modules

$$((E \cap E') + F)/((E \cap F') + F) \simeq ((E' \cap E) + F')/((E' \cap F) + F'),$$

which tells us that

$$\mathrm{Ins}_{E,F}(E') / \mathrm{Ins}_{E,F}(F') \simeq \mathrm{Ins}_{E',F'}(E) / \mathrm{Ins}_{E',F'}(F).$$

So the insertions of E' and F' between E and F have, up to isomorphism, the same quotient as the insertions of E and F between E' and F'.



Proof. By symmetry with respect to the pairs $E \leftrightarrow E'$ and $F \leftrightarrow F'$, it suffices to prove that

$$\mathrm{Ins}_{E,F}\left(E'\right)/\mathrm{Ins}_{E,F}\left(F'\right) \simeq (E \cap E')/((E \cap F') + (E' \cap F)).$$

Consider the natural maps

$$E \cap E' \hookrightarrow (E \cap E') + F \longrightarrow ((E \cap E') + F)/((E \cap F') + F) = \mathrm{Ins}_{E,F}(E')/\mathrm{Ins}_{E,F}(F').$$

We see that the composition is surjective because $E \cap E'$ gets mapped and the elements of F are zero in the last quotient. The kernel of this map is

$$(E \cap E') \cap ((E \cap F') + F) = E \cap F' + E' \cap F,$$

so by the isomorphism theorems, we are done.

Definition 2.14. Let M be a left A-module. A **finite series** for M is a collection $(M_0, \cdots, M_n)$ of A-submodules of M such that $M_0 = 0$, $M_n = M$ and $M_i \subseteq M_{i+1}$ for $i = 0, \cdots, n-1$ (equality $M_i = M_{i+1}$ is allowed) ; we denote a finite series for M by $M_\bullet$. The **length** of $M_\bullet = (M_0, \cdots, M_n)$ is defined to be the integer n.

Two finite series $M_\bullet$ and $N_\bullet$ of A-submodules of M, of length n and r respectively, are called **equivalent** if $r = n$ and there exists a permutation $\sigma \in S_n$ (the group of permutations of n elements) such that $M_i/M_{i-1} \simeq N_{\sigma(i)}/N_{\sigma(i)-1}$. The finite series $P_\bullet$ of M of length s is called a **refinement** of the series $M_\bullet$ if $\{M_0, \ldots, M_n\} \subseteq \{P_0, \ldots, P_s\}$.

A finite series $M_\bullet$ is called a **Jordan-Hölder series** for M if all succesive quotients M_i/M_{i-1} are simple. In other words, the series does not allow proper refinements, hence is a maximal element of the set of finite series of M, partially ordered under the relation of refinement. The module M is said to be of **finite length** if it admits a Jordan-Hölder (JH) series.

Theorem 2.15. Let M be a left A-module. Then any two finite series of submodules of M allow refinements which are equivalent.

Proof. Let $M_\bullet$ and $N_\bullet$ be two series of submodules of M of length r and s respectively. For $i = 1, \ldots, r$ and $j = 0, \ldots, s$, let $P_{i,j} \stackrel{\text{def}}{=} \mathrm{Ins}_{M_{i-1},M_i}(N_j)$. Then $P_{i,0} = M_{i-1}$ and $P_{i,s} = M_i$, namely

$$0 = P_{1,0} \subseteq \cdots \subseteq P_{1,s} = M_1 = P_{2,0} \subseteq \cdots \subseteq P_{2,s} \subseteq \cdots \subseteq P_{r,0} \subseteq \cdots \subseteq P_{r,s} = M.$$

This refinement arises from inserting the series $N_\bullet$ between each of the consecutive modules in $M_\bullet$. Analogously, define $Q_{i,j} \stackrel{\text{def}}{=} \mathrm{Ins}_{N_{j-1},N_j}(M_i)$ for $j = 1, \ldots, s$ and $i = 0, \ldots, r$, which refines $N_\bullet$ by inserting $M_\bullet$ between each of the consecutive modules in $N_\bullet$. We order the submodules $Q_{i,j}$ analogously, namely

$$0 = Q_{0,1} \subseteq \cdots \subseteq Q_{r,1} = N_1 = Q_{0,2} \subseteq \cdots \subseteq Q_{r,2} \subseteq \cdots \subseteq Q_{0,s} \subseteq \cdots \subseteq Q_{r,s} = M.$$

We now show that $P_{\bullet,\bullet}$ and $Q_{\bullet,\bullet}$ are equivalent. By Zassenhaus' Lemma, if $i = 1, \ldots, r$ and $j = 1, \ldots, s$, we have

$$\begin{aligned} P_{i,j}/P_{i,j-1} &= \mathrm{Ins}_{M_{i-1},M_i}(N_j)/\mathrm{Ins}_{M_{i-1},M_i}(N_{j-1}) \\ &\simeq \mathrm{Ins}_{N_{j-1},N_j}(M_i)/\mathrm{Ins}_{N_{j-1},N_j}(M_{i-1}) \\ &= Q_{i,j}/Q_{i-1,j}. \end{aligned}$$

Corollary 2.16. Let M be a left A-module of finite length. Any finite series of submodules of M can be refined to a Jordan-Hölder series. Any two Jordan-Hölder series of M are equivalent, and in particular must have the same length.

Proof. Let $M_\bullet$ be a series of submodules of M. Fix a Jordan-Hölder series $N_\bullet$ of M. By Theorem 2.15, there exists refinements $M'_\bullet$ and $N'_\bullet$ of $M_\bullet$ and $N_\bullet$ respectively, such that $M'_\bullet$ and $N'_\bullet$ are equivalent. Since $N_\bullet$ is a Jordan-Hölder series, $N'_\bullet$ is formed of $N_\bullet$ by repeating certain terms, so that in $N'_\bullet$, all successive quotients are simple or 0. Since $N'_\bullet$ and $M'_\bullet$ are equivalent, the same property holds for $M'_\bullet$.

Deleting the superfluous terms (i.e. removing the successive quotients which are zero and keep only one copy of each submodule) in $N'_\bullet$ and $M'_\bullet$, we obtain Jordan-Hölder series $M''_\bullet$ and $N''_\bullet$ with the following properties :

- $M''_\bullet$ refines $M_\bullet$
- $N''_\bullet = N_\bullet$
- $M''_\bullet$ is equivalent to $N''_\bullet$.

This means that the series $M_\bullet$ allows the Jordan-Hölder series $M''_\bullet$ as a refinement.

If $M_\bullet$ was already a Jordan-Hölder series, then in the previous construction $M_\bullet = M''_\bullet$ and $M''_\bullet$ is equivalent to $N''_\bullet$ where $N''_\bullet = N_\bullet$, hence $M_\bullet$ and $N_\bullet$ are equivalent.

Definition 2.17. Let M be a left A-module of finite length. The **length** of M is the length of any Jordan-Hölder series (which is well-defined by Corollary 2.16) and is denoted by $\ell_A(M)$ or $\ell(M)$ if A is understood.

Corollary 2.18. Let M a left A-module of finite length.

(i) If $N \leq M$ is a submodule, $N_\bullet$ is a Jordan-Hölder series for N and $(M/N)_\bullet$ is a Jordan-Hölder series for M/N, denoting by $\pi_N : M \to M/N$ the canonical projection, the series

$$0 = N_0 \subsetneq \cdots \subsetneq N_k = N = \pi_N^{-1}((M/N)_0) \subsetneq \pi_N^{-1}((M/N)_1) \subsetneq \cdots \subseteq \pi_N^{-1}((M/N)_\ell) = M$$

is a Jordan-Hölder series for M. In particular, $\ell_A(M) = \ell_A(N) + \ell_A(M/N)$ (we say that length is **additive** on short exact sequences).

(ii) If $M = N \oplus P$ for two submodules $N, P \leq M$ and $N_\bullet, P_\bullet$ are two Jordan-Hölder series for N and P respectively, then

$$0 = N_0 \subsetneq \cdots \subsetneq N_k = N = N \oplus P_0 \subsetneq N \oplus P_1 \subsetneq \cdots \subsetneq N \oplus P_\ell = N \oplus P = M$$

is a Jordan-Hölder series for M.

Proof. For (i), the successive quotients of submodules are all simple by the isomorphism theorems for A-modules. Part (ii) is a straightforward corollary of part (a).

Corollary 2.19. Let M a left A-module of finite length. Let $M_\bullet$ be a Jordan-Hölder series of length n for M. If $N_1 \leq N_2 \leq M$ are A-submodules such that N_2/N_1 is simple, there exists $i \in \{1, \cdots, n\}$ such that $M_i/M_{i-1} \simeq N_2/N_1$.

Proof. Refine the finite series $0 = N_0 \subseteq N_1 \subseteq N_2 \subseteq N_3 = M$ to a Jordan-Hölder series $N_\bullet$ for M ; because N_2/N_1 is simple, $N_\bullet$ can only be refined by adding extra submodules contained in N_1 or containing N_2. Since $M_\bullet$ and $N_\bullet$ are equivalent by Corollary 2.16, the simple quotient N_2/N_1 is isomorphic to one of the simple quotients M_{i+1}/M_i, as desired.

Corollary 2.20. Let M be a left A-module. Then M is of finite length if and only if it is artinian and noetherian.

Proof. ($\Rightarrow$) Suppose we are given an increasing chain $\{M_i\}_{i\in\mathbb{N}}$ of submodules of M ; without loss of generality, assume $M_0 = 0$. It follows that for any $n \geq 1$, the finite series $(M_0, \cdots, M_n, M)$ can be refined to a Jordan-Hölder series, so it can contain at most $\ell_A(M)$ strict inclusions. This implies that for n large enough, $M_i = M_n$ for all $i \geq n$, hence M is noetherian. The same argument proves that M is artinian by reversing the roles of M and 0 in this proof.
($\Leftarrow$) Set $M_0 \stackrel{\text{def}}{=} 0$. Since M is artinian, the set of its non-zero submodules admits a minimal element, namely M_1 ; the minimality implies that M_1 is simple. The A-module M/M_1 is also artinian, so by choosing a minimal nonzero submodule of it, we obtain a submodule $M_1 \leq M_2 \leq M$ such that M_2/M_1 is simple. Assuming $(M_0, M_1, \cdots, M_n)$ have been constructed such that the successive quotients are simple, we can construct M_{n+1} as long as $M_n \neq M$. This recursive construction cannot continue indefinitely because M is noetherian. Therefore $M_n = M$ eventually, which means we have found a Jordan-Hölder series for M.

Proposition 2.21. (Existence of the Fitting decomposition) Let M be an A-module and $\varphi \in \mathrm{End}_A(M)$.

(i) If $\mathrm{im}\,\varphi = \mathrm{im}\,(\varphi^2)$, then $M = \ker\varphi + \mathrm{im}\,\varphi$.

(ii) If $\ker\varphi = \ker(\varphi^2)$, we have $\ker\varphi \cap \mathrm{im}\,\varphi = 0$.

(iii) If M is artinian, there exists $n \geq 0$ such that $M = \ker(\varphi^n) + \mathrm{im}\,(\varphi^n)$.

(iv) If M is noetherian, there exists $n \geq 0$ such that $\ker(\varphi^n) \cap \mathrm{im}\,(\varphi^n) = 0$.

(v) If M is of finite length, there exists $n \geq 0$ such that $M = \ker(\varphi^n) \oplus \mathrm{im}\,(\varphi^n)$.

The decomposition of a finite length A-module M in (v) is called its **Fitting decomposition** with respect to φ.

Proof. (i) Pick $m \in M$. There exists $m' \in M$ such that $\varphi(m) = \varphi^2(m')$, which means $m - \varphi(m') \in \ker\varphi$. Therefore, $m = (m - \varphi(m')) + \varphi(m') \in \ker\varphi + \mathrm{im}\,\varphi$.

(ii) If $m \in \ker\varphi \cap \mathrm{im}\,\varphi$, pick $m' \in M$ such that $m = \varphi(m')$. This means $m' \in \ker(\varphi^2) = \ker\varphi$, therefore $m = \varphi(m') = 0$.

(iii) Consider the decreasing chain of submodules $\{\mathrm{im}\,(\varphi^n)\}_{n\geq 1}$. Since M is artinian, it stabilizes, so there exists $n \geq 1$ such that $\mathrm{im}\,(\varphi^n) = \mathrm{im}\,((\varphi^n)^2)$. Therefore $M = \ker(\varphi^n) + \mathrm{im}\,(\varphi^n)$ by part (i).

(iv) Consider the increasing chain of submodules $\{\ker(\varphi^n)\}_{n\geq 1}$. Since M is noetherian, it stabilizes, so there exists $n \geq 0$ such that $\ker(\varphi^n) = \ker((\varphi^n)^2)$. Therefore $\ker(\varphi^n) \cap \mathrm{im}\,(\varphi^n) = 0$.

(v) Combine parts (iii) and (iv).

Corollary 2.22. Let M be a left A-module and $\varphi \in \mathrm{End}_A(M)$.

(i) If M is artinian, φ is an isomorphism if and only if it is injective.

(ii) If M is noetherian, φ is an isomorphism if and only if it is surjective.

Proof. For (i), this follows from the expression $M = \ker(\varphi^n) + \mathrm{im}\,(\varphi^n) = \mathrm{im}\,(\varphi^n)$. For (ii), this follows from $\ker(\varphi^n) = \ker(\varphi^n) \cap \mathrm{im}\,(\varphi^n) = 0$.

Definition 2.23. A left A-module is called **indecomposable** if it is non-zero and does not admit non-trivial direct summands, i.e. cannot be written as $M = M_1 \oplus M_2$ where M_1, M_2 are non-zero.

Theorem 2.24. Let M be a left A-module which is nonzero, indecomposable and of finite length. The set of endomorphisms of $\mathrm{End}_A(M)$ which are not isomorphisms form a two-sided ideal contained in $\mathrm{Nil}(\mathrm{End}_A(M))$; in particular, an endomorphism of M is either nilpotent or an isomorphism.

Proof. Consider $\varphi \in \mathrm{End}_A(M)$. The module M admits the Fitting decomposition $M = \ker(\varphi^n) \oplus \mathrm{im}\,(\varphi^n)$, but since M is indecomposable, one of the two summands have to be zero. If $\ker(\varphi^n) = 0$, φ is an isomorphism ; if $\mathrm{im}\,(\varphi^n) = 0$, φ is nilpotent.

If $\varphi_1, \varphi_2 \in \mathrm{End}_A(M)$ are such that $\varphi_1 \circ \varphi_2$ is an isomorphism, then φ_1 and φ_2 are both isomorphisms (this follows trivially from looking at the set of units in $\mathrm{End}_A(M)$). So if either one of φ_1 or φ_2 is not an isomorphism, then their composition isn't either, which gives the statement about the nilpotent endomorphisms of M forming a two-sided ideal in $\mathrm{End}_A(M)$ when it comes to multiplication. For addition, suppose φ_1, φ_2 nilpotent and $\psi = \varphi_1 + \varphi_2$ invertible, so that $\mathrm{id}_M = \psi^{-1}\varphi_1 + \psi^{-1}\varphi_2$. Choose $n_1, n_2 \geq 1$ such that $(\psi^{-1}\varphi_i)^{n_i} = 0$. The endomorphisms $\psi^{-1}\varphi_1$ and $\psi^{-1}\varphi_2 = \mathrm{id}_M - \psi^{-1}\varphi_1$ commute, so since they are both nilpotent, by the binomial theorem,

$$\mathrm{id}_M = (\psi^{-1}\varphi_1 + \psi^{-1}\varphi_2)^{n_1+n_2} = \sum_{j=0}^{n_1+n_2} \binom{n_1+n_2}{j} (\psi^{-1}\varphi_1)^j (\psi^{-1}\varphi_2)^{n_1+n_2-j} = 0,$$

a contradiction to $M \neq 0$.

Theorem 2.25. Let M be a left A-module of finite length.

(i) There exists a direct sum decomposition $M = \bigoplus_{i=1}^n M_i$ where each M_i is indecomposable.

(ii) If $M = \bigoplus_{j=1}^m M'_j$ is another direct sum decomposition of M in indecomposable submodules, then $m = n$ and there exists a permutation $\sigma \in S_n$ (the group of permutations of $\{1, \cdots, n\}$) such that $M_{\sigma(i)} \simeq M'_i$ for $1 \leq i \leq n$.

Proof. Part (i) follows by induction on $\ell_A(M)$; if M has length 1, it is simple, thus indecomposable and "$M = M$" is the only possible decomposition of M in indecomposable submodules. If $\ell_A(M) > 1$ and M is indecomposable, we repeat the case where $\ell_A(M) = 1$. If it is not, then M is a direct sum of two non-zero submodules which have length strictly smaller than the length of M by Corollary 2.18 (i). The induction hypothesis completes the proof of this part.

Onto part (ii). Let

$$\bigoplus_{i=1}^{n} M_i = M = \bigoplus_{j=1}^{m} M'_j$$

be two direct sum decompositions of M into indecomposables. Let $\{\pi_i\}_{i=1}^n$ and $\{\pi'_j\}_{j=1}^m$ be the two families of projections corresponding to those decompositions. Without loss of generality, assume $n \leq m$. We will prove by induction on $0 \leq r \leq n$ the following result : there exists an injection $\sigma_r : \{1, \cdots, r\} \to \{1, \cdots, m\}$ and an automorphism $\varphi_r \in \mathrm{End}_A(M)$ such that $\varphi_r(M'_i) = M_{\sigma_r(i)}$ for all $1 \leq i \leq r$.

For $r = 0$, the statement is trivial. Suppose $0 < r \leq n$ and assume the statement has been proven for $r-1$. This means there exists $\sigma_{r-1} : \{1, \cdots, r-1\} \to \{1, \cdots, m\}$ and an automorphism $\varphi_{r-1} \in \mathrm{End}_A(M)$ such that $\varphi_{r-1}(M'_i) = M_{\sigma_{r-1}(i)}$. By replacing each M'_i by $\varphi_{r-1}(M'_i) = M_{\sigma_{r-1}(i)}$, we can assume without loss of generality that $M'_i = M_i$ for $1 \leq i \leq r-1$.

The restriction to M'_r of the projection $\pi'_r = \sum_{i=1}^n \pi'_r \pi_i$ is the identity of M'_r. Since M'_r is indecomposable, the endomorphisms $\pi'_r\pi_i$ cannot all be nilpotent, otherwise $\mathrm{id}_{M'_r}$ would be nilpotent, a contradiction. Pick $k \in \{1, \cdots, n\}$ such that $\pi'_r \pi_k|_{M'_r}$ is an isomorphism. We must have $k \geq r$ since for $k < r$, we have $\pi_k = \pi'_k \pi_k$, which means $\pi'_r \pi_k = \pi'_r \pi'_k \pi_k = 0$. We set

$$\sigma_r|_{\{1,\cdots,r-1\}} = \sigma_{r-1}, \quad \sigma_r(r) \overset{\text{def}}{=} k, \quad \varphi_r \overset{\text{def}}{=} \mathrm{id}_M - \pi'_r + \pi_k \pi'_r.$$

If $m \in M$ satisfies $\varphi_r(m) = 0$, we have

$$0 = \pi'_r \varphi_r(m) = (\pi'_r - \pi'^2_r + \pi'_r \pi_k \pi'_r)(m) = (\pi'_r \pi_k)(\pi'_r(m)) \quad \Longrightarrow \quad \pi'_r(m) = 0,$$

hence

$$m = \varphi_r(m) + \pi'_r(m) - (\pi_k \pi'_r)(m) = 0 + 0 - \pi_k(0) = 0,$$

which means φ_r is injective, hence an automorphism of M. Clearly, $\varphi_r(m) = m$ when $m \in \sum_{\substack{j=1 \\ j\neq r}}^m M'_j$ and $\varphi_r(M'_r) \subseteq M_k$. This means that M_k is the direct sum of $\varphi_r(M'_r)$ and $M_k \cap \left(\sum_{\substack{j=1 \\ j\neq r}}^m M'_j \right)$, but since M_k is indecomposable and $\varphi_r(M'_r) \neq 0$, this means $M_k = \varphi_r(M'_r)$, which proves our claim.

Finally, the assumption $n < m$ is contradictory since it implies

$$\bigoplus_{i=1}^{n} M_i = M = \bigoplus_{j=1}^{m} M'_j \simeq \left(\bigoplus_{j=1}^{n} \varphi_n^{-1}(M_{\sigma_n(j)}) \right) \oplus \left(\bigoplus_{j=n+1}^{m} M'_j \right),$$

and by computing lengths, we deduce that $\bigoplus_{j=n+1}^m M'_j$ has length zero.

2.2 Artinian and noetherian rings

Definition 2.26. Let A be a ring. We say that A is

(i) **left-artinian** (resp. left-noetherian) if the left A-module A_ℓ is left-artinian (resp. left-noetherian). Equivalently, A is left-artinian (resp. left-noetherian) if every descending (resp. ascending) chain of left ideals of A stabilizes.

(ii) **right-artinian** (resp. right-noetherian) if the right A-module A_ℓ is right-artinian (resp. right-noetherian).

Equivalently, A is right-artinian (resp. right-noetherian) if every descending (resp. ascending) chain of right ideals of A stabilizes.

(iii) When A is such that A_ℓ (resp. A_r) is of finite length, the **left-length** (resp. right-length) of A is the length of A_ℓ (resp. A_r).

When A is commutative, left-artinian and right-artinian is the same notion (similarly for noetherian), so we call such rings **artinian** (resp. **noetherian**). If A is commutative and A_ℓ, A_r are of finite length, the left-length equals the right-length, so we simply call it the **length** of A.

Example 2.27. (i) Let K be a field and A a K-algebra which is of finite dimension over K. Then A is left-artinian, right-artinian, left-noetherian and right-noetherian since left (resp. right) ideals of A are K-vector subspaces of A, so finite series have length bounded by $\dim_K A$.

(ii) A principal ideal domain is a commutative noetherian ring since every ideal is principal, hence finitely generated. For example, the ring of integers $\mathbb{Z}$ is noetherian. However, $\mathbb{Z}$ is not artinian since for any $n \geq 1$, the ideal $\mathfrak{a} \overset{\text{def}}{=} n\mathbb{Z}$ is such that the chain of ideals $\{\mathfrak{a}^n\}_{n\geq 1}$ is strictly increasing.

(iii) Let $\{M_i\}_{i\in I}$ be an infinite family of non-zero left A-modules and $M \overset{\text{def}}{=} \bigoplus_{i\in I} M_i$. Then $\mathrm{End}_A(M)$ is neither left-artinian or left-noetherian. To see this, for each $i \in I$, let $\mathfrak{a}_i \trianglelefteq \mathrm{End}_A(M)$ be the left ideal defined by

$$\mathfrak{a}_i \overset{\text{def}}{=} \{\varphi \in \mathrm{End}_A(M) \mid \varphi(M_i) = 0\}.$$

By looking at the projections π_i of M to M_i, we see that the collection of left ideals $\{\mathfrak{a}_i\}_{i\in I}$ are in a direct sum inside of $\mathrm{End}_A(M)$, which gives the claim (c.f. Example 2.2 (ii)).

(iv) We will see later (c.f. Corollary 4.37) that a left-artinian ring is left-noetherian. However, there exists left-artinian modules which are not left-noetherian ; in fact, this is true even in the commutative case, i.e. there exists an abelian group (in other words, a $\mathbb{Z}$-module) which is artinian but not noetherian. A classical example is that of the $\mathbb{Z}$-subalgebra of $\mathbb{Q}$ given by $\mathbb{Z}[\frac{1}{p}]$ where $p \in \mathbb{Z}$ is a prime number, which we then mod out by $\mathbb{Z}$:

$$\mathbb{Z}[\tfrac{1}{p}]/\mathbb{Z} = \left\{ \tfrac{a}{p^n} + \mathbb{Z} \mid a \in \mathbb{Z}, n \geq 1, (a, p^n) = 1 \right\}.$$

To see this, it suffices to see that the only proper subgroups of $\mathbb{Z}[\frac{1}{p}]/\mathbb{Z}$ are those generated by $\frac{1}{p^n} + \mathbb{Z}$ for some $n \geq 1$. Write $G_n \overset{\text{def}}{=} \left\langle \frac{1}{p^n} \right\rangle_{\mathbb{Z}}$. Note that by definition, $\mathbb{Z}[\frac{1}{p}] = \bigcup_{n\geq 1} G_n$. If $H \leq \mathbb{Z}[\frac{1}{p}]$ is a proper subgroup and $x \in G_n \cap H$ for some $n \geq 1$, then $x = \frac{a}{p^n}$ where $(a, p^n) = 1$,, so there exists $b, c \in \mathbb{Z}$ such that $ab + p^n c = 1$, which means that $bx \equiv \frac{1}{p^n} \pmod{\mathbb{Z}}$, hence $bx \in H$. Therefore $G_n \subseteq H$. Letting n_H be the largest integer satisfying $G_{n_H} \subseteq H$, we see by this argument that $H = G_{n_H}$. This also implies that $\mathbb{Z}[\frac{1}{p}]$ is not finitely generated, hence not noetherian ; for if $\frac{a_1}{p^{n_1}}, \cdots, \frac{a_k}{p^{n_k}}$ is a finite subset, their $\mathbb{Z}$-span is contained in $\bigcup_{i=1}^k G_{n_i}$, a proper subgroup. However, any descending chain of subgroups of $\mathbb{Z}[\frac{1}{p}]/\mathbb{Z}$ corresponds to a descending sequence of non-negative integers, thus stabilizes, which means $\mathbb{Z}[\frac{1}{p}]/\mathbb{Z}$ is artinian.

(v) A finite product of artinian (resp. noetherian) rings is artinian (resp. noetherian). To see this, pick $A_1, \cdots, A_n$ artinian (resp. noetherian) rings, so that $A \overset{\text{def}}{=} A_1 \times \cdots \times A_n$ is a left A-module. A left ideal $\mathfrak{a} \trianglelefteq A$ has to be of the form $\mathfrak{a}_1 \times \cdots \times \mathfrak{a}_n$ where $\mathfrak{a}_i \trianglelefteq A_i$ by considering the idempotents $(0, \cdots, 0, 1, 0, \cdots, 0) \in A$ (with a 1 at the i^{th} coordinate). Therefore, a decreasing (resp. increasing) sequence eventually stabilizes because it stabilizes in each component. More generally, if M_i is an artinian (resp. noetherian) A_i-module for $i = 1, \cdots, n$, then $M_1 \times \cdots \times M_n$ is an artinian (resp. noetherian) $A_1 \times \cdots \times A_n$-module by the same argument. Furthermore, any quotient of an artinian (resp. noetherian) ring by a two-sided ideal is again an artinian (resp. noetherian) ring.

(vi) Subrings of artinian (resp. noetherian) rings are not necessarily artinian (resp. noetherian). The best example would be the polynomial ring in infinitely many variables over a field K, say $A \stackrel{\text{def}}{=} K[\{x_n\}_{n\in\mathbb{N}}]$, seen as a subring of its quotient field (which is artinian and noetherian). Considering the sequence of ideals

$$\mathfrak{a}_n \stackrel{\text{def}}{=} (x_1)_A^n, \quad \mathfrak{b}_n \stackrel{\text{def}}{=} (x_1, \cdots, x_n)_A$$

we see that $\mathfrak{a}_n$ is an infinite strictly descending chain and $\mathfrak{b}_n$ is an infinite strictly ascending chain, so A is neither artinian nor noetherian.

Proposition 2.28. A finitely generated left A-module over an artinian (resp. noetherian) ring is artinian (resp. noetherian).

Proof. This follows from Proposition 2.5 since M is the quotient of the left A-module $A^{\oplus n}$ for some $n \geq 1$.

Corollary 2.29. Let A be a left-artinian ring and B be a left-finite A-algebra (i.e. an A-algebra which makes B a finitely generated left A-module). Then B is a left-artinian ring. (This generalizes Example 2.27 (i).)

Proof. If $\{\mathfrak{b}_n\}_{n\in\mathbb{N}}$ is a descending chain of left ideals in B, it is a descending chain of A-submodules of B_ℓ, which is artinian. Therefore, this chain stabilizes, i.e. B is left-artinian.

Proposition 2.30. Let M be a faithful left A-module and $\{m_i\}_{i\in I}$ be a family of generators of $M^\triangleleft$. The map $A \to M^{\oplus I}$ given by $a \mapsto (am_i)_{i\in I}$ is injective and A-linear, hence A_ℓ can be seen as a left A-submodule of $M^{\oplus I}$.

Proof. It is obvious that this map is a morphism of left A-modules. Suppose $am_i = 0$ for all $i \in I$. If $\{\varphi_i\}_{i\in I} \subseteq \text{End}_A(M)$ and $m = \sum_{i\in I}^* \varphi_i(m_i) \in M$, then

$$a\left(\sum_{i\in I}^* \varphi_i(m_i)\right) = \sum_{i\in I}^* \varphi_i(am_i) = 0,$$

which means $a \in \text{Ann}_A(M) = 0$ since ${}_{\text{End}_A(M)}\langle\{m_i\}_{i\in I}\rangle = M^\triangleleft$, hence M is a faithful left A-module.

Proposition 2.31. Let M be an artinian (resp. noetherian) left A-module. If $M^\triangleleft$ is finitely generated, the ring A_M is artinian (resp. noetherian).

Proof. The left A-module M is also a faithful left $A/\text{Ann}_A(M)$-module which is left-artinian (resp. left-noetherian) and $A_M \simeq A/\text{Ann}_A(M)$, so without loss of generality, assume M is a faithful left A-module. By Proposition 2.30, A_ℓ is isomorphic to an A-submodule of $M^{\oplus n}$ for some $n \geq 1$, which means it is a left-artinian (resp. left-noetherian) A-module, i.e. A is a left-artinian (resp. left-noetherian) ring.

Corollary 2.32. Assume A is a commutative ring and let M be a noetherian A-module. Then A_M is noetherian.

Proof. Since M is finitely generated, so is $M^\triangleleft$ since $A_M \subseteq \text{End}_A(M)$ by the commutativity assumption. The result follows from Proposition 2.31.

2.3 Simple modules

Proposition 2.33. Let M be a nonzero left A-module. Then M is simple if and only if for all $m \in M \setminus \{0\}$, $Am = M$. In particular, a simple module is a **cyclic** module, which means it is generated by a single element.

Proof. This follows from the fact that Am is a nonzero submodule of M for any $m \in M \setminus \{0\}$.

Proposition 2.34. Let A be a ring and $\mathfrak{a} \trianglelefteq A$ be a left ideal of A. The left A-module $A_\ell/\mathfrak{a}$ is cyclic, and it is simple if and only if $\mathfrak{a}$ is a left maximal ideal of A, which means that if $\mathfrak{b}$ is another left ideal of A satisfying $\mathfrak{a} \subseteq \mathfrak{b} \subseteq A_\ell$, then $\mathfrak{b} = \mathfrak{a}$ or $\mathfrak{b} = A_\ell$.

Proof. The left A-module $A_\ell/\mathfrak{a}$ is generated by $1 + \mathfrak{a}$, thus is cyclic. The left A-submodules of $A/\mathfrak{a}$ are in one-to-one correspondence with the left ideals of A containing $\mathfrak{a}$, thus the second statement holds.

Theorem 2.35. Let M be a simple left A-module. Given $m \in M \setminus \{0\}$, the map $A_\ell \to M$ given by $a \mapsto am$ induces an isomorphism $A_\ell/\mathfrak{m} \simeq M$ where $\mathfrak{m}$ is a left maximal ideal of M. There is a one-to-one correspondence between the set of left maximal ideals of A and the set of isomorphism classes of simple left A-modules given by $\mathfrak{m} \mapsto [A_\ell/\mathfrak{m}]$ (the brackets stand for the equivalence class of the left A-module).

Proof. If two simple left A-modules M_1, M_2 are isomorphic, they have the same annihilator, hence are both isomorphic to $A_\ell/\mathfrak{m}$ where $\mathfrak{m} = \mathrm{Ann}_A(M_1) = \mathrm{Ann}_A(M_2)$ is a left maximal ideal. Conversely, $A_\ell/\mathfrak{m}$ is simple for any left maximal ideal $\mathfrak{m}$, which gives the result.

Example 2.36.

(i) Let A be a ring. The simple submodules of A_ℓ are the nonzero left ideals of A which are minimal with respect to inclusion in the set of nonzero left ideals of A ; we call them the **minimal left ideals** of A. An obvious example of when A has minimal left ideals is when A is left-artinian, in which case we can use the descending chain condition and Zorn's lemma to prove the existence of a minimal left ideal.

Such ideals do not always exist, as shown by the case of a (commutative) local ring $(A, \mathfrak{m})$ which is also an integral domain since if $\mathfrak{a} \trianglelefteq A$ and A is not a field (in the case of a field, there are no non-zero ideals), we have $0 \neq \mathfrak{m}\mathfrak{a} \subsetneq \mathfrak{a}$ ($\mathfrak{a}\mathfrak{m} \neq 0$ because A is a domain, and $\mathfrak{a} = \mathfrak{m}\mathfrak{a}$ implies $\mathfrak{a} = 0$ by Nakayama's Lemma). Another trivial example is when $A = \mathbb{Z}$ since $0 \neq \mathfrak{a} \trianglelefteq \mathbb{Z}$ implies $0 \neq \mathfrak{a}^2 \subsetneq \mathfrak{a}$. In fact, any UFD or Dedekind domain also has no minimal ideals as a module over itself for the same reason.

(ii) Let K be a field, V a K-vector space, and $A \subseteq \mathrm{End}_K(V)$ be the subring generated as a vector space by id_V and the K-endomorphisms of V which are of **finite rank**. It follows that V is a simple A-module since if $W \leq V$ is an A-submodule, then W contains any finite-dimensional subspace of V, thus is equal to V. In particular, V is simple as an $\mathrm{End}_K(V)$-module, which is equal to $V^{\triangleleft}$ when we see V as a K-module.

Let $\mu \in \mathrm{Hom}_K(V, K)$ be a non-zero linear form on V. For $v \in V$, denote by $\varphi_v \in A$ the endomorphism given by $\varphi_v(w) = \mu(w)v$. It is clear that for any $\psi \in \mathrm{End}_K(V)$, we have

$$(\psi \circ \varphi_v)(w) = \psi(\mu(w)v) = \mu(w)\psi(v) = \varphi_{\psi(v)}(w) \quad \Longrightarrow \quad \psi\varphi_v = \varphi_{\psi(v)}$$

hence the map $\varphi : V \to \mathrm{End}_K(V)$ sending v to φ_v is a left $\mathrm{End}_K(V)$-linear map ; if we restrict its codomain to A, it is also a left A-linear map. Since its kernel is a proper left $\mathrm{End}_K(V)$-submodule of

V, it is zero (which can also easily be seen directly since $\mu \neq 0$), which means V maps isomorphically onto a minimal left ideal of $\mathrm{End}_K(V)$.

(iii) Let A be a ring. For A_ℓ to be a simple A-module, it is necessary and sufficient that 0 be the only proper left ideal of A, meaning that A is a division ring. In this case, any simple left A-module is isomorphic to A_ℓ. In particular, the left A-module A_ℓ is simple if and only if the right A-module A_r is simple.

(iv) Let A be a principal ideal domain. The simple A-modules are of the form $A/\mathfrak{p}$ where $\mathfrak{p} = (p)_A \in A$ is generated by a prime element of A. For $n > 1$, the A-modules $A/\mathfrak{p}^n$ are indecomposable, but not simple ; to see this, assume $(A, \mathfrak{p})$ is local (after localization at $\mathfrak{p}$), so that picking $x \in \mathfrak{p}^k \setminus \mathfrak{p}^{k+1}$ for $1 \leq k < n$, we obtain $(x)_A \simeq \mathfrak{p}^k/\mathfrak{p}^n \simeq A/\mathfrak{p}^{n-k} \not\simeq A/\mathfrak{p}^n$. In particular, if $A/\mathfrak{p}^n \simeq \mathfrak{a} \oplus \mathfrak{b}$ where $\mathfrak{a}, \mathfrak{b}$ are A-submodules (i.e. ideals of A), then $\mathfrak{a}$ and $\mathfrak{b}$ are annihilated by $\mathfrak{p}^{n-1}$, a contradiction.

Definition 2.37. Let M be a left A-module. A **maximal submodule** of M is a left A-submodule N of M such that M/N is simple. In other words, N is maximal in the set of proper submodules of M partially ordered under inclusion.

Remark 2.38. When M is a noetherian left A-module, maximal submodules always exist. We generalize this in the next proposition.

Proposition 2.39. Let M be a left A-module and $L \leq M$ a proper submodule. If M is finitely generated, then there exists a maximal submodule of M containing L.

Proof. It suffices to see that we can apply Zorn's lemma, i.e. that every chain has an upper bound. If $L \subseteq N_1 \subseteq \cdots \subseteq N_r \subseteq \cdots$ is a chain of proper submodules of M, then $N \overset{\text{def}}{=} \bigcup_{r \geq 1} N_r$ is a proper submodule of M. Otherwise, each generator lies in N_r for some $r \geq 1$, meaning that M is contained in N_r, a contradiction.

Corollary 2.40. Let M be a finitely generated left A-module. There exists a simple left A-module M' such that $\mathfrak{a} \overset{\text{def}}{=} \mathrm{Ann}_A(M')$ satisfies $\mathfrak{a}M \neq M$.

Proof. Let N be a maximal submodule of M and let $\mathfrak{a} \overset{\text{def}}{=} \mathrm{Ann}_A(M/N)$. Then $\mathfrak{a}M \subseteq N \subsetneq M$.

Proposition 2.41. Let A be a ring, $\mathfrak{b}$ a minimal left ideal of A (c.f. Example 2.36) and M a simple faithful left A-module. Then $M \simeq \mathfrak{b}$ as A-modules. In particular, all minimal left ideals of a ring A are isomorphic as A-modules.

Proof. Let $b \in \mathfrak{b} \setminus \{0\}$. Since M is a faithful A-module, there exists $m \in M \setminus \{0\}$ such that $bm \neq 0$. Define $\mathfrak{m} \overset{\text{def}}{=} \mathrm{Ann}_A(m)$. Since M is simple and $b \notin \mathfrak{m}$, we have $\mathfrak{m} + \mathfrak{b} = A$. Since $\mathfrak{b}$ is a minimal ideal, $\mathfrak{b} \cap \mathfrak{m} = 0$; otherwise, $\mathfrak{b} \cap \mathfrak{m} = \mathfrak{b}$ implies $\mathfrak{b} \subseteq \mathfrak{m} = \mathrm{Ann}_A(m)$, which is impossible since $bm \neq 0$. Therefore $A_\ell \simeq \mathfrak{m} \cap \mathfrak{b}$, hence $A/\mathfrak{m} \simeq \mathfrak{b}$.

Theorem 2.42. Let M be a faithful left A-module admitting a Jordan-Hölder series $(M_0, \cdots, M_n)$ (c.f. Definition 2.14). If $M^{\triangleleft}$ is finitely generated, every simple left A-module is isomorphic to one of the successive quotients M_{i+1}/M_i for some $0 \leq i < n$.

Proof. Every simple left A-module is a quotient of the left A-module A_ℓ. We have already seen that A_ℓ is isomorphic to a submodule of $M^{\oplus n}$ in Proposition 2.30 because M is assumed faithful. It follows that every simple left A-module is isomorphic to one of the successive quotients of a Jordan-Hölder series for $M^{\oplus n}$, but we can construct a Jordan-Hölder series for $M^{\oplus n}$ using the Jordan-Hölder series for M (c.f.

Corollary 2.18 (ii)), so that the set of isomorphism classes of simple A-modules coming from successive quotients of M equals that of $M^{\oplus n}$, completing the proof.

2.4 Completely reducible modules

Theorem 2.43. Let M be a left A-module which is the sum of a family $\{M_i\}_{i\in I}$ of simple A-submodules. For every A-submodule $L \leq M$, there exists a subset $J \subseteq I$ such that $M = L \oplus \bigoplus_{j\in J} M_j$.

Proof. Let Ω be the set of all $J \subseteq I$ such that the modules $\{M_j\}_{j\in J}$ and L are in a direct sum. We claim that Zorn's Lemma applies to $\Omega \subseteq \mathcal{P}(I)$ since the condition of being in a direct sum only concerns finitely many elements of J at a time, hence if $\{J_\alpha\}_{\alpha\in\Lambda}$ is a family of subsets of Ω which are totally ordered under inclusion, the union $\bigcup_{\alpha\in\Lambda} J_\alpha$ also lies in Ω. So assume J is a maximal element of Ω. We claim that $M = L \oplus \bigoplus_{j\in J} M_j$. Let $N \stackrel{\text{def}}{=} L \oplus \bigoplus_{j\in J} M_j \subsetneq M$. Since J is maximal in Ω, if $M_{j'}$ is a simple submodule of M, then $N \cap M_{j'} \neq \{0\}$, hence $M_{j'} \cap N = M_{j'}$ because $M_{j'}$ is simple. This implies $M_{j'} \subseteq N$; since $M_{j'}$ was arbitrary, this implies $M \subseteq N$, hence $M = N$.

Theorem 2.44. Let M be a left A-module. The following are equivalent :

(i) M is the sum of a family of simple A-submodules

(ii) M is the direct sum of a family of simple A-submodules

(iii) Every A-submodule of M is a direct summand.

A left A-module M satisfying one of the equivalent conditions above is called **completely reducible** (or **semisimple** in most of the literature).

Proof. ((i) $\Rightarrow$ (ii)) Choose $L = 0$ in Theorem 2.43.

((ii) $\Rightarrow$ (iii)) This follows by letting the submodule in (iii) be the submodule L in Theorem 2.43.

((iii) $\Rightarrow$ (i)) Let L be a cyclic submodule of M. By Proposition 2.39, there exists a maximal submodule L' of L, so that L/L' is simple. Let $N' \leq M$ be such that $L' \oplus N' = M$. The submodule $L \cap N'$ is non-zero, otherwise $L \oplus N' = M$, which means that $L/L' \simeq M/M = 0$, a contradiction. It follows that $L \cap N'$ is a non-zero submodule of L satisfying $(L \cap N') \cap L' = 0$ and $(L \cap N') + L' = L$ by maximality of L' in L, hence $L = L' \oplus (L \cap N')$ and $L/L' \simeq L \cap N'$ is simple. Therefore, any non-zero submodule of M contains a simple submodule.

Consider the sum S of all simple submodules of M and let P be a submodule such that $M = S \oplus P$. If P is nonzero, it contains a simple submodule of M, so that $P \cap S \neq 0$, a contradiction. Therefore $P = 0$, which completes the proof.

Remark 2.45. A left A-module M is completely reducible if and only if it is a completely reducible A_M-module. By Theorem 2.44, any left A-module M which is the sum of completely reducible submodules is itself completely reducible.

Example 2.46. (i) Simple left A-modules are completely reducible.

(ii) If A is a field, every cyclic A-module is simple, so every A-module is semisimple. This is the fact that every vector space admits a basis.

(iii) The $\mathbb{Z}$-module $\mathbb{Z}$ is not semisimple since simple $\mathbb{Z}$-modules are of the form $\mathbb{Z}/p\mathbb{Z}$ where p is a prime number and the only finite subgroup of $\mathbb{Z}$ is 0.

Corollary 2.47. Let M be a left A-module which is the sum of the simple submodules $\{M_i\}_{i\in I}$. For any A-submodule N, there exists $J \subseteq I$ such that $N \simeq \sum_{j\in J} M_j$ and $M/N \simeq \sum_{j\in I\setminus J} M_j$.

Proof. By Theorem 2.43, we see that there exists $J \subseteq I$ such that $M = N \oplus \sum_{j\in J} M_j$, so that $N \simeq M/\left(\sum_{j\in J} M_j\right)$ is the quotient of M by one of its submodules. Therefore, it suffices to deal with the case of the quotient. But by the same expression, $M/N \simeq \sum_{j\in J} M_j$, so we are done.

Corollary 2.48. If M is a completely reducible left A-module and $N \leq M$ is a submodule, then N and M/N are completely reducible.

Proof. Since M is completely reducible, it is the sum of its simple submodules. The result follows by Corollary 2.47 combined with Theorem 2.44.

Corollary 2.49. Let M be a left A-module which is the sum of the family of simple submodules $\{M_i\}_{i\in I}$. Then any simple submodule of M is isomorphic to one of the M_i's.

Proof. If $N \leq M$, it is isomorphic to the sum of submodules of the form M_j where $j \in J \subseteq I$ for a given subset J. For any $j \in J$, we have $0 \lneq M_j \leq \sum_{i\in J} M_i \simeq N$, which means $M_j = N$ when N is simple.

2.5 Isotypical components of completely reducible modules

Theorem 2.50. Let M be a completely reducible left A-module. If N_0 is a simple A-submodule of M, let $\{N_i\}_{i\in I}$ be the set of simple submodules of M isomorphic to N_0. Their sum $N^0 \stackrel{\text{def}}{=} \sum_{i\in I} N_i$ is isotypical of type N_0, so is a completely reducible submodule of M ; it is uniquely characterized as the sum of all simple A-submodules of M isomorphic to N_0, so we call it the **isotypical component of M of type N_0**. When $\{P_i\}_{i\in I}$ is a family of simple submodules of M satisfying

(i) Each simple A-submodule of M is isomorphic to one of the P_i

(ii) No two distinct P_i are isomorphic

then letting

$$P_i^0 \stackrel{\text{def}}{=} \sum_{\substack{N\leq M\\ N\simeq P_i}} N$$

gives the isotypical component P_i^0 of M of type P_i, and $M = \bigoplus_{i\in I} P_i^0$ is the direct sum of its isotypical components.

Proof. It is clear that M is the sum of its isotypical components and that its isotypical components are indeed isotypical by Theorem 2.44. The isotypical components are in a direct sum, for if $i \in I$, a non-zero element in $P_i^0 \cap \sum_{j\in I\setminus\{i\}} P_j^0$ implies that both submodules intersected contain a simple submodule isomorphic to P_i, but the sum only contains simple submodules isomorphic to P_j for $j \neq i$ by assumption (i) and Corollary 2.47, a contradiction by assumption (ii).

Corollary 2.51. Let M be a completely reducible left A-module with isotypical components $\{M_i\}_{i\in I}$, each

M_i being isotypical of type P_i. If $N \leq M$ is a submodule, then the isotypical component of N of type P_i, denoted by N_i, is equal to $N \cap M_i$. Furthermore, $N \simeq \bigoplus_{i\in I} N \cap M_i$.

Proof. We already know that N is completely reducible, hence it is the direct sum of its isotypical components. Since a simple submodule of N is a simple submodule of M, the isotypical component N_i of N of type P_i must be contained in M_i, which means $N = \bigoplus_{i\in I} N_i = \bigoplus_{i\in I} N \cap M_i$.

Remark 2.52. If M is an arbitrary left A-module, we can still define the isotypical components as the sum of the simple A-submodules of a given isomorphism type and the sum $\sum_{i\in I} M_i$ will still be direct. The equality $M = \bigoplus_{i\in I} M_i$ will hold precisely when M is completely reducible.

Proposition 2.53. Let $M = \bigoplus_{i\in I} M_i$ and $N = \bigoplus_{i\in I} N_i$ be two completely reducible left A-modules written in their decompositions in isotypical components of type P_i and let $f : M \to N$ be a morphism of A-modules. Then $f(M_i) \subseteq N_i$. In particular,

(i) We have $\mathrm{Hom}_A(M, N) \simeq \prod_{i\in I} \mathrm{Hom}_A(M_i, N_i)$ via the map $f \mapsto (f|_{M_i})_{i\in I}$.

(ii) If $M = N$, we have $\mathrm{End}_A(M) = \prod_{i\in I} \mathrm{End}_A(M_i)$.

Proof. This follows from the fact that $f(M_i)$ is a quotient of M_i, thus also isotypical of type P_i (c.f. Corollary 2.47) ; this implies that $f(M_i) \subseteq N_i$ since N_i is the sum of all simple submodules of N of isomorphism type P_i, and $f(M_i)$ is such a sum. The parts (i) and (ii) are trivial corollaries.

Corollary 2.54. Let M be a completely reducible left A-module and $N \leq M$ an A-submodule. The following are equivalent :

(i) $N \leq M^{\triangleleft}$ is a submodule, which means it is an $\mathrm{End}_A(M)$-submodule of M

(ii) N is the (direct) sum of isotypical components of M.

Proof. ((ii) $\Rightarrow$ (i)) By Proposition 2.53, if $f \in \mathrm{End}_A(M)$, then $f|_N : N \to M$ maps each isotypical component into itself, which means N is stable under $\mathrm{End}_A(M)$.

((i) $\Rightarrow$ (ii)) Let $N_1, N_2 \leq M$ be two simple A-submodules of M which are isomorphic. Since N_1 is a direct summand of M, fix a complement N_1' so that $M = N_1 \oplus N_1'$ and let $\pi_1 : M \to M$ be the corresponding projection. If $\varphi : N_1 \to N_2$ is an isomorphism, then $\psi_{12} \stackrel{\text{def}}{=} \varphi \circ \pi_1 \in \mathrm{End}_A(M)$ and $\psi_{12}(N_1) = N_2$. Therefore, if N is stable under A-endomorphisms of M and contains one simple submodule of isomorphism type P_i, it contains the entire isotypical component M_i of M. Since $N = \bigoplus_{i\in I} N \cap M_i$, this means either $N \cap M_i = 0$ or $N \cap M_i = M_i$, as desired.

Proposition 2.55. Let M be a completely reducible left A-module with $\{N_i\}_{i\in I}$ and $\{N_j'\}_{j\in J}$ two families of simple submodules of M such that $\bigoplus_{i\in I} N_i = M = \bigoplus_{j\in J} N_j'$. Then $|I| = |J|$.

Proof. By writing M as a direct sum of its isotypical components, we can assume without loss of generality that M is isotypical. If I is finite, then the A-length of M satisfies $\ell_A(M) = |I|$, whence J is also finite since any finite collection $J' \subseteq J$ satisfies $|J'| \leq |I|$ from the fact that $\sum_{j\in J'} N_j' \leq M$, which implies $|J| \leq |I|$. It follows that $|J| = \ell_A(M) = |I|$.

Suppose I and J infinite. For each $i \in I$, fix $m_i \in N_i \setminus \{0\}$ so that $N_i = {}_A\langle m_i \rangle$. Let $J_i \subseteq J$ be defined as follows ; write $m_i = \sum_{j\in J}^* m_{ij}'$ with $m_{ij}' \in N_j'$ and let J_i be the set of those $j \in J$ for which $m_{ij}' \neq 0$. We have $J = \bigcup_{i\in I} J_i$ because otherwise, there exists $j \in J$ such that $m_{ij}' = 0$ for all $i \in I$, meaning that N_j'

is not necessary in the sum $\sum_{j \in J} N'_j$ to obtain M, a contradiction to the fact that our sums are direct. This means that $|J| \leq |I \times \mathbb{N}| = |I||\mathbb{N}| = |I|$ because I is infinite, and by symmetry of the hypotheses, we obtain $|I| = |J|$.

Definition 2.56. Let M be a completely reducible left A-module and P a simple A-module. We denote the isotypical component of M of type P by M_P (this includes the case where $M_P = 0$, i.e. when M has no submodule isomorphic to P). We generalize the notion of left-length of an completely reducible module to include the case where M might not be a module of finite length in the sense of Jordan-Hölder series : the **length** of M, denoted by $\ell_A(M)$, is the cardinality of I where $M = \bigoplus_{i \in I} N_i$ is a decomposition of M as a direct sum of simple A-modules. If M has isotypical component M_P, we denote the length of M_P by $[M : P]_A$. Therefore, if $J(M)$ denotes an index set containing an isomorphism class representative of each simple left A-submodule of a module M, then $\ell_A(M) = \sum_{P \in J(M)} [M : P]_A$. In particular, $\ell_A(M) < \infty$ if and only if it admits a Jordan-Hölder series, in which case M is a direct sum of simple left A-modules.

If M is a left A-module, we say that M is **isotypically simple** if M is isotypical of type P for some simple left A-module P (whose isomorphism type is then uniquely determined). The isotypical components of a completely reducible left A-module are therefore its maximal isotypically simple submodules.

Corollary 2.57. Let M, N be two completely reducible left A-modules. Then M and N are isomorphic if and only if for any simple left A-module P, we have $[M : P]_A = [N : P]_A$.

Proof. Decompose M and N into isotypical components. By Proposition 2.53, assume without loss of generality that M and N are isotypical of type P. Then $M \simeq P^{\oplus I}$ and $N \simeq P^{\oplus J}$, so the result follows from Proposition 2.55.

Corollary 2.58. Let M be a completely reducible left A-module. Then $\ell_A(M) < \infty$ if and only if M is a finitely generated A-module.

Proof. Let P be a simple left A-module. The module M is the direct sum of its isotypical components and the length of M is the sum of the $[M : P]_A$ where P is simple, hence without loss of generality, assume M is isotypical of type P. Then $\mathrm{Ann}_A(M) = \mathfrak{m}$ is a left maximal ideal where $A/\mathfrak{m} \simeq P$ and M is finitely generated if and only if we have a surjective morphism of A-modules $A_\ell^{\oplus r} \to M$, which by the latter is equivalent to a surjective morphism $(A_\ell/\mathfrak{m})^{\oplus r} \to M$. This implies $\ell_A(M) \leq r < \infty$, and conversely, $\ell_A(M) < \infty$ implies $M \simeq (A_\ell/\mathfrak{m})^{\oplus \ell_A(M)}$ is finitely generated.

Another way to prove this is as follows : write $M = \bigoplus_{i \in I} M_i$ as a direct sum decomposition into simple A-submodules. If I is finite, since each M_i is cyclic, M is finitely generated. Conversely, if M is finitely generated, a finite subset of M can only span a finite amount of the M_i's, thus I must be finite.

2.6 Centralizer and bicentralizer of a completely reducible module

Proposition 2.59. Let M be a completely reducible left A-module.

(i) The module M is simple (resp. isotypically simple) if and only if it is a simple (resp. isotypically simple) $C_A^2(M)$-module.

(ii) The A-submodules of M are precisely the $C_A^2(M)$-submodules of $M^{\lhd\lhd}$.

(iii) If M is an isotypically simple left A-module of type P where P is a simple A-submodule of M, then the restriction map $\varphi \mapsto \varphi|_P$ induces an isomorphism $C_A^2(M) \simeq C_A^2(P)$.

(iv) Let $\{M_P\}_{P \in I}$ be the isotypical components of M where I indexes a family of simple submodules of

M as in Theorem 2.50. The map

$$C_A^2(M) \to \prod_{P \in I} C_A^2(M_P), \quad \varphi \mapsto (\varphi|_{M_P})_{P \in I}$$

is an isomorphism.

Proof. Since $A_M \subseteq C_A^2(M)$, we already know that a $C_A^2(M)$-submodule of M is an A-submodule. Conversely, if $N \leq M$ is an A-submodule, then N is a direct summand, which means it is a $C_A^2(M)$-submodule by Proposition 1.31. Therefore, A-submodules and $C_A^2(M)$-submodules agree, so the notions of simple (resp. isotypically simple) agree in both cases (namely, over A and over $C_A^2(M)$), which proves part (i) and (ii). Part (iii) follows from Proposition 1.56. It remains to prove part (iv).

It is clear that the given map is injective since each M_P is a $C_A^2(M)$-submodule, so that $\varphi = \bigoplus_{P \in I} \varphi|_P$. For surjectivity, let $\varphi_P \in C_A^2(M_P)$. There exists a unique $\varphi \in \mathrm{End}_{\mathbb{Z}}(M)$ such that $\varphi|_P = \varphi_P$, so it suffices to show that $\varphi \in C_A^2(M)$. For each $\psi \in C_A(M) = \mathrm{End}_A(M)$, recalling Proposition 2.53, we see that $\psi(M_P) \subseteq M_P$, which implies that $\psi|_{M_P} \in C_A(M_P)$. Since $\varphi_P \in C_A^2(M_P)$, it commutes with $\psi|_{M_P}$, hence φ commutes with ψ, which completes the proof.

Remark 2.60. Equip M with the discrete topology and $\mathrm{End}_{\mathbb{Z}}(M)$ with the topology of pointwise convergence (or equivalently, the subspace topology coming from the inclusion $\mathrm{End}_{\mathbb{Z}}(M) \subseteq M^M = \mathrm{Hom}_{\mathbf{Set}}(M, M)$ where each copy of M has the discrete topology). The topology we just put $\mathrm{End}_{\mathbb{Z}}(M)$ makes it into a Hausdorff topological ring, meaning that addition and multiplication (given by composition of endomorphisms) is continuous ; this is obvious by using the definition of continuity via convergent sequences, and the Hausdorff property is obtained as follows : given $\varphi, \psi \in \mathrm{End}_{\mathbb{Z}}(M)$ distinct, they differ at at least one $m \in M$ (unless $M = 0$, in which case $\mathrm{End}_{\mathbb{Z}}(M) = 0$), so since M is Hausdorff, we can pick two neighborhoods U_φ of $\varphi(m)$ and U_ψ of $\psi(m)$. We then set

$$V_\varphi \stackrel{\text{def}}{=} \{\varphi' \in \mathrm{End}_{\mathbb{Z}}(M) \mid \varphi'(m) \in U_\varphi\}$$

and define V_ψ similarly. The V_φ and V_ψ are disjoint neighborhoods of φ and ψ in $\mathrm{End}_{\mathbb{Z}}(M)$.

Furthermore, if $S \subseteq \mathrm{End}_{\mathbb{Z}}(M)$, the centralizer $C_{\mathrm{End}_{\mathbb{Z}}(M)}(S)$ (c.f. Definition 1.20) is closed in $\mathrm{End}_{\mathbb{Z}}(M)$, for if $\varphi_n \in C_{\mathrm{End}_{\mathbb{Z}}(M)}(S)$ converges to $\varphi \in \mathrm{End}_{\mathbb{Z}}(M)$ and $\psi \in S$, we see that for all $m \in M$, there exists a large enough integer n_m such that

$$\varphi(\psi(m)) = \varphi_{n_m}(\psi(m)) = \psi(\varphi_{n_m}(m)) = \psi(\varphi(m)) \quad \Longrightarrow \quad \varphi \in C_{\mathrm{End}_{\mathbb{Z}}(M)}(S).$$

It follows that $C_A(M)$ and $C_A^2(M)$ are closed subrings of $\mathrm{End}_{\mathbb{Z}}(M)$, and we will now prove that A_M is dense in $C_A^2(M)$ when M is completely reducible ; this is called the **density theorem**. For two subsets $S_1, S_2 \subseteq \mathrm{End}_{\mathbb{Z}}(M)$, the equality $\overline{S_1} = S_2$ expresses the following : pick $\varphi_2 \in S_2$ arbitrary. A neighborhood base of φ_2 can be taken as

$$U_{m_1, \cdots, m_n} \stackrel{\text{def}}{=} \{\psi \in \mathrm{End}_{\mathbb{Z}}(M) \mid \forall 1 \leq j \leq n, \quad \psi(m_j) = \varphi_2(m_j)\} = \bigcap_{j=1}^n U_{m_j}.$$

Then $\overline{S_1} = S_2$ if and only if for every $m_1, \cdots, m_n \in M$ and $\varphi_2 \in S_2$, there exists $\varphi_1 \in S_1$ such that $\varphi_1(m_j) = \varphi_2(m_j)$ for $1 \leq j \leq n$. The equality $\overline{A_M} = C_A^2(M)$ now boils down to the statement of the density theorem given below.

Lemma 2.61. Let M be a completely reducible left A-module, $\psi \in C_A^2(M)$ and $m \in M$. There exists $a \in A$ such that $\psi(m) = am$.

Proof. This is because the A-submodule ${}_A\langle m\rangle$ is also a $C_A^2(M)$-submodule by Proposition 2.59, which means that $\psi(m) \in {}_A\langle m\rangle$ can be written in the form am for some $a \in A$.

Theorem 2.62. (Density theorem) Let M be a completely reducible left A-module, $\psi \in C_A^2(M)$ and $m_1, \cdots, m_n \in M$. There exists $a \in A$ such that $\psi(m_j) = am_j$ for all $1 \leq j \leq n$.

Proof. Consider the bicentralizer of $M^{\oplus n}$. If $P \leq M$ is a simple submodule, then we have a canonical isomorphism $(M^{\oplus n})_P \simeq (M_P)^{\oplus n}$, which induces a canonical isomorphism

$$C_A^2(M) \simeq \prod_P C_A^2(P) \simeq C_A^2(M^{\oplus n})$$

by Proposition 2.59, which is essentially given by $\psi \mapsto \psi^{\oplus n} \overset{\text{def}}{=} (\psi, \cdots, \psi)$. Applying Lemma 2.61 to $M^{\oplus n}$, $\psi^{\oplus n}$ and $(m_1, \cdots, m_n)$, we see that there exists $a \in A$ such that $\psi(m_j) = am_j$, as desired.

Corollary 2.63. Let M be a completely reducible left A-module. When $M^{\triangleleft}$ is a finitely generated $\mathrm{End}_A(M)$-module, we have the equality $A_M = C_A^2(M)$.

Proof. Let $\{m_1, \cdots, m_n\}$ be a set of generators for $M^{\triangleleft}$. By the density theorem, for each $\varphi \in C_A^2(M)$, there exists $a \in A$ such that $\varphi|_{\{m_1,\cdots,m_n\}} = a_M|_{\{m_1,\cdots,m_n\}}$. Since both φ and a_M are endomorphisms of $M^{\triangleleft}$ by definition of $C_A(M)$ and $C_A^2(M)$, this means that $\varphi = a_M$, which implies $A_M = C_A^2(M)$.

Corollary 2.64. Let $M_1, \cdots, M_n$ be pairwise non-isomorphic simple left A-modules such that each $M_i{}^{\triangleleft}$ is finitely generated. If $a_1, \cdots, a_n \in A$, there exists $a \in A$ such that $a_{M_i} = (a_i)_{M_i}$ for $1 \leq i \leq n$.

Proof. It suffices to see that the isotypical components of $M \overset{\text{def}}{=} \bigoplus_{i=1}^n M_i$ are the M_i's and that $M^{\triangleleft}$ is finitely generated (because $\mathrm{End}_A(M) \simeq \prod_{i=1}^n \mathrm{End}_A(M_i)$ by Proposition 2.53), which implies

$$A_M = C_A^2(M) \simeq \prod_{i=1}^n C_A^2(M_i) = \prod_{i=1}^n A_{M_i}$$

by Proposition 2.59 and the previous corollary.

2.7 Centralizer of a simple module

Theorem 2.65. (Schur's Lemma) Let M, N be two left A-modules and $f : M \to N$ be a morphism not identically zero.

(i) If M is simple, f is injective.

(ii) If N is simple, f is surjective.

(iii) If both M and N are simple, f is an isomorphism.

As a result, when M is a simple A-module, $\mathrm{End}_A(M)$ is a skew field.

Proof. The first three parts follow from the fact that $\ker f \leq M$ and $\operatorname{im} f \leq N$. Setting $M = N$, we see that every non-zero endomorphism of M is an isomorphism, meaning that for each $f \in \mathrm{End}_A(M) \setminus \{0\}$, $f^{-1} \in \mathrm{End}_A(M)$ satisfies $ff^{-1} = f^{-1}f = \mathrm{id}_M$, completing the proof.

It follows that when M is simple, $M^{\triangleleft}$ is a left $C_A(M)$-vector space. Note that $C_A^2(M) = C_{C_A(M)}(M^{\triangleleft}) = \mathrm{End}_{C_A(M)}(M^{\triangleleft})$ is precisely the set of $C_A(M)$-linear endomorphisms of this vector space.

Lemma 2.66. Let K be an algebraically closed field and D be a skew field which is also a K-algebra of finite dimension. Then $D = K$.

Proof. Let $x \in D$. Denote by $K(x)$ the smallest skew field of D generated by K and x, or in other words, the set of all $y \in D$ which can be written as a product of polynomials in x and their inverses. This K-algebra is by definition a skew field which is commutative, and therefore is a finite field extension of K since D is finite over K. The fact that K is algebraically closed implies that every algebraic extension of K is equal to K, therefore $K(x) = K$, meaning that $x \in K$.

Corollary 2.67. (Burnside's Theorem) Let K be an algebraically closed field, A a K-algebra and M a simple left A-module which is finite-dimensional over K (via its A-module structure). Then $A_M = C_A^2(M) = \mathrm{End}_K(M)$ and $C_A(M) = K_M = K$ is the ring of homotheties of M seen as a K-module.

Proof. It suffices to see that $C_A(M) = K_M$ since the fact that K is a field implies $K_M = K$ (because $M \neq 0$ and $\mathrm{Ann}_A(M) \trianglelefteq K$) and the other statements in the theorem follow from Corollary 2.63. The inclusions

$$K_M \subseteq C_A(M) = \mathrm{End}_A(M) \subseteq \mathrm{End}_K(M)$$

finish the proof by Lemma 2.66 since $\mathrm{End}_A(M)$ is a skew field and a K-algebra of finite rank (because $\dim_K \mathrm{End}_K(M) = (\dim_K M)^2 < \infty$ by assumption on M).

Corollary 2.68. Let K be an algebraically closed field, A a K-algebra and $M_1, \cdots, M_n$ be pairwise non-isomorphic simple left A-modules which are finite-dimensional over K (via their A-module structure). Given $c_i \in \mathrm{End}_K(M_i)$ for $1 \le i \le n$, there exists $a \in A$ such that $a_{M_i} = c_i$ for all $1 \le i \le n$. In other words, the map $A \to \prod_{i=1}^n \mathrm{End}_K(M_i)$ given by restriction ($a \mapsto (a_{M_1}, \cdots, a_{M_n})$) is surjective.

Proof. By Proposition 2.53, we know that $M \overset{\text{def}}{=} \bigoplus_{i=1}^n M_i$ is finitely generated over

$$C_A(M) = \prod_{i=1}^n C_A(M_i) = \prod_{i=1}^n K_{M_i} = K^{\oplus n}$$

because it is finite-dimensional over K ; the result follows from Corollary 2.64.

Chapter 3

Simple and semisimple rings

In this chapter, A denotes a ring and D denotes a division ring.

3.1 Left & right vector spaces over a skew field

We treat the particular case of D-modules when D is a skew field (the letter D stands for "division ring").

Definition 3.1. Let D be a division ring. A **left D-vector space** (resp. **right D-vector space**) is a left D-module (resp. right D-module). In this section, we denote a left D-vector space by the letter V. Submodules are called **vector subspaces** and elements of V are called **vectors**.

A **basis** for a left D-vector space V is a subset $S \subseteq V$ such that $V = \bigoplus_{s \in S} {}_D\langle s \rangle$. A subset $L \subseteq V$ is called **linearly independent** if it is a basis of ${}_D\langle L \rangle$. A subset $S \subseteq V$ is said to **span** V or to be a **generating subset of** V if ${}_D\langle S \rangle = V$.

Lemma 3.2. Every cyclic left D-vector space is simple and there is only one isomorphism class of simple left D-vector spaces ; they are all isomorphic to D_ℓ.

> ***Proof.*** Let V be a cyclic D-module and $v \in V$ be a generator. If $0 \lneq W \leq V$ is a non-zero vector subspace, by hypothesis we can write an element $w \in W \setminus \{0\}$ in the form dv for some $d \in D$. Then $v = d^{-1}(dv) = d^{-1}w \in W$, meaning that $W \supseteq V$, i.e. $W = V$.
>
> If V is simple, then the map $\varphi_v : D_\ell \to V$ defined by $\varphi_v(d) = dv$ is left D-linear and non-zero when $v \in V \setminus \{0\}$ because $\varphi_v(d'd) = d'dv = d'\varphi_v(d)$, meaning that it is an isomorphism $D_\ell \simeq V$.

Theorem 3.3. Every left D-vector space V has a basis. More precisely, if $L \subseteq S \subseteq V$ are two subsets where L is linearly independent (i.e. L is a basis of the vector space ${}_D\langle L \rangle$) and S is a generating subset of V, there exists a basis B for V such that $L \subseteq B \subseteq S$.

> ***Proof.*** Consider the vector subspace $W \stackrel{\text{def}}{=} {}_D\langle L \rangle$ and the family of simple D-submodules $\{{}_D\langle s \rangle\}_{s \in S}$. By Lemma 3.2, we see that V is the sum of its simple submodules, hence is semisimple by Theorem 2.44. By Theorem 2.43 applied to the family $\{{}_D\langle s \rangle\}_{s \in S}$ and the vector subspace W, we see that there exists a subset $L' \subseteq S$ such that $V = W \oplus \bigoplus_{\ell' \in L'} {}_D\langle \ell' \rangle$. This means that $B \stackrel{\text{def}}{=} L \cup L'$ is a basis for V since L is a basis for W. By definition, $L \subseteq B \subseteq S$, so we are done. To prove that V admits a basis, set $L = \varnothing$ and $S = V$.

Definition 3.4. Let V be a left D-vector subspace. Since V is isotypically simple of type D_ℓ, the **dimension** of V is defined as its length as a left D-module (c.f. Definition 2.56), namely $\dim_D V \stackrel{\text{def}}{=} \ell_D(V)$. The dimension of V equals the cardinality of any basis for V by Theorem 3.3. The **codimension** of $W \leq V$ is written $\operatorname{codim}_D(W, V)$ and is defined as $\dim_D(V/W)$. If $f : V \to W$ is a D-linear map, the **rank** of f is given by $\operatorname{rk}(f) \stackrel{\text{def}}{=} \dim_D \operatorname{im} f$.

Corollary 3.5. Let V be a left D-vector space.

(i) The vector space V is finite-dimensional if and only if it is finitely generated.

(ii) Two left D-vector spaces are isomorphic if and only if they have the same dimension.

(iii) A linearly independent subset $L \subseteq V$ is a basis if and only if it is maximal among the set of linearly independent subsets of V.

(iv) A generating subset $S \subseteq V$ is a basis if and only if it is minimal among the set of generating subsets of V.

(v) Dimension is additive : if $V = \bigoplus_{i \in I} V_i$, then $\dim V = \sum_{i \in I} V_i$.

(vi) Every vector subspace $W \leq V$ admits a complement, namely a subspace $W' \leq V$ such that $V = W \oplus W'$. In particular every short exact sequence of vector spaces splits.

Proof. For part (i), this follows from Theorem 3.3 (if it is finitely generated, the finite set of generators contains a basis). Part (ii) follows from Corollary 2.57 and parts (iii) and (iv) follow from Theorem 3.3. Part (v) follows since a basis B for V can be given by taking a union of bases B_i for each V_i, so that $B = \bigcup_{i \in I} B_i$ satisfies

$$\dim_D V = |B| = \sum_{i \in I} |B_i| = \sum_{i \in I} \dim_D V_i.$$

Part (vi) follows from the fact that V is completely reducible.

Proposition 3.6. Let A be a ring and $\varphi : A \to D$ be a morphism of rings where D is a division ring. If E is a free left A-module, then any two bases for E have the same cardinality.

Proof. Turn D into a (D, A)-bimodule by $da \stackrel{\text{def}}{=} d\varphi(a)$. Consider the left D-vector space $V \stackrel{\text{def}}{=} D \otimes_A E$. If B is a basis for E, then $1 \otimes B \stackrel{\text{def}}{=} \{1 \otimes b \mid b \in B\}$ is a basis for V of the same cardinality. Therefore, any two bases B, B' of E induce two bases $1 \otimes B, 1 \otimes B'$ of V which are of the same cardinality, implying $|B| = |B'|$.

Corollary 3.7. Let A be a commutative ring. If E is a free A-module, any two bases for E have the same cardinality.

Proof. By Krull's theorem, A admits a maximal ideal $\mathfrak{m}$, so we can apply Proposition 3.6 to the projection $\pi_{\mathfrak{m}} : A \to A/\mathfrak{m}$ where $A/\mathfrak{m}$ is a field.

Proposition 3.8. Let

$$0 \longrightarrow V_1 \longrightarrow V_2 \longrightarrow \cdots \longrightarrow V_n \longrightarrow 0$$

be an exact sequence of finite-dimensional left D-vector spaces. Then

$$\sum_{i=1}^{n} (-1)^i \dim_D V_i = 0.$$

Proof. By induction on n. If $n = 1$ or $n = 2$, there is nothing to prove. Consider the new sequence whose beginning is replaced by

$$0 \longrightarrow V_2/V_1 \longrightarrow V_3 \longrightarrow \cdots \longrightarrow V_n \longrightarrow 0.$$

It is still exact, hence $-\dim_D(V_2/V_1) + \sum_{i=3}^n (-1)^{i-1} \dim_D V_i = 0$. Since $\dim_D(V_2/V_1) = \dim_D V_2 - \dim_D V_1$ by the case $n = 2$, substituting and multiplying by -1 gives $\sum_{i=1}^n (-1)^i \dim_D V_i = 0$.

Corollary 3.9. Let W_1, W_2 be two vector subspaces of a left D-vector space V. We have the formula

$$\dim_D(W_1 + W_2) + \dim_D(W_1 \cap W_2) = \dim_D W_1 + \dim_D W_2.$$

Proof. It suffices to apply Proposition 3.8 to the exact sequence

$$0 \longrightarrow W_1 \cap W_2 \longrightarrow W_1 \oplus W_2 \longrightarrow W_1 + W_2 \longrightarrow 0.$$

where the second map is given by the difference between the two inclusions $\iota_{W_i} : W_i \to V$.

Corollary 3.10. Let V be a finite-dimensional left D-vector space and $\{W_i\}_{i \in I}$ a family of vector subspaces satisfying $\sum_{i \in I} W_i = V$. We have the inequality

$$\dim_D V \leq \sum_{i \in I} \dim_D W_i.$$

Proof. Since V is finite-dimensional, we can assume without loss of generality that I is finite. Write the family as $W_1, \cdots, W_n$. By induction on n and replacing the family $W_1, \cdots, W_{n-1}$ by $\sum_{i=1}^{n-1} W_i$, it suffices to restrict to the case $n = 2$, which follows from Corollary 3.9.

Theorem 3.11. (Rank-nullity formula) Let $f : V \to W$ be a D-linear map between left D-vector spaces. Then

$$\mathrm{rk}(f) + \dim \ker f = \dim V, \quad \mathrm{rk}(f) + \dim \operatorname{coker} f = \dim W.$$

As a corollary, $\mathrm{rk}(f) \leq \min\{\dim_D V, \dim_D W\}$.

Proof. Write $V = \ker f \oplus W'$ and $W = \operatorname{im} f \oplus W'$, so that

$$\operatorname{im} f \simeq V/\ker f \simeq W', \quad \operatorname{coker} f \simeq W/\operatorname{im} f,$$

hence by taking dimensions, we obtain both equalities.

Proposition 3.12. Let V be a finite-dimensional left D-vector space and $f \in \mathrm{End}_D(V)$. The following are equivalent :

(i) The endomorphism f is bijective

(ii) The endomorphism f is injective

(iii) The endomorphism f is surjective

(iv) The endomorphism f admits a left-inverse

(v) The endomorphism f admits a right-inverse

(vi) The endomorphism f is an isomorphism.

(vii) $\mathrm{rk}(f) = \dim_D V$.

Proof. Obvious from the rank-nullity formula.

Example 3.13. Let $n, m, p \geq 1$ be three integers and $f : D_\ell^{\oplus m} \to D_\ell^{\oplus n}$ and $g : D_\ell^{\oplus n} \to D_\ell^{\oplus p}$ be two D-linear maps which are determined by their matrix forms, constructed as follows : if $\{v_1, \cdots, v_m\}$ is the standard basis of $D_\ell^{\oplus m}$ and $\{w_1, \cdots, w_n\}$ is the standard basis of $D_\ell^{\oplus n}$, defining coefficients $b_{ij} \in D$ via the equations $f(v_j) = \sum_{i=1}^n a_{ij} w_i$, for any $d_1, \cdots, d_m \in D$, we have

$$f\left(\sum_{j=1}^m d_j v_j\right) = \sum_{j=1}^m d_j f(v_j) = \sum_{j=1}^m d_j f(v_j) = \sum_{j=1}^m d_j \left(\sum_{i=1}^n b_{ij} w_i\right) = \sum_{i=1}^n \left(\sum_{j=1}^m d_j b_{ij}\right) w_i.$$

Repeating this computation in an analogous manner, we deduce that if (b_{ij}) is the matrix form of f and (a_{ij}) is the matrix form of g, then the matrix form of $g \circ f$ corresponds to the following matrix multiplication :

$$\begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{p1} & \cdots & a_{pn} \end{bmatrix} \circ \begin{bmatrix} b_{11} & \cdots & b_{1m} \\ \vdots & \ddots & \vdots \\ b_{n1} & \cdots & b_{nm} \end{bmatrix} = [a_{ij}][b_{ij}] = \left[\sum_{k=1}^n b_{ik} a_{kj}\right].$$

Note that $\circ$ is not usual matrix multiplication, but matrix multiplication where multiplication of coefficients is performed in D^{opp} rather than in D. It follows from this example that the isomorphism of rings $\mathrm{End}_D(D_\ell) \simeq D^{\mathrm{opp}}$ of Proposition 1.28 extends to the isomorphism $\mathrm{End}_D(D_\ell^{\oplus n}) \simeq \mathrm{Mat}_{n\times n}(D^{\mathrm{opp}})$.

3.2 Centralizer of a completely reducible module

We go back to the situation where A is a ring.

Proposition 3.14. Let P be a simple A-module and M an isotypically simple module of type P. Consider the rings $\mathrm{End}_A(P)$ and $\mathrm{End}_A(M)$ (recall that $\mathrm{End}_A(P)$ is a division ring since P is a simple A-module).

(i) The A-module $\mathrm{Hom}_A(P, M)$ can be given the structure of a $(\mathrm{End}_A(M), \mathrm{End}_A(P))$-bimodule (c.f. Remark 1.47), i.e. it is a left $\mathrm{End}_A(M)$-module, a right $\mathrm{End}_A(P)$-vector space and both module structures are compatible.

(ii) The canonical morphism $\mathrm{End}_A(M) \to \mathrm{End}_{\mathrm{End}_A(P)}(\mathrm{Hom}_A(P, M))$ induced by the $\mathrm{End}_A(M)$-module structure on $\mathrm{Hom}_A(P, M)$ (compatible with the $\mathrm{End}_A(P)$-module structure, hence multiplication by an element of $\mathrm{End}_A(M)$ is $\mathrm{End}_A(P)$-linear) is an isomorphism of rings. The $\mathrm{End}_A(M)$-module $\mathrm{Hom}_A(P, M)$ is simple and its centralizer satisfies

$$C_{\mathrm{End}_A(M)}(\mathrm{Hom}_A(P, M)) \simeq \mathrm{End}_A(P)^{\mathrm{opp}}.$$

(iii) The canonical map $\mathrm{Hom}_A(P, M) \otimes_{\mathrm{End}_A(P)} P \to M$ given by $\varphi \otimes p \mapsto \varphi(p)$ is an isomorphism of left A-modules and of left $\mathrm{End}_A(M)$-modules.

(iv) The $\mathrm{End}_A(M)$-module $M^{\triangleleft}$ is isotypical of type $\mathrm{Hom}_A(P, M)$.

(v) We have the formulas

$$\ell_A(M) = \dim_{\mathrm{End}_A(P)} \mathrm{Hom}_A(P, M), \quad \ell_{\mathrm{End}_A(M)}(M^{\triangleleft}) = \dim_{\mathrm{End}_A(P)} P.$$

(vi) The left A-submodules of M and the $\mathrm{End}_A(P)$-vector subspaces of $\mathrm{Hom}_A(P,M)$ are in one-to-one correspondence via the formulas

$$(M' \leq M) \mapsto \mathrm{Hom}_A(P,M') \subseteq \mathrm{Hom}_A(P,M), \quad (V \leq \mathrm{Hom}_A(P,M)) \mapsto V \otimes_{\mathrm{End}_A(P)} P \subseteq M,$$

the inclusions being produced by the canonical maps : the inclusion $\mathrm{Hom}_A(P,M') \subseteq \mathrm{Hom}_A(P,M)$ is given by post-composition with the inclusion map $M' \subseteq M$ and the inclusion $V \otimes_{\mathrm{End}_A(P)} M \subseteq M$ is given by recalling that $V \subseteq \mathrm{Hom}_A(P,M)$, so we can map a product $\varphi \otimes p \in V \otimes_{\mathrm{End}_A(P)} P$ to the composition $\varphi(p)$, which is injective by part (iii).

Proof. Part (i) follows from Proposition 2.59. Since P is a cyclic A-module, the map $\mathrm{End}_A(M) \to \mathrm{End}_{\mathrm{End}_A(P)}(\mathrm{Hom}_A(P,M))$ is an isomorphism by letting the pair (P,M) play the role of the pair (M,V) in Theorem 1.59 (vi). Since $\mathrm{End}_A(P)$ is a skew field, $\mathrm{Hom}_A(P,M)$ is a simple $\mathrm{End}_{\mathrm{End}_A(P)}(\mathrm{Hom}_A(P,M))$-module (this is the fact that given two vectors in a vector space V, there is an endomorphism of V mapping one vector to the other), hence a simple $\mathrm{End}_A(M)$-module by part (i).

We can use the fact that $\mathrm{Hom}_A(P,M)$ is a free $\mathrm{End}_A(P)$-module to apply Corollary 1.38 and deduce that

$$\begin{aligned} &\mathrm{End}_A(M) \simeq \mathrm{End}_{\mathrm{End}_A(P)}(\mathrm{Hom}_A(P,M)) = C_{\mathrm{End}_A(P)}(\mathrm{Hom}_A(P,M)) \\ \implies \quad & C_{\mathrm{End}_A(M)}(\mathrm{Hom}_A(P,M)) \simeq C^2_{\mathrm{End}_A(P)}(\mathrm{Hom}_A(P,M)) = \mathrm{End}_A(P)_{\mathrm{Hom}_A(P,M)} = \mathrm{End}_A(P)^{\mathrm{opp}}. \end{aligned}$$

The A-linearity and $\mathrm{End}_A(M)$-linearity of the map given in part (iii) is obvious ; it is an isomorphism by Theorem 1.59 (v). If we fix an isomorphism of A-modules $M \simeq P^{\oplus I}$, we obtain an isomorphism of $\mathrm{End}_A(P)$-modules

$$\mathrm{Hom}_A(P,M) \simeq \mathrm{Hom}_A(P,P^{\oplus I}) \simeq \mathrm{End}_A(P)^{\oplus I},$$

which implies $\ell_A(M) = \dim_{\mathrm{End}_A(P)} \mathrm{Hom}_A(P,M)$.

Considering P as a right $\mathrm{End}_A(P)^{\mathrm{opp}}$-module and $\mathrm{Hom}_A(P,M)$ as a left $\mathrm{End}_A(P)^{\mathrm{opp}}$-module, we can identify $\mathrm{Hom}_A(P,M) \otimes_{\mathrm{End}_A(P)} P$ with $P \otimes_{\mathrm{End}_A(P)^{\mathrm{opp}}} \mathrm{Hom}_A(P,M)$; this identification is $\mathrm{End}_A(M)$-linear. Note that the action of $\mathrm{End}_A(P)^{\mathrm{opp}}$ on $\mathrm{Hom}_A(P,M)$ corresponds to the action of $C_{\mathrm{End}_A(M)}(\mathrm{Hom}_A(P,M))$ by part (ii) and P is a free $\mathrm{End}_A(P)^{\mathrm{opp}}$-module since $\mathrm{End}_A(P)^{\mathrm{opp}}$ is a division ring. By applying Theorem 1.59 (i) to this situation, the role of the triple (A,M,W) there being replaced by that of $(\mathrm{End}_A(M), \mathrm{Hom}_A(P,M), P)$ here, we see that

$$P \otimes_{\mathrm{End}_A(P)^{\mathrm{opp}}} \mathrm{Hom}_A(P,M) \simeq \mathrm{Hom}_A(P,M) \otimes_{\mathrm{End}_A(P)} P \simeq M^{\triangleleft}$$

is an isotypical $\mathrm{End}_A(M)$-module of type $\mathrm{Hom}_A(P,M)$. Part (vi) is a corollary of Theorem 1.59 because every subspace of $\mathrm{Hom}_A(P,M)$ is free and every submodule of M is isotypical of type P.

Corollary 3.15. Let P be a simple left A-module ; recall that $D \stackrel{\text{def}}{=} C_A(P)$ is a division ring by Schur's Lemma and that $P^{\triangleleft}$ is a left D-vector space. Let V be a right $C_A(P)$-vector space (so that $V \otimes_D P^{\triangleleft}$ is a left A-module by multiplication on elements of P) and $S \subseteq \mathrm{End}_D(V)$ be a subset. Given $\varphi \in \mathrm{End}_D(V)$, we can extend this to an endomorphism $\varphi \otimes \mathrm{id}_S \in \mathrm{End}_A(V \otimes_D P^{\triangleleft})$ by $(\varphi \otimes \mathrm{id}_S)(v \otimes p) \stackrel{\text{def}}{=} \varphi(v) \otimes p$. For an A-submodule $N \leq V \otimes_D P^{\triangleleft}$, the following are equivalent :

(i) The submodule N is left invariant by every $\varphi \in S$, i.e. $(\varphi \otimes \mathrm{id}_P)(N) \subseteq N$

(ii) The submodule N has the form $W \otimes_D P^{\triangleleft}$ where $W \leq V$ is a D-vector subspace left invariant by every $\varphi \in S$, i.e. $\varphi(W) \subseteq W$.

Proof. Find a set I such that $V \simeq d^{\oplus I}$ and let $M \stackrel{\text{def}}{=} P^{\oplus I}$. Note that we have an identification

$$V \simeq D^{\oplus I} = \mathrm{End}_A(P)^{\oplus I} \subseteq \mathrm{Hom}_A(P, P^{\oplus I}) = \mathrm{Hom}_A(P, M).$$

given by summing the maps $(\varphi_i)_{i\in I} \in \mathrm{End}_A(P)^{\oplus I}$ to get a map $\bigoplus_{i\in I} \varphi_i : P \to P^{\oplus I}$; this inclusion is also right D-linear, so V can be seen as a D-vector subspace of $\mathrm{Hom}_A(P, M)$. It follows that the functor $(-) \otimes_D P$ applied to this inclusion preserves its injectivity (because the corresponding exact sequence of D-modules is split), so we get an inclusion

$$V \otimes_D P \subseteq \mathrm{Hom}_A(P, M) \otimes_D P \simeq M$$

by Proposition 3.14 (iii). By Proposition 3.14 (vi), the left A-submodules of M are in an inclusion-preserving bijection with the right D-vector subspaces of $\mathrm{Hom}_A(P, M)$, so the left A-submodules of $V \otimes_D P$ are in bijection with the right D-vector subspaces of V. By writing $N = W \otimes_D P$, we see that N is stable under the endomorphisms $\varphi \otimes \mathrm{id}_P$ for all $\varphi \in S$ if and only if W is stable under the endomorphisms $\varphi \in S$, which proves the equivalence.

Corollary 3.16. Let E be a division ring and S be a family of ring endomorphisms of E. Note that for each $\varphi \in S$, $\varphi(E) \subseteq E$ is isomorphic to E (via the map $\varphi : E \to \varphi(E)$), so it is a division subring of E. Let $D \stackrel{\text{def}}{=} E^S$ be the set of $e \in E$ which are left invariant by each $\varphi \in S$ (i.e. $\varphi(e) = e$ for all $\varphi \in S$). Note that D is a division ring (because E is). For a right D-vector space V, we turn $V \otimes_D E$ into a left E-vector space. For an E-vector subspace $U \leq V \otimes_D E$, the following are equivalent :

(i) The subspace U is stable under every endomorphism of the form $\mathrm{id}_V \otimes \varphi$ for $\varphi \in S$

(ii) There exists a D-vector subspace $W \leq V$ such that $U = W \otimes_D E$.

Proof. Consider the $\mathbb{Z}$-subalgebra A of $\mathrm{End}_{\mathbb{Z}}(E)$ generated by S and $(E_r)_E$, the ring of homotheties of the right E-module E ; note that in A, the multiplication of two right homotheties is not given by multiplication in E but by composition in $\mathrm{End}_{\mathbb{Z}}(E)$, so E is a left A-module (even though we are acting by homotheties on the right) ; if e_{E_r} denotes multiplication by $e \in E$ on the right, the left-A-linearity of multiplication by $e_{E_r} \in A$ is reflected in the equation

$$(e_{E_r} \circ e'_{E_r})(e'') = e_{E_r}(e'_{E_r}(e'')).$$

The left A-module E is simple since $(E_r)_E \subseteq A$ and the right E-module E_r is simple. We also see that $C_A(E) \subseteq C_E(E_r)$ since if $\psi \in \mathrm{End}_{\mathbb{Z}}(E)$ commutes with all elements of A, it commutes in particular with all elements of $(E_r)_E$, i.e. is a right E-linear map. But we have seen that as sets, $C_E(E_r) = E_{E_\ell}$ (c.f. Proposition 1.28 ; we said "as sets" because we need to add "$^{\mathrm{opp}}$" to get an isomorphism of rings), so $C_A(E) \subseteq (E_\ell)_E$. This means that if $\psi \in C_A(E)$, then there exists $e_\psi \in E$ such that $\psi(e') = e_\psi e'$ and for all $\varphi \in S$,

$$e_\psi = e_\psi \varphi(1) = \psi(\varphi(1)) = \varphi(\psi(1)) = \varphi(e_\psi) \quad \implies \quad e_\psi \in D.$$

Conversely, if $e_\psi \in D$, then $\psi \in C_A(E)$, so it follows that $C_A(E) = (E_\ell)_D$ is the ring of homotheties of E seen as a left D-module and can therefore be identified with D. The result now follows from Corollary 3.15.

Proposition 3.17. Let M be a completely reducible with decomposition into isotypical components written as $M = \bigoplus_P M_P$. Then $M^\triangleleft = \bigoplus_P (M_P)^\triangleleft$ is also a decomposition of $M^\triangleleft$ into isotypical components, each $(M_P)^\triangleleft$ being isotypically simple of type $\mathrm{Hom}_A(P, M_P)$ by Proposition 3.14 (iv). In particular, if M is completely reducible, then $M^\triangleleft$ is also completely reducible.

Proof. First of all, recall that by Proposition 2.53 (ii),

$$C_A(M) = \mathrm{End}_A(M) = \prod_P \mathrm{End}_A(M_P) = \prod_P C_A(M_P)$$

where the identification is given by $\varphi \mapsto (\varphi|_{M_P})_P$. Since each M_P is isotypical, we can apply Proposition 3.14 (iv) and deduce that $(M_P)^{\triangleleft}$ is also an isotypical $C_A(M_P)$-module, hence an isotypical $C_A(M)$-submodule of M. Since M_P is stable under $C_A^2(M) = C_A(M^{\triangleleft})$ by Proposition 1.31, it is a sum of isotypical components of $M^{\triangleleft}$ by Corollary 2.54, but since $(M_P)^{\triangleleft}$ is itself isotypical, $(M_P)^{\triangleleft}$ is an isotypical component of $M^{\triangleleft}$.

3.3 Semisimple rings

Proposition 3.18. Let A be a ring. The following are equivalent :

(i) Every left A-module is completely reducible

(ii) The A-module A_ℓ is completely reducible.

A ring A with these properties is called **semisimple**.

Proof. The implication ((ii) $\Rightarrow$ (i)) is obvious. For the converse, note that every left A-module is isomorphic to the quotient of an isotypical module of type A_ℓ by choosing a set of generators, so the result follows from the fact that the direct sum and quotient of completely reducible modules is completely reducible.

Corollary 3.19. If $\varphi : A \to B$ is a surjective morphism of rings and A is semisimple, then B is semisimple. In particular, if $\mathfrak{a} \trianglelefteq A$ is a two-sided ideal and A is semisimple, then $A/\mathfrak{a}$ is semisimple.

Proof. The morphism turns B into an A-module which is completely reducible, so in particular B_ℓ is completely reducible, which means B is semisimple.

Remark 3.20. Let A be a semisimple ring.

(i) Since A_ℓ is a cyclic A-module (being generated by $1 \in A$) and semisimple, it is of finite length by Corollary 2.58, hence A_ℓ is left-artinian and left-noetherian.

(ii) The opposite ring A^{opp} is also semisimple, thus there is no necessity of defining the notions of "left-semisimple" and "right-semisimple". To see this, note that $(A^{\mathrm{opp}})_\ell \simeq A_r = (A_\ell)^{\triangleleft}$ by Proposition 1.28. But then the fact that A_ℓ is semisimple implies that $(A_\ell)^{\triangleleft}$ is semisimple by Proposition 3.17.

Proposition 3.21. Let M be a left A-module such that $M^{\triangleleft}$ is finitely generated. The following are equivalent :

(i) The module M is completely reducible.

(ii) The ring of homotheties A_M is semisimple.

Proof. The implication ((ii) $\Rightarrow$ (i)) is trivial since M is a left A_M-module. Conversely, if M is completely reducible, $(A_M)_\ell$ is isomorphic to a submodule of $M^{\oplus n}$ by Proposition 2.30, hence A_M is semisimple.

Corollary 3.22. Let D be a division ring and V a finite-dimensional left D-vector space. Let A be a subring of the ring of endomorphisms $\mathrm{End}_D(V)$. Then the following are equivalent :

(i) The A-module V is completely reducible.

(ii) The ring A is semisimple.

In particular, this is true if $D = K$ is a field and A is a K-subalgebra of $\mathrm{End}_K(V)$.

Proof. Note that $D \subseteq \mathrm{End}_A(V)$ since $A \subseteq \mathrm{End}_D(V)$; this implies that $V^{\triangleleft}$ is finitely generated since it is a finite-dimensional D-vector space. The $\mathrm{End}_D(V)$-module V is faithful, so $A = A_V$ is semisimple if and only if V is a completely reducible A-module by Proposition 3.21.

Proposition 3.23. A ring A is semisimple if and only if it is isomorphic to the endomorphism ring of a completely reducible B-module M of finite length for some ring B.

Proof. ($\Rightarrow$) If M is a completely reducible B-module, so is $M^{\triangleleft}$ by Proposition 3.17. Since $M^{\triangleleft\triangleleft}$ is finitely generated (because M is by its complete reducibility and $B_M \subseteq C_B^2(M)$), we deduce that $A \simeq \mathrm{End}_B(M) = C_B(M)_{M^{\triangleleft}}$ is semisimple by Proposition 3.21.

($\Leftarrow$) If A is semisimple, then by Remark 3.20, so is

$$A^{\mathrm{opp}} \simeq (A_{A_r})^{\mathrm{opp}} \simeq C_A(A_\ell) = \mathrm{End}_A(A_\ell).$$

by Proposition 1.28. The left A-module A_ℓ is semisimple, so this means A is isomorphic to the endomorphism ring of the semisimple left A-module A_ℓ.

Proposition 3.24. Let A be a semisimple ring. The isotypical components of A_ℓ, the isotypical components of A_r and the minimal two-sided ideals of A all coincide (by “minimal”, we mean “minimal with respect to being non-zero under the partial order given by inclusion”).

Proof. The two-sided ideals of A are the left A-submodules of A_ℓ stable under multiplication on the right by A, i.e. table under A_{A_r}, or equivalently, under $(A_{A_r})^{\mathrm{opp}} \simeq C_A(A_\ell)$ by Proposition 1.28. It follows from Corollary 2.54 that the two-sided ideals of A are precisely the sum of isotypical components of A_ℓ, so the minimal two-sided ideals of A are the isotypical components of A_ℓ. By repeating the process with A_r, we come to the same conclusion.

Proposition 3.25. Let A be a semisimple ring. Every simple left A-module is isomorphic to a minimal left ideal of A.

Proof. Let M be a simple left A-module. There exists a left maximal ideal $\mathfrak{m}$ such that $M \simeq A_\ell/\mathfrak{m}$, but since A_ℓ is a semisimple left A-module, $A_\ell = \mathfrak{m} \oplus \mathfrak{n}$ for some left ideal $\mathfrak{n} \leq A_\ell$. The left A-module $\mathfrak{n}$ is also completely reducible, so the maximality of $\mathfrak{m}$ implies the minimality of $\mathfrak{n}$. Apply the argument symmetrically for the case of right A-modules.

Proposition 3.26. Let A be a semisimple ring. For every left ideal $\mathfrak{a} \trianglelefteq A$, there exists an idempotent $e_{\mathfrak{a}} \in \mathfrak{a}$ such that $\mathfrak{a} = {}_A(e_{\mathfrak{a}}) = \mathfrak{a}e_{\mathfrak{a}}$ and $1 = e_{\mathfrak{a}} + e_{\mathfrak{a}'}$ where $\mathfrak{a}'$ is a supplementary left ideal to $\mathfrak{a}$, i.e. $A = \mathfrak{a} \oplus \mathfrak{a}'$.

Proof. Let $\mathfrak{a}' \leq A_\ell$ be a supplementary left ideal of $\mathfrak{a}$ in A, so that $A = \mathfrak{a} \oplus \mathfrak{a}'$. By Corollary 1.18, the family of projections $\{\pi_{\mathfrak{a}}, \pi_{\mathfrak{a}'}\}$ is a family of orthogonal idempotents, but since $\pi_{\mathfrak{a}}, \pi_{\mathfrak{a}'} \in \mathrm{End}_A(A_\ell) = C_A(A_\ell) = (A_{A_r})^{\mathrm{opp}}$, we see that $e \stackrel{\mathrm{def}}{=} \pi_{\mathfrak{a}}(1)$, $e' \stackrel{\mathrm{def}}{=} \pi_{\mathfrak{a}'}(1)$ satisfy

$${}_A(e) = \mathfrak{a}, \quad {}_A(e') = \mathfrak{a}', \quad e^2 = e, \quad (e')^2 = e', \quad ee' = e'e = 0.$$

Letting $e_{\mathfrak{a}} \overset{\text{def}}{=} e$ and $e_{\mathfrak{a}'} \overset{\text{def}}{=} e'$, we see that $\mathfrak{a} = {}_A(e_{\mathfrak{a}}) = \mathfrak{a}e_{\mathfrak{a}}$.

Proposition 3.27. Let A be a semisimple ring. The following are equivalent :

(i) There is only one isomorphism class of simple left A-modules

(ii) There is only one isomorphism class of simple right A-modules

(iii) The ring A has a unique left maximal ideal

(iv) The ring A has a unique right maximal ideal

(v) The left A-module A_ℓ is isotypically simple

(vi) The right A-module A_r is isotypically simple

(vii) The only two-sided ideals of A are A and 0.

A non-zero ring satisfying any of the equivalent properties above is called **simple**. If B is a commutative ring, a B-algebra A is called **simple** if A is simple as a ring.

Proof. By Proposition 3.24, we see that (v), (vi) and (vii) are equivalent. It is clear that (i) and (iii) (resp. (ii) and (iv)) are equivalent since for two left ideals $\mathfrak{m}_1, \mathfrak{m}_2 \trianglelefteq A$, we have $A/\mathfrak{m}_1 \simeq A/\mathfrak{m}_2$ as left A-modules if and only if $\mathfrak{m}_1 = \mathfrak{m}_2$ (compare annihilators of those modules). It is also clear that (i) (resp. (ii)) implies (v) (resp. (vi)). The converse is also true by Corollary 2.47 since any simple left (resp. right) A-module is a quotient of the isotypical module $A_\ell^{\oplus I}$ (resp. $A_r^{\oplus I}$), so they all belong to the same isomorphism class.

Example 3.28.

- Any skew field D is simple since D_ℓ is a simple left D-module.
- Any simple commutative ring is a field since it has no non-zero proper two-sided ideals.
- Simple rings are semisimple by definition since A_ℓ is completely reducible and isotypical ; the fact that it is completely reducible is equivalent to the semisimplicity of A.
- If A is a simple ring, so is A^{opp} since the condition (vii) is symmetric with respect to multiplication.

Proposition 3.29. Let M be a left A-module such that $M^{\triangleleft}$ is finitely generated. The following are equivalent :

(i) A_M is a simple ring

(ii) M is isotypically simple

When either of the assumptions hold, if M is isotypical of type P where P is simple, we have $P \simeq A_M/\mathfrak{m}_M$ where $\mathfrak{m}_M$ is the unique left maximal ideal of A_M, or equivalently, the unique left maximal ideal of A containing $\operatorname{Ann}_A(M)$.

Proof. We already know that A_M is semisimple if and only if M is completely reducible by Proposition 3.21. If A_M is simple, there is only one class of simple left A-modules, so the complete reducibility of M implies that it is isotypically simple. Conversely, as in the proof of Proposition 3.21, we see that $(A_M)_\ell$ is isomorphic to a submodule of $M^{\oplus n}$ for some $n \geq 1$, so $(A_M)_\ell$ is isotypically simple, hence A_M is simple.

Theorem 3.30. Let A be a semisimple ring. The minimal two-sided ideals $A_1, \cdots, A_n$ admit a unit element and form simple subrings of A such that as a ring, $A = \prod_{i=1}^n A_i$. Conversely, if $A_1, \cdots, A_n$ are simple rings, then $\prod_{i=1}^n A_i$ is a semisimple ring whose minimal two-sided ideals are the following subsets, each identified with A_i :

$$0 \times \cdots \times 0 \times A_i \times 0 \times \cdots \times 0, \quad i = 1, \cdots, n.$$

Proof. Consider the semisimple ring A. The completely reducible left A-module A_ℓ is a direct sum of its isotypical components $A_1, \cdots, A_n$ (there are finitely many of them since A_ℓ is of finite length by Remark 3.20), which are minimal two-sided ideals of A by Proposition 3.24. Under the decomposition $A_\ell = \bigoplus_{i=1}^n A_i$, write $1 \in A$ as $1 = \bigoplus_{i=1}^n e_i$ where $e_i \in A_i$. Note that the fact that the ideals A_i are two-sided implies that $A_i A_j \subseteq A_i \cap A_j = 0$ for $1 \leq i, j \leq n$ with $i \neq j$. The action of 1 on A_i is therefore the same as that of e_i, so e_i is a unit element for the subring A_i. By definition, A_i is an isotypical left A-module, hence also isotypical as a module over the ring $A/\mathrm{Ann}_A(A_i) \simeq A_i$, which means it is simple. Conversely, given simple rings $A_1, \cdots, A_n$, the ring $A \overset{\text{def}}{=} \prod_{i=1}^n A_i$ is clearly semisimple since $A_\ell = \bigoplus_{i=1}^n A_i$ is completely reducible when seen as a direct sum of the completely reducible submodules A_i because the A-module A_i is annihilated by the A_j for $i \neq j$.

Definition 3.31. The minimal two-sided ideals of a semisimple ring are called its **simple components**.

Corollary 3.32. Every quotient of a semisimple ring A by a two-sided ideal $\mathfrak{a}$ is a semisimple ring isomorphic to a subring of A, for which we have an isomorphism of rings $A \simeq (A/\mathfrak{a}) \times \mathfrak{a}$ and $\mathfrak{a}$ is a subring of A with $\pi_{\mathfrak{a}}(1)$ as its identity element.

Proof. The $A/\mathfrak{a}$-submodules of an $A/\mathfrak{a}$-module M correspond to its A-submodules (since their annihilators all contain $\mathfrak{a}$). Since A is semisimple, M is a completely reducible A-module, hence a completely reducible $A/\mathfrak{a}$-module, which means $A/\mathfrak{a}$ is semisimple. Since $\mathfrak{a}$ is a left A-submodule of A, it admits a complement $\mathfrak{a}'$ such that $A_\ell = \mathfrak{a} \oplus \mathfrak{a}'$, which implies that $A \simeq \mathfrak{a} \times A/\mathfrak{a}$. The rest is obvious.

Proposition 3.33. Let $A_1, \cdots, A_n$ be simple rings and $A \overset{\text{def}}{=} \prod_{i=1}^n A_i$. The ring A admits precisely n distinct isomorphism classes of simple left A-modules. Given a simple A-module M, there exists a unique $i \in \{1, \cdots, n\}$ such that

$$\mathrm{Ann}_A(M) = {}_A(A_1, \cdots, \mathfrak{m}_i, \cdots, A_n)_A = A_1 \times \cdots \times A_{i-1} \times 0 \times A_{i+1} \times \cdots \times A_n$$

(where $\mathfrak{m}_i$ is the unique left maximal ideal of A_i) and M is a simple A_i-module under the identification $A/\mathrm{Ann}_A(M) \simeq A_i$.

Proof. Let M be a simple left A-module. For $1 \leq i \leq n$, consider the submodule

$$A_i M \overset{\text{def}}{=} \left\{ \sum_j^* a_j m_j \;\middle|\; a_j \in A_i,\, m_j \in M \right\}.$$

Then $A_i M$ is an A-submodule of M since $A_i A_j = 0$ for $i \neq j$. Therefore, there exists precisely one i such that $A_i M \neq 0$ (in which case $A_i M = M$), because the contrary implies

$$M = A_i M = A_i(A_j M) = 0.$$

Assume $A_i M = M \neq 0$. By letting $\mathfrak{m}_i$ be the unique left maximal ideal of A_i and identifying the quotients $A_i/\mathfrak{m}_i \simeq A/\mathrm{Ann}_A(M)$, the A_i-module M is simple precisely because it is a simple A-module. It follows that each simple A-module is a simple A_i-module for a unique $1 \leq i \leq n$, so there are precisely n isomorphism classes of simple A-modules, each one being represented by the simple A_i-module $A_i/\mathfrak{m}_i$ where $\mathfrak{m}_i$ is the unique left maximal ideal of A_i.

Theorem 3.34. Let D be a division ring.

(i) Let V be a finite-dimensional left D-vector space of dimension $r > 0$. The ring $A \overset{\text{def}}{=} \text{End}_D(V)$ is simple and the isotypically simple left A-module A_ℓ is of type V and has length r, i.e. $\ell_A(A_\ell) = r$. Considered as an A-module, V is simple.

(ii) Let A be a simple ring such that $\ell_A(A_\ell) = s$ and M be a simple left A-module. We obtain a division ring $D \overset{\text{def}}{=} C_A(M) = \text{End}_A(M)$ and the equality $\dim_D M = s$. Furthermore, the canonical morphism of rings $\varphi : A \to C_A^2(M) = \text{End}_D(M)$ defined by $a \mapsto a_M$ is an isomorphism, so that $A \simeq \text{End}_D(M)$.

In other words, a finite-dimensional vector left D-vector space V of dimension $\dim_D V$ corresponds to its endomorphism ring A of length $\ell_A(A_\ell)$ via $A = \text{End}_D(V)$ and $D = \text{End}_A(V)$, for which $\dim_D V = \ell_A(A_\ell)$. An element $\varphi \in \text{End}_{\mathbb{Z}}(V)$ commutes with every element of A_V (resp. D_V) if and only if it is in D_V (resp. A_V), so this gives the identities

$$Z(A) = Z(\text{End}_D(V)) = Z(D) = Z(\text{End}_A(V)).$$

Proof. (i) If $v_1 \in V \setminus \{0\}$, one can extend $\{v_1\}$ to a D-basis $\{v_1, v_2, \cdots, v_r\}$ for V by Theorem 3.3, so that as an A-module, ${}_A\langle v_1 \rangle = V$. This shows that V is a simple A-module. It is a faithful A-module since an endomorphism of V which vanishes on all of V is zero by definition. Consider the A-linear map $A \to V^{\oplus r}$ defined for $\varphi \in A = \text{End}_D(V)$ by $\varphi \mapsto (\varphi(v_1), \cdots, \varphi(v_r))$. This map is bijective ; it is the correspondence between an endomorphism of V and the collection of its r columns when written in matrix form. Since V is a simple A-module, this shows that $\ell_A(A_\ell) = \ell_A(V^{\oplus r}) = r$. In particular, A is isotypically simple of type V.

(ii) We know that $A_{A_\ell} = C_A^2(A_\ell)$ by Corollary 1.38. Since A_ℓ is isotypically simple of type M, we obtain a canonical isomorphism

$$A \simeq A_{A_\ell} = C_A^2(A_\ell) \simeq C_A^2(M^{\oplus s}) \simeq C_A^2(M).$$

This also implies that $A_M = C_A^2(M)$ and that M is a faithful A-module. Since $C_A^2(M) = C_{C_A(M)}(M^{\triangleleft}) = \text{End}_D(M)$, we just identified A with $\text{End}_D(M)$, the endomorphism ring of the left D-vector space M. Since A is of finite length, it is left-artinian, so the dimension $\dim_D M$ is finite ; otherwise, the ring $\text{End}_D(M) = A$ would not be left-artinian by Example 2.27. By part (i), we see that $\dim_D M = \ell_A(A_\ell) = r$.

The last equality follows from Corollary 1.38 since V is a free (and thus faithful) D-module.

Corollary 3.35. Let D_1, D_2 be division rings and M_i be a finite-dimensional vector space over D_i for $i = 1, 2$. If the rings $\text{End}_{D_1}(M_1)$ and $\text{End}_{D_2}(M_2)$ are isomorphic, then D_1 and D_2 are isomorphic and $\dim_{D_1} M_1 = \dim_{D_2} M_2$.

Proof. The isomorphism between $\text{End}_{D_1}(M_1)$ and $\text{End}_{D_2}(M_2)$ show that these rings have equal lengths as left modules over themselves, thus the equality in dimensions. Since D_i is the endomorphism ring of any simple $\text{End}_{D_i}(M_i)$-module and that the rings $\text{End}_{D_i}(M_i)$ are isomorphic, so are D_1 and D_2 when the modules M_1 and M_2 are identified along the isomorphism of rings $\text{End}_{D_1}(M_1) \simeq \text{End}_{D_2}(M_2)$.

Corollary 3.36. Let A be a ring and M be an isotypically simple A-module of finite length r. The ring $B \overset{\text{def}}{=} \text{End}_A(M)$ is simple and $\ell_B(B_\ell) = r$.

Proof. By Proposition 3.14, fixing a simple A-module P such that $M \simeq P^{\oplus r}$, we see that $B = \mathrm{End}_A(M) \simeq \mathrm{End}_A(P)$ is isomorphic to the endomorphism ring of a left $\mathrm{End}_A(P)$-vector space of dimension r. We can then apply Theorem 3.34 to complete the proof.

Corollary 3.37. Let M be a left A-module over the semisimple ring A. Then $M^{\triangleleft}$ is finitely generated and $A_M = C_A^2(M)$. (In fact, an upper bound for the number of generators may be computed as $\ell_A(A_\ell)$.

Proof. The second assertion follows from the first via Corollary 2.63 since the semisimplicity of A implies that M is completely reducible.

Since M has finitely many isotypical components, we can restrict to the case that M is isotypically simple of type P where P is a simple left A-module. Seeing P as a simple module over one of the simple components A_i of A instead of all of A (this is because only one of the A_i's is not contained in the annihilator of P), we see that $D \overset{\text{def}}{=} \mathrm{End}_A(P)$ is a division ring. By Proposition 3.14 (v), note that $B = \mathrm{End}_A(M)$ satisfies $\ell_B(M^{\triangleleft}) = \dim_D P$. The latter is an upper bound for the minimal number of generators of $M^{\triangleleft}$, so it suffices to show that $\dim_D P < \infty$; this is clear by Theorem 3.34 since $\mathrm{End}_D(P) = A_i$ is simple of finite length and $\dim_D P = \ell_{A_i}((A_i)_\ell) < \infty$.

As for the upper bound, note that $\ell_A(A_\ell) = \sum_{i=1}^n \ell_{A_i}((A_i)_\ell)$ where $A = \prod_{i=1}^n A_i$ is the decomposition of A as the product of its simple components.

Theorem 3.38. Let A be a semisimple ring with simple components $A_1, \cdots, A_n$, so that $A = \prod_{i=1}^n A_i$. Then $Z(A) = \prod_{i=1}^n Z(A_i)$ and each $Z(A_i)$ is a field. More precisely, if $A = \mathrm{End}_D(V)$ where D is a division ring and V a left D-vector space of finite dimension, then $Z(A) = Z(D)_V$ consists of those endomorphisms of V given by multiplication by central elements of D. In particular, the following holds :

(i) The ring A is a simple ring if and only if $Z(A)$ is a field

(ii) If A is a semisimple ring, then $Z(A)$ is semisimple.

Proof. The identity $Z(A) = \prod_{i=1}^n Z(A_i)$ follows by definition of multiplication. The fact that $Z(A_i)$ is a field follows by Corollary 1.38 identifying A_i with the endomorphism ring of a simple A_i-module P so that $D_i \overset{\text{def}}{=} \mathrm{End}_{A_i}(P_i)$ is a division ring satisfying $A_i = \mathrm{End}_{D_i}(P_i)$ and

$$Z(A_i) = Z(\mathrm{End}_{D_i}(P_i)) = Z(D_i)_{P_i} \simeq Z(D_i) \subseteq D_i.$$

As a division subring of the division ring D_i which is commutative, $Z(A_i)$ is a field. It is then clear that $Z(A)$ is a field if and only if $n = 1$ since a direct product of fields is not a field.

Definition 3.39. Let K be a field.

(i) A **central K-algebra** is a K-algebra A with structure map $\varphi : K \to A$ satisfying $Z(A) = \varphi(K)$.

(ii) A **central simple algebra over** K (written CSA for short) is a central K-algebra A which is a simple ring.

Corollary 3.40. Let K be a field.

(i) If A is a finite-dimensional CSA over K, then there exists a division ring D which is a CSA over K and for which $A \simeq \mathrm{Mat}_{n\times n}(D)$ for some integer $n \geq 1$.

(ii) If A is a CSA which is finite-dimensional over K and we assume K is algebraically closed, then $A \simeq \mathrm{End}_K(K^{\oplus n}) \simeq \mathrm{Mat}_{n\times n}(K)$ for some integer $n \geq 1$.

Proof. Let P be a simple A-module. By Theorem 3.34, we see that letting $D \overset{\text{def}}{=} \operatorname{End}_A(P)$, we have $A \simeq \operatorname{End}_D(P)$. Letting $n = \dim_D P$, this proves that $A \simeq \operatorname{Mat}_{n\times n}(D^{\text{opp}})$, so since D^{opp} is a division ring and $Z(D^{\text{opp}}) = Z(D) = Z(\operatorname{End}_A(P)) = Z(A) = K$, the division ring D is also a CSA. This proves part (i), and part (ii) follows since a division ring which is a CSA over K is isomorphic to K as a K-algebra.

Chapter 4

Radicals

In this chapter, A denotes a ring and M is a left A-module.

4.1 Radical of a module

Definition 4.1. Let $U \leq A$ be a subgroup of the additive group $(A, +)$ and $V \leq M$ be a subgroup of the additive group $(M, +)$. Their **product** is denoted by UV and is the abelian subgroup of M generated by the products uv where $u \in U$ and $v \in V$. In symbols,

$$UV \overset{\text{def}}{=} \langle \{uv \mid u \in U, v \in V\} \rangle_{\mathbb{Z}}.$$

The map $U \times V \to M$ defined by $(u, v) \mapsto uv$ is $\mathbb{Z}$-bilinear, so it factors through a map of abelian groups $U \otimes_{\mathbb{Z}} V$ and UV is the image of the corresponding map $U \otimes_{\mathbb{Z}} V \to M$.

More generally, if $U_1, \cdots, U_n \leq A$ are subgroups of $(A, +)$, we define

$$U_1 \cdots U_n V \overset{\text{def}}{=} \langle \{u_1 \cdots u_n v \mid u_i \in U_i, v \in V\} \rangle_{\mathbb{Z}}.$$

Again, this is the image of the map $U_1 \times \cdots \times U_n \times V \to M$ defined by $(u_1, \cdots, u_n, v) \mapsto u_1 \cdots u_n v$, and also the image of the corresponding additive map $U_1 \otimes_{\mathbb{Z}} \cdots \otimes_{\mathbb{Z}} U_n \otimes_{\mathbb{Z}} V \to M$.

Taking the particular case where $M = A_\ell$, we can define the products $U_1 U_2$ for two additive subgroups $U_1, U_2 \leq A$ by the same formulas. This definition of the product is associative, namely, for three additive subgroups $U_1, U_2, U_3 \leq A$, we have

$$U_1(U_2 U_3) = (U_1 U_2) U_3 = U_1 U_2 U_3.$$

which is clear since all three are generated by the same subsets of A by associativity of multiplication in A.

Remark 4.2. (i) If $\{U_i\}_{i \in I}$ is a family of additive subgroups of A and $\{V_j\}_{j \in J}$ is a family of additive subgroups of M, letting $U = \sum_{i \in I} U_i$ and $V = \sum_{j \in J} V_j$, we obtain

$$UV = \sum_{i \in I, j \in J} U_i V_j.$$

This is clear since tensor products commute with direct sums.

(ii) If $U_1, U_2 \leq A$ are two additive subgroups and $f : A \to B$ is a morphism of rings to another ring B, then $f(U_1 U_2) = f(U_1) f(U_2)$ (since they are both generated by the same elements).

(iii) If $\mathfrak{a} \trianglelefteq A$ is a left ideal, then for every additive subgroup $V \leq M$, $\mathfrak{a}V$ is an A-submodule of M. In particular, for any additive subgroup $U \leq A$, $\mathfrak{a}U$ is a left ideal of A. Analogously, if $\mathfrak{b}$ is a right ideal in A, $U\mathfrak{b}$ is a right ideal of A, so $\mathfrak{a}\mathfrak{b}$ is a two-sided ideal in A.

(iv) Let $\mathfrak{a}_1, \mathfrak{a}_2$ be two left ideals of A. The operation $(\mathfrak{a}_1, \mathfrak{a}_2) \mapsto \mathfrak{a}_1\mathfrak{a}_2$ is an associative operation on the set of left ideals of A. We define the n^{th} **power** of a left ideal by the recursive definition $\mathfrak{a}^0 \stackrel{\text{def}}{=} A$ and $\mathfrak{a}^n \stackrel{\text{def}}{=} \mathfrak{a}^{n-1}\mathfrak{a}$. For every $n \geq 0$, we have $\mathfrak{a}^{n+1} \subseteq \mathfrak{a}^n$. We define a similar notion for right ideals. Multiplying a right ideal $\mathfrak{b}$ with a left ideal $\mathfrak{a}$ to form the subgroup $\mathfrak{b}\mathfrak{a} \leq A$, we obtain the inclusion $\mathfrak{b}\mathfrak{a} \subseteq \mathfrak{b} \cap \mathfrak{a}$. More generally, if $\mathfrak{a}_2, \cdots, \mathfrak{a}_{n-1}$ are two-sided ideals of A, $\mathfrak{a}_1$ is a right ideal of A and $\mathfrak{a}_n$ is a left ideal of A, then

$$\mathfrak{a}_1 \cdots \mathfrak{a}_n \subseteq \bigcap_{i=1}^{n} \mathfrak{a}_i.$$

This is clear since $\mathfrak{a}_1 \cdots \mathfrak{a}_{i-1}\mathfrak{a}_i\mathfrak{a}_{i+1} \cdots \mathfrak{a}_n \subseteq A \cdots A\mathfrak{a}_i A \cdots A = \mathfrak{a}_i$. If additionally, $\mathfrak{a}_1$ is a left ideal, then $\mathfrak{a}_1 \cdots \mathfrak{a}_n$ is a left ideal ; similarly, if $\mathfrak{a}_n$ is also a right ideal, then $\mathfrak{a}_1 \cdots \mathfrak{a}_n$ is a right ideal.

Definition 4.3. Let A be a ring.

(i) An element $x \in A$ is said to be **nilpotent** if there exists $n \geq 1$ such that $x^n = 0$. The set of nilpotent elements of A is denoted by $\mathrm{Nil}(A)$. (When A is commutative, $\mathrm{Nil}(A)$ is a subgroup by the binomial theorem.)

(ii) If $x, y \in A$ are two elements such that $xy = yx = 1$, we say that x, y are **units** of A. The set of units of A is denoted by $A^\times$ and it forms a group under multiplication. If $xy = 1$ for some $x, y \in A$ but yx is not necessarily equal to 1, we say that x is **right-invertible** with **right inverse** y ; similarly, y is **left-invertible** with **left inverse** x.

(iii) A left (resp. right) ideal $\mathfrak{a}$ of A is said to be **nilpotent** if there exists $n \geq 1$ such that $\mathfrak{a}^n = 0$.

(iv) A left (resp. right) ideal $\mathfrak{a}$ contained in $\mathrm{Nil}(A)$ is called a **nilideal**.

Remark 4.4. (i) When $x \in \mathrm{Nil}(A)$, $1 - x \in A^\times$. To see this, assume $n \geq 0$ is such that $x^n = 0$ and use the geometric progression formula :

$$\left(\sum_{i=0}^{n-1} x^i\right)(1-x) = (1-x)\left(\sum_{i=0}^{n-1} x^i\right) = 1 - x^n = 1.$$

(ii) The equation $\mathfrak{a}^n = 0$ is equivalent to the following property : any product of n elements of $\mathfrak{a}$ is equal to zero (because those products generate $\mathfrak{a}^n$).

(iii) A nilpotent ideal $\mathfrak{a}$ is evidently a nilideal, but the converse is not true in general. (It would be nice to have easy examples, but Bourbaki (c.f. Algèbre, Chapitre 8, §6, n° 1, Remarques) has a rather hard one.)

Definition 4.5. Recall that a proper submodule $N \leq M$ is said to be **maximal** if M/N is simple (c.f. Definition 2.37). The **radical** of a left A-module M is denoted by $\mathrm{rad}(M)$ and is defined as the intersection of all maximal submodules of M. If $\mathrm{rad}(M) = 0$, we say that M is **radical-free**. Equivalently, $\mathrm{rad}(M)$ is the intersection of all kernels of morphisms of A-modules $f : M \to P$ where P is a simple left A-module, or in other words, $\mathrm{rad}(M)$ is the set of all $m \in M$ such that whenever $f : M \to P$ is a morphism of A-modules and P is simple, then $f(m) = 0$.

It is possible that M admits no maximal submodule in which case we set $\mathrm{rad}(M) \stackrel{\text{def}}{=} M$ (this is the same definition as above but intersecting over the empty family of maximal submodules of M).

Remark 4.6. The module $A/\mathfrak{a}$ is radical-free if and only if $\mathfrak{a}$ is the intersection of left maximal ideals.

Proposition 4.7. If M is a non-zero finitely generated left A-module, then $\operatorname{rad}(M) \neq M$.

Proof. This follows from the existence of maximal submodules, proven in Proposition 2.39.

Proposition 4.8. If $f : M \to N$ is a morphism of left A-modules, then $f(\operatorname{rad}(M)) \subseteq \operatorname{rad}(N)$.

Proof. Let P be a simple A-module and $g : N \to P$ a morphism of left A-modules. The composition $g \circ f : M \to P$ vanishes on $\operatorname{rad}(M)$, hence g vanishes on $f(\operatorname{rad}(M))$; this means $f(\operatorname{rad}(M)) \subseteq \ker g$. Taking the intersection over all such g gives the result.

Proposition 4.9. Let N be an A-submodule of the left A-module M.

(i) We have $\operatorname{rad}(N) \subseteq \operatorname{rad}(M)$

(ii) We have $\operatorname{rad}(M/N) \supseteq (\operatorname{rad}(M) + N)/N$. In particular, if $N \subseteq \operatorname{rad}(M)$, we have $\operatorname{rad}(M/N) = \operatorname{rad}(M)/N$.

(iii) If $\{M_i\}_{i\in I}$ is a family of left A-modules, we have $\operatorname{rad}(\prod_{i\in I} M_i) \subseteq \prod_{i\in I} \operatorname{rad}(M_i)$.

(iv) If $\{M_i\}_{i\in I}$ is a family of left A-modules, we have $\operatorname{rad}(\bigoplus_{i\in I} M_i) = \bigoplus_{i\in I} \operatorname{rad}(M_i)$.

Proof. Part (i) and the first statement of part (ii) are corollaries of Proposition 4.8. For the second statement of part (ii), the stronger statement of equality instead of inclusion follows from the fact that N is contained in every maximal submodule of M, hence the maximal submodules of M and those of M/N are in bijective correspondence.

Let N_i be a maximal submodule of M_i. Then

$$N(i) \overset{\text{def}}{=} N_i \times \prod_{\substack{j\in I \\ j\neq i}} M_j$$

is a maximal submodule of $M \overset{\text{def}}{=} \prod_{i\in I} M_i$, hence $\operatorname{rad}(\prod_{i\in I} M_i) \subseteq N(i)$ for all maximal submodules N_i of M_i, meaning that $\operatorname{rad}(\prod_{i\in I} M_i) \subseteq \prod_{i\in I} \operatorname{rad}(M_i)$, which is part (iii).

Applying the same argument as in part (iii) to the direct sum, we obtain $\operatorname{rad}(\bigoplus_{i\in I} M_i) \subseteq \bigoplus_{i\in I} \operatorname{rad}(M_i)$. However, since $M_i \subseteq \bigoplus_{j\in I} M_j$, in this case we can also obtain $\operatorname{rad}(M_i) \subseteq \operatorname{rad}(\bigoplus_{j\in I} M_j)$ by part (i). Summing all these submodules gives $\bigoplus_{i\in I} \operatorname{rad}(M_i) \subseteq \operatorname{rad}(\bigoplus_{i\in I} M_i)$, thus implying the equality in part (iv).

Corollary 4.10. Let M be a finitely generated left A-module and $N \leq M$ an A-submodule satisfying $N + \operatorname{rad}(M) = M$. Then $N = M$.

Proof. By Proposition 4.9 (ii), we see that $\operatorname{rad}(M/N) \supseteq (\operatorname{rad}(M) + N)/N = M/N$, which implies equality throughout. By Proposition 4.7, this implies that $M/N = 0$.

Corollary 4.11. The submodule $\operatorname{rad}(M)$ is the smallest submodule N such that M/N is radical-free.

Proof. If M/N is radical-free, by Proposition 4.9, we see that $0 = \operatorname{rad}(M/N) \supseteq (\operatorname{rad}(M) + N)/N$, hence $N = \mathrm{rad}(M) + N$, meaning $\mathrm{rad}(M) \subseteq N$. By the second statement of Proposition 4.9 part (ii),

$$\mathrm{rad}(M/\mathrm{rad}(M)) = \mathrm{rad}(M)/\mathrm{rad}(M) = 0.$$

Proposition 4.12. Let M be a finitely generated left A-module with chosen set of generators $\{m_1, \cdots, m_r\}$. For $m \in M$, the following are equivalent :

(i) $m \in \mathrm{rad}(M)$

(ii) For all $a_1, \cdots, a_r \in A$, the elements $\{m_1 + a_1 m, \cdots, m_r + a_r m\}$ also form a set of generators for M.

Proof. In any case, set $N \stackrel{\text{def}}{=} {}_A\langle m_1 + a_1 m, \cdots, m_r + a_r m\rangle$. If $m \in \mathrm{rad}(M)$, we see that $N + \mathrm{rad}(M) = M$, hence $N = M$, which proves that (i) implies (ii). For the converse, suppose that $m \in M \setminus \mathrm{rad}(M)$, so that there exists a maximal submodule N of M not containing m. We know that ${}_A\langle m\rangle + N = M$, so for each index $1 \le i \le r$, since $m_i \in M = {}_A\langle m\rangle + N$, we find $a_i \in A$ such that $m_i + a_i m \in N$, meaning that ${}_A\langle m_1 + a_1 m, \cdots, m_r + a_r m\rangle \subseteq N$. In particular, ${}_A\langle m_1 + a_1 m, \cdots, m_r + a_r m\rangle \neq M$.

Proposition 4.13. Let M be a finitely generated left A-module. The following are equivalent :

(i) M is radical-free, i.e. $\mathrm{rad}(M) = 0$

(ii) M is isomorphic to a submodule of a product of simple left A-modules.

As a corollary, every finitely generated and completely reducible left A-module is radical-free.

Proof. ((i) $\Rightarrow$ (ii)) Let $\{M_i\}_{i\in I}$ be a family of maximal submodules of M whose intersection is zero and consider the family of maps $\pi_i : M \to M/M_i$; note that M/M_i is simple by definition of maximality. Their product gives a morphism $\pi : M \to \prod_{i\in I} M/M_i$ which has kernel equal to $\bigcap_{i\in I} M_i = 0$. Therefore, $M \simeq \pi(M)$ and the latter is a submodule of a product of simple left A-modules.
((ii) $\Rightarrow$ (i)) Let $\{P_i\}_{i\in I}$ be a family of simple left A-modules and assume $M \subseteq \prod_{i\in I} P_i$. Note that by definition, a simple module is radical-free. It follows that

$$\mathrm{rad}(M) \subseteq \mathrm{rad}\left(\prod_{i\in I} P_i\right) \subseteq \prod_{i\in I} \mathrm{rad}(P_i) = 0.$$

Since a completely reducible module M can be written as $M \simeq \bigoplus_{i\in I} P_i \subseteq \prod_{i\in I} P_i$, we see that $\mathrm{rad}(M) = 0$.

4.2 Radical of a ring

Let A be a ring. Recall Definition 2.7 where we defined the Jacobson radical of A (or simply the radical of A) as the radical of the left A-module A_ℓ, i.e. $\mathrm{Jac}(A) \stackrel{\text{def}}{=} \mathrm{rad}(A_\ell)$ is the intersection of all the left maximal ideals of A (this is the non-commutative generalization of the Jacobson radical of a commutative ring). As in the case of left A-modules, the ring A is said to be **radical-free** if $\mathrm{Jac}(A) = 0$.

Remark 4.14. In theory, we should have defined the left Jacobson radical and the right Jacobson radical of A, as we quickly mentioned in Definition 2.7. However, we will see that if we defined these two notions, they will always agree, so we only have to speak of the Jacobson radical of a ring. Because of this, we will call it the Jacobson radical and when necessary, the notion which could have been called the right Jacobson radical would be equal to the left Jacobson radical of A^{opp}, so we will denote it by $\mathrm{Jac}(A^{\mathrm{opp}})$ instead of introducing a new notation.

Proposition 4.15. Let A be a ring.

(i) If M is a left A-module, the annihilator

$$\mathrm{Ann}_A(M) \stackrel{\mathrm{def}}{=} \{a \in A \,|\, aM = 0\}$$

is a two-sided ideal of A.

(ii) The radical $\mathrm{Jac}(A)$ is the intersection of all the annihilators of simple left A-modules. By part (i), it is a two-sided ideal of A.

(iii) The radical $\mathrm{Jac}(A)$ is the smallest element in the set of annihilators of all completely reducible left A-modules.

Proof. (i) This is obvious since if $a \in \mathrm{Ann}_A(M)$, $b \in A$ and $m \in M$, we have $bm \in M$, hence $(ab)m = a(bm) = 0$ and $(ba)m = b(am) = b0 = 0$.

(ii) It suffices to see that if P is a simple A-module, then the morphism $\varphi : A_\ell \to P$ is entirely determined by $p \stackrel{\mathrm{def}}{=} \varphi(1)$ since $\varphi(a) = a\varphi(1) = ap$. By the simplicity of P, p will always generate P as long as $p \neq 0$. It also follows that $\mathrm{Ann}_A(P) = \{a \in A \,|\, ap = 0\} = \ker \varphi$ is a left maximal ideal since if $p \neq 0$, $A_\ell/\mathrm{Ann}_A(P) = A_\ell/\ker\varphi \simeq P$. Conversely, if $\mathfrak{m}$ is a left maximal ideal of A, the morphism $\varphi : A_\ell \to A_\ell/\mathfrak{m}$ is a morphism of left A-modules from A_ℓ to a simple left A-module $P \stackrel{\mathrm{def}}{=} A_\ell/\mathfrak{m}$ with kernel equal to $\mathfrak{m}$. This establishes the correspondence between the kernels of morphisms to simple modules and annihilators of simple modules, so their intersections are the same.

(iii) If P is a simple left A-module, the kernel of the morphism $\varphi : A_\ell \to P$ defined by $\varphi(1) \stackrel{\mathrm{def}}{=} p \in P \setminus \{0\}$ is independent of the choice of p since it is equal to $\mathrm{Ann}_A(P)$. If M is completely reducible with isotypical component M_P of type P, then

$$\mathrm{Ann}_A(M) = \bigcap_{\substack{P \text{ simple} \\ M_P \neq 0}} \mathrm{Ann}_A(M_P) = \bigcap_{\substack{P \text{ simple} \\ M_P \neq 0}} \mathrm{Ann}_A(P).$$

Letting $\mathfrak{m} \trianglelefteq A$ denote an arbitrary left maximal ideal of A and $M_0 \stackrel{\mathrm{def}}{=} \bigoplus_{\mathfrak{m} \trianglelefteq A} A_\ell/\mathfrak{m}$, we see that

$$\mathrm{Jac}(A) = \bigcap_{\mathfrak{m} \trianglelefteq A} \mathfrak{m} = \bigcap_{\mathfrak{m} \trianglelefteq A} \mathrm{Ann}_A(A_\ell/\mathfrak{m}) = \mathrm{Ann}_A(M_0)$$

contains the annihilator of every completely reducible left A-module, which proves the claim since M_0 is itself completely reducible by construction.

Corollary 4.16. et A be a ring and M a left A-module. (Recall Theorem 2.9.)

(i) We have $\mathrm{Jac}(A)M \subseteq \mathrm{rad}(M)$.

(ii) (Nakayama's Lemma, second version) If M is finitely generated and $N \leq M$ is an A-submodule of M such that $N + \mathrm{Jac}(A)M = M$, then $N = M$.

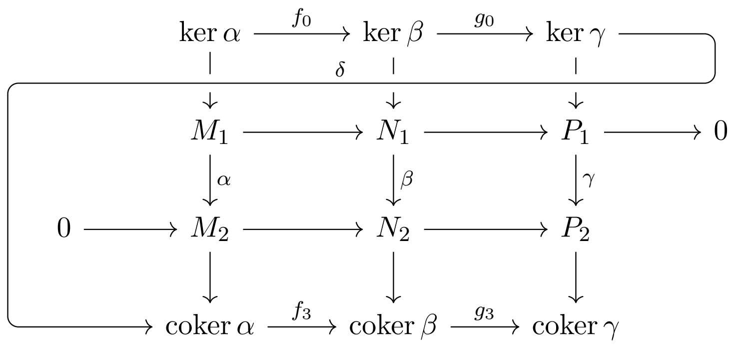
Proof. (i) Every simple A-module is annihilated by $\mathrm{Jac}(A)$, so if $f : M \to P$ is a morphism of A-module where P is a simple left A-module, we see that $f(\mathrm{Jac}(A)M) = \mathrm{Jac}(A)f(M) \subseteq \mathrm{Jac}(A)P = 0$, which means $\mathrm{Jac}(A)M \subseteq \ker f$. Taking the intersection over all such f gives the result.

(ii) This follows from Theorem 2.9 by considering the left A-module M/N, since $\mathrm{Jac}(A)(M/N) = M/N$ implies $M/N = 0$, i.e. $N = M$.

Theorem 4.17. (Snake's lemma). Let

$$\begin{array}{ccccccc} & & M_1 & \xrightarrow{f_1} & N_1 & \xrightarrow{g_1} & P_1 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle\beta} & & \downarrow{\scriptstyle\gamma} & & \\ 0 & \longrightarrow & M_2 & \xrightarrow{f_2} & N_2 & \xrightarrow{g_2} & P_2 & & \end{array}$$

be a commutative diagram of left A-modules with exact rows. Then this diagram can be extended



and there exists a **connecting** homomorphism $\delta : \ker\gamma \to \operatorname{coker}\alpha$ ("connecting" is nothing more but its name, i.e. does not mean δ has any extra properties) such that the following sequence is exact :

$$\ker\alpha \xrightarrow{f_0} \ker\beta \xrightarrow{g_0} \ker\gamma \xrightarrow{\delta} \operatorname{coker}\alpha \xrightarrow{f_3} \operatorname{coker}\beta \xrightarrow{g_3} \operatorname{coker}\gamma.$$

Furthermore, if $f_1 : M_1 \to N_1$ is injective, so is $f_0 : \ker\alpha \to \ker\beta$, and if $g_2 : N_2 \to P_2$ is surjective, so is $g_3 : \operatorname{coker}\beta \to \operatorname{coker}\gamma$.

Proof. We define δ as follows. Let $p_1 \in \ker\gamma$. Then there exists $n_1 \in N_1$ with $g_1(n_1) = p_1$. Since $g_2(\beta(n_1)) = \gamma(g_1(n_1)) = \gamma(p_1) = 0$, we have $\beta(n_1) \in \ker g_2 = \operatorname{im} f_2$, so there exists $m_2 \in A_2$ with $f_2(m_2) = \beta(n_1)$. We let $\delta(p_1)$ be the equivalence class of m_2 in $\operatorname{coker}\alpha = M_2/\operatorname{im}\alpha$.
The choice of n_1 and m_2 in the above construction is not unique, but the equivalence class of $f_2(m_2)$ in $\operatorname{coker}\alpha$ is. To see this, suppose n_1, n_1' are such that $g_1(n_1) = p_1 = g_1(n_1')$. Then $n_1 - n_1' \in \ker g_1 = \operatorname{im} f_1$, so there exists $m_1 \in A_1$ with $f_1(m_1) = n_1 - n_1'$. Pick m_2, m_2' such that $f_2(m_2) = \beta(n_1)$ and $f_2(m_2') = \beta(n_1')$. Then

$$f_2(m_2 - m_2') = f_2(m_2) - f_2(m_2') = \beta(n_1) - \beta(n_1') = \beta(n_1 - n_1') = \beta(f_1(m_1)) = f_2(\alpha(m_1)).$$

Since f_2 is injective, this means $m_2 \equiv m_2' \pmod{\operatorname{im}\alpha}$, showing that $\delta(p_1)$ is well-defined.
Onto exactness at $\ker\gamma$. Assume $p_1 = g_1(n_1)$ with $n_1 \in \ker\beta$. Then $f_2(m_2) = \beta(n_1) = 0$, but f_2 is injective, so $m_2 = 0$, which means $\delta(p_1) = 0$. Therefore $\delta \circ g_0 = 0$. Now suppose $\delta(c_1) = 0$, and choose b_1 and a_2 which defined $\delta(c_1)$. This means $a_2 = \alpha(a_1)$ for some $a_1 \in A_1$, and since

$$\beta(n_1) = f_2(m_2) = f_2(\alpha(m_1)) = \beta(f_1(m_1)) \quad \Longrightarrow \quad n_1 - f_1(m_1) \in \ker\beta,$$

we see that $g_1(n_1 - f_1(m_1)) = g_1(n_1) = p_1$, so $\ker\delta = \operatorname{im} g_0$.

Finally, exactness at $\operatorname{coker}\alpha$. The composition $f_3 \circ \delta$ is clearly zero ; picking $c_1 \in \ker\gamma$ and corresponding n_1, m_2, we have

$$f_3(\delta(p_1)) = f_3(\overline{m}_2) = \overline{f_2(m_2)} = \overline{\beta(n_1)} = 0.$$

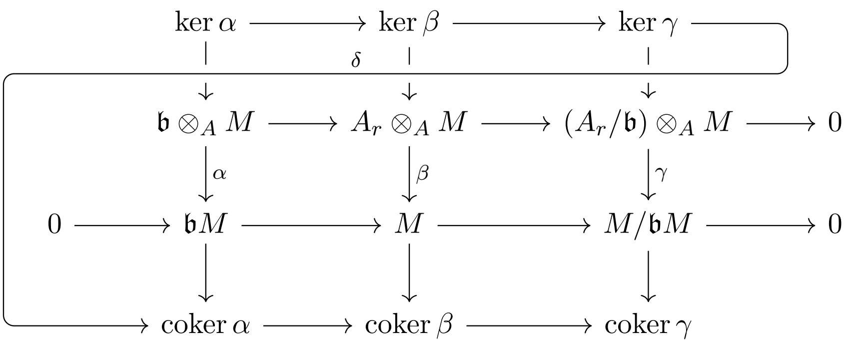
Now assume $\overline{m}_2 \in \operatorname{coker}\alpha$ satisfies $f_3(\overline{m}_2) = 0$. This means $\overline{f_2(m_2)} = 0$, so there exists $n_1 \in B_1$ with $\beta(n_1) = f_2(m_2)$. It follows that $\delta(g_1(n_1)) = \overline{m}_2$ by definition of δ, so $\ker f_3 = \operatorname{im}\delta$.
For left-exactness of the kernel, if $M_1 \to N_1$ is injective, note that the maps $\ker\alpha \to M_1 \to N_1$ are both injective, hence f_0 is injective. Similarly one proves that g_3 is surjective if $N_2 \to P_2$ is.

Corollary 4.18. Let A be a ring, M a left A-module and $\mathfrak{b} \trianglelefteq A$ a right ideal. The right ideal $\mathfrak{b}$ and the left A-module M can be multiplied to form the subgroup $\mathfrak{b}M$ of M, in which case we can take the quotient $M/\mathfrak{b}M$ as abelian groups ($\mathfrak{b}M$ is not a left A-submodule of M in general). We have an isomorphism of abelian groups

$$(A_r/\mathfrak{b}) \otimes_A M \simeq M/\mathfrak{b}M.$$

Furthermore, if $\mathfrak{b}$ is a two-sided ideal, then we have an isomorphism of left A-modules $A/\mathfrak{b} \otimes_A M \simeq M/\mathfrak{b}M$.

Proof. Consider the following commutative diagram of abelian groups :



The vertical maps α, β and γ are induced by the multiplication map $A \times M \to M$ of the left A-module M. The second row is exact by construction and the first row is right-exact by the right-exactness of the tensor product (c.f. Theorem 1.51). It is clear that β is an isomorphism and α is surjective, so $\ker\gamma = 0$ by exactness of the kernel-cokernel exact sequence from the Snake Lemma. Surjectivity of γ is also obvious since the right square between the two sequences commutes, the map $M \to M/\mathfrak{b}M$ is surjective and β is an isomorphism.

Corollary 4.19. Let M be a left A-module.

(i) If M is finitely generated and $\mathfrak{b} \trianglelefteq A$ is a right ideal contained in $\operatorname{Jac}(A)$, then $(A_r/\mathfrak{b}) \otimes_A M = 0$ implies $M = 0$.

(ii) Let N be a finitely generated left A-module and $\mathfrak{b} \trianglelefteq A$ a right ideal contained in $\operatorname{Jac}(A)$. If $f : M \to N$ is a morphism of A-modules (M is not assumed finitely generated) and the map $\operatorname{id} \otimes f : (A_r/\mathfrak{b}) \otimes_A M \to (A_r/\mathfrak{b}) \otimes_A N$ is surjective, then f is surjective.

Proof. (i) Since $A_r/\mathfrak{b} \otimes_A M \simeq M/\mathfrak{b}M$ by Corollary 4.18, the equation $(A_r/\mathfrak{b}) \otimes_A M = 0$ implies $\operatorname{Jac}(A)M = M$, hence $M = 0$ by Theorem 2.9 (iii) since M is finitely generated.

(ii) It is clear that $\operatorname{im}(\operatorname{id}_{A_r/\mathfrak{b}} \otimes f) = A_r/\mathfrak{b} \otimes \operatorname{im} f$, so the surjectivity of $\operatorname{im}(\operatorname{id}_{A_r/\mathfrak{b}} \otimes f)$ implies

$$A_r/\mathfrak{b} \otimes \operatorname{im} f = \operatorname{im}(\operatorname{id}_{A_r/\mathfrak{b}} \otimes f) = A_r/\mathfrak{b} \otimes N \quad \Longrightarrow \quad A_r \otimes (N/\operatorname{im} f) = 0$$

since we can tensor the following exact sequence with $A_r/\mathfrak{b}$:

$$0 \longrightarrow \operatorname{im} f \longrightarrow N \longrightarrow N/\operatorname{im} f \longrightarrow 0.$$

By part (i), since N is finitely generated, so does $N/\operatorname{im} f$, which implies $N/\operatorname{im} f = 0$, i.e. f is surjective.

Proposition 4.20. Let A be a ring and $\mathfrak{a} \trianglelefteq A$ be a two-sided ideal.

(i) We have the inclusion of two-sided ideals $\operatorname{Jac}(A/\mathfrak{a}) \supseteq (\operatorname{Jac}(A) + \mathfrak{a})/\mathfrak{a}$ in $A/\mathfrak{a}$.

(ii) If $\mathfrak{a} \subseteq \operatorname{Jac}(A)$, we have $\operatorname{Jac}(A/\mathfrak{a}) = \operatorname{Jac}(A)/\mathfrak{a}$.

(iii) The two-sided ideal $\operatorname{Jac}(A)$ is the smallest two-sided ideal $\mathfrak{a}$ such that $A/\mathfrak{a}$ is radical-free.

Proof. Parts (i) and (ii) are straightforward corollaries of Proposition 4.9. By part (i), if $\operatorname{Jac}(A/\mathfrak{a}) = 0$, then $\operatorname{Jac}(A) + \mathfrak{a} = \mathfrak{a}$, which means $\operatorname{Jac}(A) \subseteq \mathfrak{a}$; together with part (ii) which shows that $\operatorname{Jac}(A/\operatorname{Jac}(A)) = 0$, this proves part (iii).

Theorem 4.21. Let A be a ring and $x \in A$. The following are equivalent :

(i) $x \in \operatorname{Jac}(A)$

(ii) For all $a \in A$, $1 - ax$ is left-invertible, i.e. there exists $y_{a,x} \in A$ such that $y_{a,x}(1 - ax) = 1$.

Proof. This is actually a corollary of Proposition 4.12 applied to $M = A_\ell$ and $m_1 = 1$ since $\operatorname{Jac}(A) = \operatorname{rad}(A_\ell)$, $A_\ell = {}_A\langle 1 \rangle$ and the left-invertibility condition is equivalent to ${}_A\langle 1 - ax \rangle = A_\ell$.

Lemma 4.22. Let $x \in A$. If x is left-invertible and right-invertible, then x is invertible (i.e. we can pick a left-inverse for x which is also a right-inverse). Furthermore, when this is the case, the inverse is unique ; we denote the inverse by x^{-1}.

Proof. Suppose y is a left-inverse and z is a right-inverse. Then

$$z = 1z = (yx)z = y(xz) = y1 = y.$$

Applying this to the case where both y and z are inverses for x, we obtain unicity of the inverse.

Corollary 4.23. Let A be a ring.

(i) The two-sided ideal $\operatorname{Jac}(A)$ is the largest two-sided ideal such that $1 - x$ is invertible for all $x \in A$.

(ii) We have $\operatorname{Jac}(A) = \operatorname{Jac}(A^{\mathrm{opp}})$ (c.f. Remark 4.14).

(iii) An element $x \in A$ belongs to $\operatorname{Jac}(A)$ if and only if $1 - ax$ is invertible for all $a \in A$.

(iv) Every nilideal (i.e. a left or right ideal consisting of nilpotent elements) is contained in $\operatorname{Jac}(A)$.

(v) If $\{A_i\}_{i \in I}$ is a family of rings, then $\operatorname{rad}(\prod_{i \in I} A_i) = \prod_{i \in I} \operatorname{Jac}(A_i)$.

Proof. Let $\mathfrak{a} \trianglelefteq A$ be a two-sided ideal such that $1 - x$ is invertible for all $x \in A$. Then for all $a \in A$, $ax \in \mathfrak{a}$, hence $1 - ax$ is also invertible, and in particular left-invertible, which shows that $\mathfrak{a} \subseteq \operatorname{Jac}(A)$.

To finish the proof, it suffices to show that $x \in \mathrm{Jac}(A)$ implies that $1-x$ is invertible.

By assumption, there exists $y_{1,x} \in A$ such that $y_{1,x}(1-x) = 1$, i.e. $1 - y_{1,x} = -y_{1,x}x$. It follows that $z_x \overset{\text{def}}{=} 1 - y_{1,x} = -y_{1,x}x \in \mathrm{Jac}(A)$. Therefore, we can pick $y_{1,z_x} \in A$ such that $y_{1,z_x}y_{1,x} = y_{1,z_x}(1-z_x) = 1$. It follows that $y_{1,x}$ is both left-invertible and right-invertible, hence is invertible and $y_{1,x}^{-1} = 1-x$ by Lemma 4.22.

The statement of part (i) being symmetric with respect to multiplication, we see that $\mathrm{Jac}(A)$ and $\mathrm{Jac}(A^{\mathrm{opp}})$ are both characterized by part (i) and thus must be equal, which proves part (ii). Part (iii) follows from part (ii) and Theorem 4.21.

Let $\mathfrak{n}$ be a nilideal and $x \in \mathfrak{n}$. Since $ax \in \mathfrak{n}$ is nilpotent, $1-ax$ is invertible by Remark 4.4, which implies $ax = 1-(1-ax) \in \mathrm{Jac}(A)$ by part (iii). Finally, part (v) also follows from part (iii) since if $a_i, x_i \in A$, the I-tuple $(1-a_ix_i)_{i\in I} = 1 - (a_i)_{i\in I}(x_i)_{i\in I}$ is invertible if and only if each $1 - a_ix_i \in A_i$ is invertible.

Theorem 4.24. Let A be a ring and $\mathfrak{a} \trianglelefteq A$ a left ideal. The following are equivalent :

(i) $\mathfrak{a} \subseteq \mathrm{Jac}(A)$

(ii) If M is a finitely generated left A-module, the equation $\mathfrak{a}M = M$ implies $M = 0$.

Proof. By Proposition 4.7 and Theorem 2.9, if $\mathfrak{a} \subseteq \mathrm{Jac}(A)$ and M is a non-zero finitely generated left A-module, we have $\mathrm{rad}(M) \neq M$, hence $\mathfrak{a}M \subseteq \mathrm{Jac}(A)M \subseteq \mathrm{rad}(M) \neq M$. Conversely, if $\mathfrak{a}M \neq M$ for every non-zero finitely generated left A-module, then $\mathfrak{a}P \neq P$ for every simple left A-module. By the simplicity of P, this means $\mathfrak{a}P = 0$, i.e. $\mathfrak{a} \subseteq \mathrm{Ann}_A(P)$, so $\mathfrak{a} \subseteq \mathrm{Jac}(A)$ by Proposition 4.15.

Example 4.25. (i) Let A be an integral domain and let $B \overset{\text{def}}{=} A[[x_1, \cdots, x_n]]$ be the commutative ring of formal power series in the n variables $x_1, \cdots, x_n$. This is an integral domain, which can be proved by induction on n since $B = A[[x_1, \cdots, x_{n-1}]][[x_n]]$ and if $f, g \in A[[x]]$ satisfy $fg = 0$, then writing $f = \sum_{n \geq k} f_n x^n$ and $g = \sum_{n\geq \ell} g_n x^n$ with $f_k, g_\ell \neq 0$, it follows that $f_k g_\ell = 0$, which is a contradiction since A is assumed to be an integral domain. The group of units $B^\times$ is the set of those $f \in B$ for which $f(0, \cdots, 0) \in A^\times$. When A is a field, the set of $f \in B$ for which $f(0, \cdots, 0) = 0$ form the unique maximal ideal of B, so that $(B, \mathrm{Jac}(B))$ is a **local ring**. See [Commutative Algebra, Proposition 4.38] for explanations.

(ii) When $(A, \mathfrak{m})$ is a commutative local integral domain which is not a field (so that $\mathfrak{m} = \mathrm{Jac}(A) \neq 0$), the field of quotients $Q(A)$ is radical-free, so it is possible for a subring of a radical-free ring to have a non-zero radical (in constrast with the case of modules where $N \leq M$ implies $\mathrm{rad}(N) \subseteq \mathrm{rad}(M)$).

(iii) Let A be an integral domain and I a set. The polynomial ring $B \overset{\text{def}}{=} A[\{x_i\}_{i\in I}]$ is radical-free. To see this, pick $f \in B \setminus \{0\}$; if $g \in B$ has positive degree, then so does $1 - fg$, which cannot be invertible, hence $f \in B \setminus \mathrm{Jac}(B)$, which implies $\mathrm{Jac}(B) = 0$.

(iv) Consider the subring $A[x_1, \cdots, x_n] \subseteq A[[x_1, \cdots, x_n]]$. We know that $A[[x_1, \cdots, x_n]]$ is a local ring, hence its radical ideal is the one described in part (i). Note that even though $\mathrm{Jac}(A[x_1, \cdots, x_n]) = 0$, we have

$$\mathrm{Jac}(A[[x_1, \cdots, x_n]]) \cap A[x_1, \cdots, x_n] = (x_1, \cdots, x_n)_{A[x_1, \cdots, x_n]} \neq 0.$$

In other words, it is not because a subring A of a ring B satisfies $\mathrm{Jac}(A) = 0$ that $A \cap \mathrm{Jac}(B) = 0$.

(iv) Let K be a field, I a set and $A \subseteq K^I$ be a K-subalgebra. Then $\mathrm{Jac}(A) = 0$. To see this, for every $i \in I$, the map $K^I \to K$ defined by $f \mapsto f_i$, when restricted to A, has as a kernel the maximal ideal

$\mathfrak{m}_i \trianglelefteq A$ of functions $f : I \to K$ vanishing at $i \in I$. The intersection of all those ideals is the set of functions vanishing everywhere, thus equal to zero.

Proposition 4.26. Let A be a PID.

(i) A is radical-free if and only if it is a field or $\operatorname{Spec}(A)$ is infinite.

(ii) Since PIDs are UFDs, let $x \in A$ be written as $x = up_1^{i_1} \cdots p_n^{i_n}$ where $p_1, \cdots, p_n \in A$ are prime elements, $i_1, \cdots, i_n \geq 1$ are integers and $u \in A^\times$. Then $A/_A(x)$ is radical-free if and only if x is square-free, i.e. $i_1 = \cdots = i_n = 1$.

Proof. (i) Fields are clearly radical-free, so assume A is not a field, hence it admits at least one prime element. The maximal ideals of A are of the form $(p)_A$ where $p \in A$ is a prime element. The element $x \in A$ belongs to $\operatorname{Jac}(A) = \bigcap_p (p)_A$ if and only if it is divisible by each prime element p. If $x \in \operatorname{Jac}(A) \setminus \{0\}$, this means x is divisible by all primes in A, so there must be finitely many of them. Conversely, if $\operatorname{Spec}(A) = \{(p_1)_A, \cdots, (p_n)_A\}$ is finite, then $\operatorname{Jac}(A) = (p_1 \cdots p_n)_A \neq 0$ (because PIDs are integral domains).

(ii) Write $x = \prod_{j=1}^n p_j^{i_j}$ (we can assume $u = 1$ since $(x)_A = (ux)_A$). By the Chinese Remainder Theorem (c.f. [Commutative Algebra, Theorem 2.17]), we have

$$A/(x)_A = \prod_{j=1}^n A/(p_j)_A^{i_j}.$$

We know by Corollary 4.23 (v) that this implies $\operatorname{Jac}(A/(x)_A) = \prod_{j=1}^n \operatorname{Jac}(A/(p_j)_A^{i_j})$, so we can restrict to the case where $x = p^i$ is a prime power. By part (i), since $\operatorname{Spec}(A) = \{(p)_A\}$ is finite, it is radical-free if and only if it is a field, i.e. $i = 1$.

Remark 4.27. Letting $A = \mathbb{Z}$, we see that a radical-free ring can admit quotients with non-zero radical (in this case, they are $\mathbb{Z}/n\mathbb{Z}$ where n is a non-zero non-square-free integer) since $\operatorname{Jac}(\mathbb{Z}/n\mathbb{Z}) = m\mathbb{Z}/n\mathbb{Z}$ where m is the square-free part of n, i.e. if $n = \prod_{j=1}^n p_j^{i_j}$ with $i_j \geq 1$, then $m = \prod_{j=1}^n p_j$. Furthermore, $\operatorname{Jac}(\mathbb{Z}) = 0$ implies $\operatorname{Jac}(\mathbb{Z})M = 0$ for all $\mathbb{Z}$-modules M, even though $\operatorname{rad}(M) \neq 0$ for some abelian groups (such as the examples of $\mathbb{Z}/n\mathbb{Z}$ above since their Jacobson radical is the same as their radical as a $\mathbb{Z}$-module).

4.3 Radical of artinian rings/modules

Theorem 4.28. Let A be a left-artinian ring. Then $\operatorname{Jac}(A)$ is the largest two-sided nilpotent ideal of A.

Proof. Every two-sided nilpotent ideal of A is contained in $\operatorname{Jac}(A)$ by Corollary 4.23 (iv), so it suffices to show that $\operatorname{Jac}(A)$ is nilpotent. The sequence $\{\operatorname{Jac}(A)^n\}_{n \in \mathbb{N}}$ is decreasing, so since A is artinian, there exists $n_0 \geq 1$ such that for all $n \geq 1$, we have $\operatorname{Jac}(A)^{n_0+n} = \operatorname{Jac}(A)^{n_0}$. Suppose $\operatorname{Jac}(A)^{n_0} \neq 0$. We deduce the existence of left ideals $\mathfrak{a} \trianglelefteq A$ such that $\operatorname{Jac}(A)^{n_0}\mathfrak{a} \neq 0$ (since $\operatorname{Jac}(A)$ is such an ideal). The fact that A is artinian implies that A_ℓ is an artinian left A-module, which means that every decreasing sequence of left ideals of A stabilizes. By Zorn's Lemma, this proves the existence of a left ideal $\mathfrak{a}_0$ minimal with respect to the condition that $\operatorname{Jac}(A)^{n_0}\mathfrak{a}_0 \neq 0$. Since

$$\operatorname{Jac}(A)^{n_0}(\operatorname{Jac}(A)\mathfrak{a}_0) = \operatorname{Jac}(A)^{n_0+1}\mathfrak{a}_0 = \operatorname{Jac}(A)^{n_0}\mathfrak{a}_0 \neq 0,$$

we deduce that $\operatorname{Jac}(A)\mathfrak{a}_0 \subseteq \mathfrak{a}_0$ is also a left ideal of A satisfying the required restriction, implying that $\operatorname{Jac}(A)\mathfrak{a}_0 = \mathfrak{a}_0$. To obtain a contradiction, it suffices to show that $\mathfrak{a}_0$ is finitely generated by Nakayama's Lemma (c.f. Theorem 2.9 (iii)) since it would imply $\mathfrak{a}_0 = 0$ (and $\operatorname{Jac}(A)^{n_0}\mathfrak{a}_0 \neq 0$). By assumption, there exists $a \in \mathfrak{a}_0$ such that $\mathrm{Jac}(A)^{n_0}{}_A(a) \neq 0$, so since ${}_A(a) \subseteq \mathfrak{a}_0$, this implies ${}_A(a) = \mathfrak{a}_0$ is generated by one element.

Theorem 4.29. Let M be a left A-module. The following are equivalent :

(i) M is completely reducible and of finite length

(ii) M is completely reducible and finitely generated

(iii) M is artinian and radical-free.

Proof. The equivalence of (i) and (ii) is given by Corollary 2.58. We already know that a completely reducible module of finite length is artinian by Corollary 2.20 and radical-free by Proposition 4.13.

Conversely, suppose M artinian, radical-free and non-zero (the result is trivial if $M = 0$). Consider the set of all finite intersections of maximal submodules of M. Since $M \neq 0$ and $\mathrm{rad}(M) = 0$, this set is non-empty, i.e. M admits at least one maximal submodule. Since it is artinian, every decreasing chain of such finite intersections eventually stabilizes, so we can apply Zorn's Lemma and find a minimal element N_0. If N is a maximal submodule of M, we have $N \cap N_0 \subseteq N_0$, so by minimality of N_0, this implies $N \cap N_0 = N_0$, i.e. $N_0 \subseteq N$. So N_0 equals the intersection of all maximal submodules of M since it is itself a finite intersection of maximal submodules of M, therefore $N_0 = \mathrm{rad}(M) = 0$. Pick maximal submodules $M_1, \cdots, M_r$ of M such that $\bigcap_{i=1}^r M_i = 0$. The product of the projection maps $M \to M/M_i$ gives a morphism of A-modules $f : M \to \prod_{i=1}^r M/M_i$ where each M/M_i is a simple left A-module, so since $\prod_{i=1}^r M/M_i$ is a completely reducible left A-module of finite length, so does $M \simeq f(M)$.

Corollary 4.30. The quotient of an artinian left A-module M by its radical $\mathrm{rad}(M)$, namely $M/\mathrm{rad}(M)$, is a completely reducible left A-module of finite length.

Proof. Indeed, this quotient is artinian by Proposition 2.5 and radical-free by Corollary 4.11, so we can apply Theorem 4.29.

Corollary 4.31. Let A be a ring. Then A is semisimple if and only if it is left-artinian and radical-free. (In particular, it is also right-artinian since A^{opp} is then semisimple.)

Proof. This follows from Corollary 4.30 applied to A_ℓ and the fact that when A is semisimple, A_ℓ is of finite length by Corollary 2.58 since it is completely reducible by definition.

Corollary 4.32. The quotient of a left-artinian ring A by its radical, i.e. $A/\mathrm{Jac}(A)$, is semisimple.

Proof. This follows straightforwardly from Corollary 4.31.

Corollary 4.33. A non-zero ring A is simple if and only if it is artinian and $\{0, A\}$ is its set of two-sided ideals. In other words, if a ring has $\{0, A\}$ as its set of two-sided ideals, then the following are equivalent :

(i) A is simple

(ii) A is semisimple

(iii) A is left-artinian.

Proof. By definition (c.f. Proposition 3.27), a non-zero ring A is simple if and only if it is semisimple and has $\{0, A\}$ as its set of two-sided ideals. By Theorem 2.9, the condition on the set of two-sided ideals of A implies that $\mathrm{Jac}(A) = 0$ (because $\mathrm{Jac}(A) = A$ implies $A = 0$ and $\mathrm{Jac}(A)$ is a two-sided ideal), so A is simple if and only if it is semisimple, which is equivalent to A being left-artinian by Corollary 4.31.

4.4 Modules over an artinian ring

Theorem 4.34. Let A be a left-artinian ring and M a left A-module. The following are equivalent :

(i) M is completely reducible

(ii) $\mathrm{Jac}(A)M = 0$

(iii) A_M is a semisimple ring.

As a corollary, a left-artinian ring has only finitely many isomorphism classes of simple left A-modules which can be put in a one-to-one correspondence with the simple components of the semisimple ring $A/\mathrm{Jac}(A)$.

Proof. Of course, (iii) implies (i) since every module over a semisimple ring is completely reducible by definition (c.f. Proposition 3.18). To see that (i) implies (ii), it suffices to see that $\mathrm{Ann}_A(M)$ is the intersection of the annihilator of a family of simple left A-modules and $\mathrm{Jac}(A)M$ is the intersection of the annihilators of all simple left A-modules, implying that $\mathrm{Jac}(A) \subseteq \mathrm{Ann}_A(M)$, e.g. $\mathrm{Jac}(A)M = 0$. Finally, the equation $\mathrm{Jac}(A)M = 0$ implies that $A_M = A/\mathrm{Ann}_A(M)$ is a quotient ring of $A/\mathrm{Jac}(A)$, so since this ring is artinian and radical-free, it is semisimple by Corollary 4.31.

The last statement follows from Proposition 3.33 since for any simple left A-module M, we have $\mathrm{Jac}(A) \subseteq \mathrm{Ann}_A(M)$, so the A-module structure of M is the same as its $A/\mathrm{Jac}(A)$-module structure, and so A and $A/\mathrm{Jac}(A)$ have the same isomorphism classes of simple modules.

Theorem 4.35. Let A be a ring possessing a two-sided nilpotent ideal $\mathfrak{n}$ such that $A/\mathfrak{n}$ is semisimple (for example, if A is left-artinian, we can take $\mathfrak{n} \stackrel{\text{def}}{=} \mathrm{Jac}(A)$, c.f. Theorem 4.34 where we take $M \stackrel{\text{def}}{=} (A/\mathrm{Jac}(A))_\ell$).

For an arbitrary left A-module M, the following are equivalent :

(i) M is of finite length

(ii) M is artinian

(iii) M is noetherian.

Proof. ((i) $\Rightarrow$ (ii),(iii)) This follows by Corollary 2.20.

((ii),(iii) $\Rightarrow$ (i)) To show that M is of finite length, since $\mathfrak{n}^r = 0$ for some $r \geq 1$, it suffices to consider the modules $M_i \stackrel{\text{def}}{=} \mathfrak{n}^i M/\mathfrak{n}^{i+1}M$ for $0 \leq i < r$. Since M_i is an $A/\mathfrak{n}$-module (because $\mathfrak{n} \subseteq \mathrm{Ann}_A(M)$) and $\ell_A(M_i) = \ell_{A/\mathfrak{n}}(M_i)$, it suffices to show that the $A/\mathfrak{n}$-module M_i has finite length. But $A/\mathfrak{n}$ is semisimple, so M_i is a completely reducible $A/\mathfrak{n}$-module. Whether M is noetherian or artinian, this implies that M_i is a finite direct sum of simple $A/\mathfrak{n}$-modules, and therefore has finite length.

Corollary 4.36. Let A be a left-artinian ring and M a finitely generated left A-module. Then M is of finite length.

Proof. Since M is a quotient of the artinian left A-module $A_\ell^{\oplus n}$, it is artinian, hence of finite length by Theorem 4.35.

Corollary 4.37. Let A be a left-artinian ring. Then A_ℓ has finite length, hence A is left-noetherian.

Proof. This follows from Theorem 4.35 and Corollary 4.36.

Corollary 4.38. In a commutative artinian ring, we have $\mathrm{Jac}(A) = \mathrm{Nil}(A)$.

Proof. Since A is commutative, $\mathrm{Nil}(A)$ is an ideal of A. Because A is noetherian by Corollary 4.37, this ideal is finitely generated. Write $\mathrm{Nil}(A) = {}_A(a_1, \cdots, a_n)$. Fix N such that $a_i^N = 0$ for all $1 \le i \le n$. For any $b_1, \cdots, b_n \in A$, by the multinomial formula, we have

$$(b_1 a_1 + \cdots + b_n a_n)^M = \sum_{\substack{j_1+\cdots+j_n=M \\ j_1,\cdots,j_n \ge 0}} \binom{M}{j_1, \cdots, j_n} \prod_{i=1}^n (b_i a_i)^{j_i}.$$

Picking M large enough so that each n-tuple non-negative integers $(j_1, \cdots, j_n)$ satisfying $j_1 + \cdots + j_n = M$ is such that at least one of the coefficients is larger than N, this sum always vanishes, showing that $\mathrm{Nil}(A)^M = 0$, i.e. $\mathrm{Nil}(A)$ is a nilpotent ideal. Since $\mathrm{Jac}(A)$ is a nilpotent ideal of A, we have $\mathrm{Jac}(A) \subseteq \mathrm{Nil}(A)$. By Theorem 4.28, we have equality.

Proposition 4.39. Let A be a commutative ring. The following are equivalent :

(i) A is artinian and $\mathrm{Nil}(A) = 0$

(ii) A is artinian and radical-free

(iii) A is semisimple

(iv) There exist finitely many fields $F_1, \cdots, F_n$ such that $A \simeq \prod_{i=1}^n F_i$

(v) Every prime ideal in $\mathrm{Spec}\,(A) = \{\mathfrak{m}_1, \cdots, \mathfrak{m}_n\}$ is maximal and we have $A \simeq \prod_{i=1}^n A/\mathfrak{m}_i$.

Proof. The equivalence of (i) and (ii) follows from Corollary 4.38 ; that of (ii) and (iii) follows from Corollary 4.31. When A is semisimple, its simple components are fields, so since A is a direct product of its simple components, (iii) implies (iv) ; the converse is obvious. The implication (v) $\Rightarrow$ (iv) is clear by taking $F_i = A/\mathfrak{m}_i$. Conversely, it suffices to see that letting $A = \prod_{i=1}^n F_i$ and $\mathfrak{m}_i \overset{\text{def}}{=} \prod_{\substack{j=1 \\ j \neq i}}^n F_j$, we have $\mathrm{Spec}\,(\prod_{i=1}^n F_i) = \{m_1, \cdots, \mathfrak{m}_n\}$ and $A \simeq \prod_{i=1}^n A/\mathfrak{m}_i$.

Corollary 4.40. Let K be a field and A a commutative K-algebra which is radical-free (or equivalently, for which $\mathrm{Nil}(A) = 0$). If $B \subseteq A$ is a K-subalgebra which is finite-dimensional over K, then B is artinian and isomorphic to a finite direct product of finite field extensions of K. In particular, if K is algebraically closed, then $B \simeq K^n$.

Proof. Since B is finite-dimensional over K, it has to be artinian (since a decreasing chain of ideals leads to a decreasing chain of K-subspaces). It is also radical-free since $\mathrm{Jac}(B) = \mathrm{Nil}(B) \subseteq \mathrm{Jac}(A) = 0$ because any nilpotent element of B generates a nilpotent ideal of A, e.g. a nilideal of A ; such ideals are contained in $\mathrm{Jac}(A) = 0$ by Corollary 4.23 (iv). If $\mathrm{Spec}\,(B) = \{\mathfrak{m}_1, \cdots, \mathfrak{m}_n\}$, the field extensions $B/\mathfrak{m}_i$ are finite over K because B is. In particular, when K is algebraically closed, $B/\mathfrak{m}_i \simeq K$.

Corollary 4.41. Let K be an algebraically closed field and A a finite-dimensional commutative K-algebra. Then every simple A-module is one-dimensional over K.

Proof. Every simple A-module M can be considered as a simple A-module over $A/\mathrm{Jac}(A)$. Since $A/\mathrm{Jac}(A)$ is artinian and radical-free, we can assume without loss of generality that A is semisimple. It follows that M is a simple module over one of the simple components of A ; these are all isomorphic to K by Corollary 4.40, hence $\dim_K M = 1$.

We finish this section by considering the following application.

Theorem 4.42. Let K be a field and V be a finite-dimensional K-vector space. For a subset $S \subseteq \mathrm{End}_K(V)$, let $A \subseteq \mathrm{End}_K(V)$ be the K-subalgebra generated by the set S (note that $\mathrm{id}_V \in A$ by definition). Since $\mathrm{End}_K(V)$ is a finite K-algebra, A also is, hence A is an artinian K-algebra by Example 2.27. Furthermore, the following are equivalent :

(i) The K-algebra A is semisimple

(ii) The left A-module V is completely reducible

(iii) If $W \leq V$ is a subspace such that for any $\varphi \in S$, $\varphi(W) \subseteq W$ (or in other words, a subspace W which is stable under S), there exists a complement $W' \leq V$ such that $V = W \oplus W'$ and W' is also stable under S ; this is a direct sum of A-modules.

Proof. The equivalence of (i) and (ii) follows by Theorem 4.34 since $\mathrm{id}_V \in A$, hence V is a faithful A-module (meaning that the inclusion map $A \subseteq \mathrm{End}_K(V)$ induces the isomorphism $A \simeq A_V$). The equivalence of (ii) and (iii) is clear since subspaces of V stable under S are the same as A-submodules.

Definition 4.43. Let K be a field and V a finite-dimensional K-vector space.

(i) A collection of endomorphisms $S \subseteq \mathrm{End}_K(V)$ satisfying one of the equivalent conditions of Theorem 4.42 is called **semisimple**.

(ii) An endomorphism $\varphi \in \mathrm{End}_K(V)$ is said to be **semisimple** if $\{\varphi\}$ is semisimple.

(iii) If $\{\varphi_i\}_{i \in I}$ is a family of endomorphisms of V, we say it is semisimple if the subset $S \subseteq \mathrm{End}_K(V)$ of all endomorphisms $s \in \mathrm{End}_K(V)$ satisfying $s = \varphi_i$ for some $i \in I$ is semisimple.

Example 4.44. Let K be a field and V be a finite-dimensional K-vector space. An endomorphism $\varphi \in \mathrm{End}_K(V)$ is semisimple if and only if its minimal polynomial $\mathrm{m}_{\varphi,K}(t) \in K[t]$ is separable, i.e. factors as a product of distinct irreducible factors. To see this, write $\mathrm{m}_{\varphi,K}(t) = \prod_{i=1}^m f_i(t)^{n_i}$ where $f_1(t), \cdots, f_m(t) \in K[t]$ are distinct irreducible polynomials and $n_i \geq 1$. By the Chinese Remainder Theorem,

$$K[t]/(f(t)) \simeq \prod_{i=1}^n K[t]/(f_i(t)^{n_i}),$$

and note that the latter is semisimple if and only if it has no nilpotent elements by Proposition 4.39, i.e. if and only if $n_1 = \cdots = n_m = 1$.

Theorem 4.45. Let K be a field and V be a finite-dimensional K-vector space. Suppose $S \subseteq \mathrm{End}_K(V)$ consists of commuting endomorphisms, i.e. $\varphi \circ \psi = \psi \circ \varphi$ for all $\varphi, \psi \in S$. If S is semisimple and $T \subseteq S$, then T is semisimple. In particular, every $\varphi \in S$ is semisimple in this case.

Proof. The K-algebra $A \subseteq \mathrm{End}_K(V)$ generated by S is commutative, semisimple and finite-dimensional over K. It follows by Proposition 4.39 that it is artinian and has no nilpotents, so any K-subalgebra of A is also artinian and has nilpotents, i.e. is semisimple by the same result. By Theorem 4.42, this means that T is semisimple (by considering the K-subalgebra of A generated by T). The case of $\varphi \in S$ is dealt with by taking $T = \{\varphi\}$.

Chapter 5

Tensor products of K-algebras

In this chapter, K is a field, A and B are K-algebras, M is a left A-module and N is a left B-module.

5.1 Modules over tensor products

Definition 5.1. In what follows, we will often consider a given abelian group as a module over different rings and look at its radical. To distinguish between the radicals over its different module structures, given a left A-module M, we write $\mathrm{rad}_A(M)$ for the radical of the left A-module M.

We begin with a lemma which might seem irrelevant now, but to prevent confusion with future notation, we prove it now and use it later.

Lemma 5.2. Let C be a ring and $B \subseteq C$ be a subring which turns C into a free right B-module. Let N be a left B-module and note that the left $C \otimes_B B$-module $C \otimes_B N$ can be seen as a left C-module (resp. left B-module) by multiplication on the first factor (resp. on the second factor, or using the canonical $C \otimes_B B$-module structure of $C \otimes_B N$ and using the isomorphism $C \otimes_B B \simeq C$). Define the map $\iota_N : N \to C \otimes_B N$ by $\iota_N(n) \stackrel{\text{def}}{=} 1 \otimes n$, which is B-linear. We then have

$$\iota_N^{-1}(\mathrm{rad}_C(C \otimes_B N)) \subseteq \mathrm{rad}_B(N).$$

Proof. We first deal with the case where N is a simple left B-module, in which case $\mathrm{rad}_B(N) = 0$, thus we have to show that $\iota_N^{-1}(\mathrm{rad}_C(C \otimes_B N)) = 0$. Let $n \in N \setminus \{0\}$; we need to show that $\iota_N(n) = 1 \otimes n \notin \mathrm{rad}_C(C \otimes_B N)$. By simplicity of N, we have ${}_B\langle n \rangle = N$, hence ${}_C\langle 1 \otimes n \rangle = C \otimes_B N$. We know that $C \otimes_B N \neq 0$ by the assumption that C is a free right B-module. The equality ${}_C\langle 1 \otimes n \rangle = C \otimes_B N$ also implies that $C \otimes_B N$ is a finitely generated left C-module, hence $\mathrm{rad}_C(C \otimes_B N) \neq C \otimes_B N$ by Proposition 4.7. We deduce that $1 \otimes n \notin \mathrm{rad}_C(C \otimes_B N)$, proving that $\iota_N^{-1}(\mathrm{rad}_C(C \otimes_B N)) = 0$.

Now suppose N arbitrary and let $g : N \to P$ be a morphism of left B-modules where P is simple. We have the following commutative diagram :

$$\begin{array}{ccc} N & \xrightarrow{\quad g \quad} & P \\ \downarrow{\scriptstyle \iota_N} & & \downarrow{\scriptstyle \iota_P} \\ C \otimes_B N & \xrightarrow{\mathrm{id} \otimes g} & C \otimes_B P \end{array}$$

By the first case, since $\mathrm{rad}_B(P) = 0$, the first paragraph shows that $\iota_P^{-1}(\mathrm{rad}_C(C \otimes_B P)) = 0$. Let $n \in N$

be such that $\iota_N(n) \in \mathrm{rad}_C(C \otimes_B N)$. By using the commutativity of the square and Proposition 4.8,

$$\iota_P(g(n)) = (1 \otimes g)(\iota_N(n)) \in (\mathrm{id} \otimes g)(\mathrm{rad}_C(C \otimes_B N)) \subseteq \mathrm{rad}_C(C \otimes_B P) \quad \Longrightarrow \quad g(n) = 0.$$

Since g was arbitrary, this means $n \in \mathrm{rad}_B(N)$, showing that $\iota_N^{-1}(\mathrm{rad}_C(C \otimes_B N)) \subseteq \mathrm{rad}_B(N)$.

Definition 5.3. Let A, B be K-algebras, M be a left A-module and N a left B-module. It is understood that all four of A, B, M and N are K-vector spaces via their module/algebra structure. We understand that the algebra structures turn each of A, B, M and N into left K-modules, hence (K, K)-bimodules since $K = K^{\mathrm{op}}$, which allows us to take tensor products without any left/right-related issues.

The **tensor product of the K-algebras A and B** is the K-vector space $A \otimes_K B$ whose multiplication is given by the K-multilinear map

$$A \times B \times A \times B \to A \otimes_K B, \quad (a, b, a', b') \mapsto aa' \otimes bb'.$$

This extends to a K-bilinear map $(A \otimes_K B) \times (A \otimes_K B) \to A \otimes_K B$ and turns $A \otimes_K B$ into a K-algebra. More generally, the K-multilinear map

$$A \times B \times M \times N \to M \otimes_K N, \quad (a, b, m, n) \mapsto (am) \otimes (bn)$$

turns $M \otimes_K N$ into a left $(A \otimes_K B)$-module. Furthermore, we have canonical inclusion maps

$$\iota_{A,B}^A : A \to A \otimes_K B, \quad a \mapsto a \otimes 1$$

and similarly, we have

$$\iota_{A,B}^B : B \to A \otimes_K B, \quad b \mapsto 1 \otimes b.$$

Because A and B are tensored over K which is a field, these maps are injective (the tensor products of bases for A and B is a basis for $A \otimes_K B$; this is pure linear algebra, no theory of non-commutative rings needed). In particular, if $M = A_\ell$, we see that $A \otimes_K N$ is canonically endowed with an $(A \otimes_K B)$-module structure. We note that by Proposition 1.53, we have a natural isomorphism of $(A \otimes_K B)$-modules

$$A \otimes_K N \simeq A \otimes_K (B \otimes_B N) \simeq (A \otimes_K B) \otimes_B N, \quad a \otimes n \mapsto (a \otimes 1) \otimes n$$

where $A \otimes_K B$ is seen as a right B-module via the morphism of rings $\iota_{A,B}^B$, so we can think of $A \otimes_K N$ as being obtained by N via extension of scalars along the map $\iota_{A,B}^B : B \to A \otimes_K B$. We shall often need the map

$$\iota_{A,N} : N \to A \otimes_K N, \quad n \mapsto 1 \otimes n.$$

For the same reasons as with $\iota_{A,B}^A$ and $\iota_{A,B}^B$, this map is injective. Finally, if $N = B_\ell$, we note that the left $(A \otimes_K B)$-module structures on $A \otimes_K (B_\ell)$ and $(A \otimes_K B)_\ell$ coincide.

Remark 5.4. One can deduce that if $N' \leq N$ is a B-submodule of the left B-module N, then

$$(A \otimes_K N') \cap \iota_{A,N}(N) = \iota_{A,N}(N') = \iota_{A,N'}(N')$$

using the following commutative diagram of injective maps :

$$\begin{array}{ccc} N' & \xrightarrow{\subseteq} & N \\ \downarrow{\scriptstyle \iota_{A,N'}} & & \downarrow{\scriptstyle \iota_{A,N}} \\ A \otimes_K N' & \xrightarrow{\subseteq} & A \otimes_K N \end{array}$$

(The exactness of the tensor product $A \otimes_K (-)$ (which gives the injectivity of the bottom map) follows from the fact that K is a field, so that any K-module is free, hence flat.) Another way to obtain the result is to extend the linearly independent set $\{1\} \subseteq A$ to a K-basis of A, so that $\iota_{A,N}(N)$ corresponds to those elements of $A \otimes_K N$ which can be written in the form $1 \otimes n = \iota_{A,N}(n)$ for some $n \in N$.

Proposition 5.5. Let A and B be two K-algebras, M a left A-module and N a left B-module. Recall that $A \otimes_K N$ is a left $(A \otimes_K B)$-module (c.f. Definition 5.3). The equality

$$\iota_{A,N}^{-1}(\mathrm{rad}_{A\otimes_K B}(A \otimes_K N)) = \mathrm{rad}_B(N)$$

holds in the following three cases :

(i) the K-algebra A is a finite-dimensional K-vector space

(ii) the left B-module N is finitely generated and there exists an increasing sequence $\{A_i\}_{i\in\mathbb{N}}$ of K-subalgebras of A which are finite-dimensional over K, e.g. $A_i \subseteq A_{i+1}$ and $\bigcup_{i\geq 1} A_i = A$ (for instance, when A is a field and the extension A/K is algebraic)

(iii) $N = B_\ell$ and $\mathrm{Jac}(B) = \mathrm{rad}_B(N)$ is a nilpotent two-sided ideal of B (we already know it is a two-sided ideal by Proposition 4.15, and it is nilpotent when B is left-artinian for instance, c.f. Theorem 4.28).

Proof. Fix $C \overset{\mathrm{def}}{=} A \otimes_K B$, so that B can be seen as a subring of C by using the injective morphism of rings $\iota_{A,B}^B : B \to A \otimes_K B = C$. By Lemma 5.2, the inclusion $(\subseteq)$ holds, so it suffices to establish the reverse inclusion $(\supseteq)$.

(i) Let $g : A \otimes_K N \to P$ be a morphism of $(A \otimes_K B)$-modules where P is a simple $(A \otimes_K B)$-module. It suffices to show that $g|_{\mathrm{rad}_{A\otimes_K B}(A\otimes_K N)} = 0$ to deduce that $\mathrm{rad}_B(N) \subseteq \iota_{A,N}^{-1}(\mathrm{rad}_{A\otimes_K B}(A \otimes_K N))$.

By restriction of scalars, we can consider P as a left B-module, which we denote by $P_{[B]}$. The composition $g \circ \iota_{A,N} : N \to A \otimes_K N \to P_{[B]}$ is a morphism of B-modules, hence $(g \circ \iota_{A,N})(\mathrm{rad}_B(N)) \subseteq \mathrm{rad}_B(P_{[B]})$ by Proposition 4.8. Since $\iota_{A,N}$ is injective, it remains to show that $\mathrm{rad}_B(P_{[B]}) = 0$.

We note that since the subsets $\iota_{A,B}^A(A)$ and $\iota_{A,B}^B(B)$ of $A \otimes_K B$ commute with one another :

$$(a \otimes 1)(1 \otimes b) = a \otimes b = (1 \otimes b)(a \otimes 1),$$

we have the inclusion $A_P \subseteq \mathrm{End}_B(P_{[B]})$, i.e. multiplication by an element $a \in A$ in P is an endomorphism of B-modules of $P_{[B]}$. It follows by Proposition 4.8 that $\mathrm{rad}(B)P_{[B]}$ is a B-submodule and an A-submodule of $P_{[B]}$, thus an $(A \otimes_K B)$-submodule of P. Since P is simple and A is finite-dimensional over K, the B-module $P_{[B]}$ is finitely generated (if $p \in P$ satisfies ${}_{A\otimes_K B}\langle p\rangle = P$, fix a basis $\{a_1, \cdots, a_n\}$ of A over K so that ${}_B\langle (a_1 \otimes 1)p, \cdots, (a_n \otimes 1)p\rangle = P_{[B]}$). We deduce $\mathrm{rad}_B(P_{[B]}) \neq P_{[B]}$ by Proposition 4.7, so the simplicity of the $(A \otimes_K B)$-module P implies that the proper $(A \otimes_K B)$-submodule $\mathrm{rad}_B(P_{[B]})$ is zero.

(ii) Suppose ${}_B\langle n_1, \cdots, n_k\rangle = N$ and take an increasing sequence $\{A_n\}_{n\in\mathbb{N}}$ as stated in the assumptions. Let $n \in \mathrm{rad}_B(N)$, so that we have to show that $1 \otimes n \in \mathrm{rad}_{A\otimes_K B}(A \otimes_K N)$. By right-exactness of the tensor product, we see that ${}_{A\otimes_K B}\langle 1 \otimes n_1, \cdots, 1 \otimes n_k\rangle = A \otimes_K N$ is finitely generated, so by Proposition 4.12, it suffices to show that for any $c_1, \cdots, c_k \in A \otimes_K B$, we have

$${}_{A\otimes_K B}\langle 1 \otimes n_1 + c_1(1 \otimes n), \cdots, 1 \otimes n_k + c_k(1 \otimes n)\rangle = A \otimes_K N.$$

However, the elements $c_1, \cdots, c_k$ are all contained within some A_i for a given i large enough, so that attempting to prove the same result for A_i instead of A can be done via part (i) since A_i is finite-dimensional over K because

$$n \in \mathrm{rad}_B(N) = \iota_{A,N}^{-1}(\mathrm{rad}_{A_i\otimes_K B}(A_i \otimes_K N))$$

implies that

$${}_{A_i\otimes_K B}\langle 1 \otimes n_1 + c_1(1 \otimes n), \cdots, 1 \otimes n_k + c_k(1 \otimes n)\rangle = A_i \otimes_K N.$$

by Proposition 4.12 applied again. Writing $A \otimes_K N = A \otimes_{A_i} (A_i \otimes_K N)$, the right-exactness of the tensor product gives us the desired equality by applying the functor $A \otimes_{A_i} (-)$ to the previous one.

(iii) We now want to show that

$$\mathrm{rad}_B(B_\ell) = \mathrm{Jac}(B) \subseteq (\iota^B_{A,B})^{-1}(\mathrm{Jac}(A \otimes_K B)) = \iota^{-1}_{B,B_\ell}(\mathrm{rad}_{A\otimes_K B}(A \otimes_K B_\ell)).$$

by assuming that $\mathrm{Jac}(B)^k = 0$ for some $k \geq 1$. Let $J \stackrel{\text{def}}{=} {}_{A\otimes_K B}\langle \mathrm{Jac}(B)\rangle_{A\otimes_K B}$ be the two-sided ideal of $A \otimes_K B$ generated by $\mathrm{Jac}(B)$. A generic element of J will have the form $\sum_i^* a_i \otimes b_i$ where the * indicates that the sum has finitely many terms, $a_i \in A$ and $b_i \in \mathrm{Jac}(B)$ since elements of $\iota^A_{A,B}(A)$ and $\iota^B_{A,B}(B)$ commute. It follows that J^k is generated as a two-sided ideal of $A \otimes_K B$ by products of k elements of $\iota^B_{A,B}(B)$, hence $J^k = 0$. By Corollary 4.23, it follows that

$$\iota^B_{A,B}(\mathrm{Jac}(B)) \subseteq J \subseteq \mathrm{Jac}(A \otimes_K B) \quad \Longrightarrow \quad \mathrm{Jac}(B) \subseteq (\iota^B_{A,B})^{-1}(\mathrm{Jac}(A \otimes_K B)).$$

Corollary 5.6. Let A, B be two K-algebras such that B is left-artinian. If $A \otimes_K B$ is radical-free, then B is semisimple.

Proof. We see that $\mathrm{Jac}(B) = 0$ by Proposition 5.5, so B is left-artinian and radical-free. By Corollary 4.31, it is semisimple.

Remark 5.7. Given a ring A, we can consider the group of ring automorphisms of A under composition ; we denote it by $\mathrm{Aut}(A)$. We always have a morphism of groups

$$\varphi : A^\times \to \mathrm{Aut}(A), \quad a \mapsto (\varphi_a : x \mapsto axa^{-1}).$$

(The check that φ_a respects addition, multiplication and unit element is trivial.) This morphism is trivial if and only if $A^\times \subseteq Z(A)$. In particular, if A is a division ring, then the set of elements $x \in A$ such that $\varphi_a(x) = x$ for all $a \in A$ is precisely $Z(A)$. Another way to see this last statement is that $G \stackrel{\text{def}}{=} A^\times$ acts on A via φ, and the set of fixed points is $A^G = Z(A)$. In the case where A is a central K-algebra which is a division ring, this means $A^G = K$. We also call A^G the **ring of invariants** of G acting on A.

Proposition 5.8. Let K be a field, A be a K-algebra which is a division ring and B a K-algebra. For any left B-module N, the equality

$$\mathrm{rad}_{A\otimes_K B}(A \otimes_K N) = A \otimes_K \iota^{-1}_{A,N}(\mathrm{rad}_{A\otimes_K B}(A \otimes_K N))$$

holds in the two following cases :

(i) There exists a group action $G \circlearrowright A$ acting by ring automorphisms (i.e. is given by a morphism of groups $\varphi : G \to \mathrm{Aut}(A)$) such that $K = A^G$ is the ring of elements left invariant by G. (By Remark 5.7, this is the case if A is a central K-algebra.)

(ii) The B-module N is finitely generated and the division ring A is a field such that the extension A/K is separable (algebraic or transcendental).

Proof. Without loss of generality, assume K is a subring of A and that the K-algebra structure map $K \to A$ is given by inclusion, so that in case (i), we have $A^G = K$.

(i) Note that if $N' \leq N$ is a B-submodule such that $\mathrm{rad}_{A\otimes_K B}(A \otimes_K N) = A \otimes_K N' \subseteq A \otimes_K N$, then $\iota^{-1}_{A,N}(\mathrm{rad}_{A\otimes_K B}(A \otimes_K N)) = N'$. So it suffices to prove the existence of a B-submodule N'

such that $\mathrm{rad}_{A\otimes_K B}(A\otimes_K N) = A\otimes_K N'$. By Corollary 3.16, since $A^G = K$, it suffices to show that $\mathrm{rad}_{A\otimes_K B}(A\otimes_K N)$ is stable under every $g\otimes \mathrm{id}_N \in \mathrm{End}_B(A\otimes_K N)$ (flip the factors tensored in Corollary 3.16 to obtain the required statement!).

Consider the group action $G \circlearrowleft A$ acting by K-linear automorphisms of A and pick $g \in G$. The element $g\otimes \mathrm{id}_N$ acts by B-linear automorphisms on the $(A\otimes_K B)$-module $A\otimes_K N$ by the formula $(g\otimes \mathrm{id}_N)(a\otimes n) \stackrel{\text{def}}{=} g(a)\otimes n$. It follows that if $P \le A\otimes_K N$ is an $(A\otimes_K B)$-submodule, so does $(g\otimes \mathrm{id}_N)(P)$:

$$\begin{aligned} a(g\otimes \mathrm{id}_N)\left(\sum_i^* a_i\otimes n_i\right) &= \sum_i^* a g(a_i)\otimes n_i \\ &= \sum_i^* g(g^{-1}(a)a_i)\otimes n_i \\ &= (g\otimes \mathrm{id}_N)\left(g^{-1}(a)\left(\sum_i^* a_i\otimes n_i\right)\right). \end{aligned}$$

(The latter shows that the B-submodule $(g\otimes \mathrm{id}_N)(P)$ is also an A-submodule of $A\otimes_K N$, hence an $(A\otimes_K B)$-submodule.) The action of G on $A\otimes_K N$ thus permutes the set of $(A\otimes_K B)$-submodules of $A\otimes_K N$ in an inclusion-preserving way, so that it also permutes the set of maximal $(A\otimes_K B)$-submodules of $A\otimes_K N$. This implies that $\mathrm{rad}_{A\otimes_K B}(A\otimes_K N)$ is stable under the action of G since it is the intersection of all those maximal submodules.

(ii) Let $N' \stackrel{\text{def}}{=} \iota_{A,N}^{-1}(\mathrm{rad}_{A\otimes_K B}(A\otimes_K N))$. It is clear that $\mathrm{rad}_{A\otimes_K B}(A\otimes_K N) \supseteq A\otimes_K N'$, so it suffices to show that $\mathrm{rad}_{A\otimes_K B}(A\otimes_K N) \subseteq A\otimes_K N'$. Pick $z \stackrel{\text{def}}{=} \sum_{i=1}^n a_i\otimes n_i \in \mathrm{rad}_{A\otimes_K B}(A\otimes_K N)$, so that we wish to show that $n_i \in N'$.

Let Ω be an algebraic closure for A and $\sigma \in \mathrm{Aut}(\Omega/K)$. The automorphism $\sigma\otimes \mathrm{id}_N \in \mathrm{Aut}(\Omega\otimes_K N)$ can be restricted to an isomorphism of B-modules $\sigma\otimes \mathrm{id}_N : A\otimes_K N \to \sigma(A)\otimes_K N$: it becomes an isomorphism of $A\otimes_K B$-modules if we see $\sigma(A)\otimes_K N$ as a $\sigma(A)\otimes_K B$-module and twist this module structure via the isomorphism $\sigma\otimes \mathrm{id}_B : A\otimes_K B \to \sigma(A)\otimes_K B$. It follows that

$$(\sigma\otimes \mathrm{id}_N)(z) \in \mathrm{rad}_{A\otimes_K B}(\sigma(A)\otimes_K N) = \mathrm{rad}_{\sigma(A)\otimes_K B}(\sigma(A)\otimes_K N).$$

(The latter equality holds because the $\sigma(A)\otimes_K B$-submodules of $\sigma(A)\otimes_K N$ and its $A\otimes_K B$-submodules agree.) We have an isomorphism of K-algebras

$$\Omega\otimes_K B \simeq \Omega\otimes_{\sigma(A)} (\sigma(A)\otimes_K B),$$

so since the extension $\Omega/\sigma(A)$ is algebraic, we see that $(\sigma\otimes \mathrm{id}_N)(z) \in \mathrm{rad}_{\Omega\otimes_K B}(\Omega\otimes_K N)$ by Proposition 5.5 (ii) ; to see this, let the extension $\Omega/\sigma(A)$ play the role of A/K in Proposition 5.5, so that

$$\mathrm{rad}_{\Omega\otimes_K B}(\Omega\otimes_K N) = \Omega\otimes_{\sigma(A)} \left(\mathrm{rad}_{\sigma(A)\otimes_K B}(\sigma(A)\otimes_K N)\right).$$

(The K-algebra $\sigma(A)\otimes_K B$ plays the role of B in Proposition 5.5 and the role of N is played by $\sigma(A)\otimes_K N$ which is a finitely generated $\sigma(A)\otimes_K B$-module since N is a finitely generated B-module.)

By [Commutative Algebra,Theorem 13.52], there exists $\sigma_1,\cdots,\sigma_n \in \mathrm{Gal}(\Omega/K)$ such that the matrix $(\sigma_i(a_j))_{ij} \in \mathrm{Mat}_{n\times n}(\Omega)$ is invertible : let $(\mu_{ij})_{ij} \in \mathrm{Mat}_{n\times n}(\Omega)$ be its inverse. We see that for each $1 \leq i \leq n$,

$$\sum_{j=1}^{n} \mu_{ij}(\sigma_j \otimes \mathrm{id}_N)(z) = \sum_{j=1}^{n} \mu_{ij}(\sigma_j \otimes \mathrm{id}_N) \left(\sum_{k=1}^{n} a_k \otimes n_k \right) = \left(\sum_{j,k=1}^{n} \mu_{ij}\sigma_j(a_k) \right) \otimes n_k = 1 \otimes n_i$$

is an element of $\mathrm{rad}_{\Omega \otimes_K B}(\Omega \otimes_K N)$. By Lemma 5.2, since $A \otimes_K N$ is a finitely generated $(A \otimes_K B)$-module and the extension Ω/A is algebraic, considering the map $\iota_{\Omega,N}$ extending the $(A \otimes_K B)$-module $A \otimes_K N$ to an $(\Omega \otimes_K B)$-module $\Omega \otimes_K N$, we have

$$1 \otimes n_i \in \iota_{\Omega,N}^{-1}(\mathrm{rad}_{\Omega \otimes_K B}(\Omega \otimes_K N)) = \mathrm{rad}_{A \otimes_K B}(A \otimes_K N),$$

or in other words, $n_i \in N'$, which completes the proof.

Corollary 5.9. Let K be a field, A be a K-algebra which is a division ring containing K in its center and B a K-algebra. For any left B-module N, the inclusion

$$\mathrm{rad}_{A \otimes_K B}(A \otimes_K N) \subseteq A \otimes_K \mathrm{rad}_B(N)$$

holds in the two following cases :

(i) There exists a group action $G \circlearrowleft A$ acting by ring automorphisms (i.e. is given by a morphism of groups $\varphi : G \to \mathrm{Aut}(A)$) such that $K = A^G$ is the ring of elements left invariant by G. (By Remark 5.7, this is the case if A is a central K-algebra.)

(ii) The B-module N is finitely generated and the division ring A is a field such that the extension A/K is algebraic and separable.

Proof. This is clear by the proposition and Lemma 5.2 (which applies because K is a field, so A is a free K-module).

Corollary 5.10. Let A/K be a separable field extension and B a K-algebra. For any left B-module N, the equality

$$\mathrm{rad}_{A \otimes_K B}(A \otimes_K N) = A \otimes_K \mathrm{rad}_B(N)$$

holds in the three following cases :

(i) The field extension A/K is finite

(ii) The field extension A/K is algebraic and N is a finitely generated B-module

(iii) The ideal $\mathrm{rad}(B)$ is a nilpotent ideal of B and $N = B_\ell$.

Proof. The cases (ii) and (iii) are straightforward from Proposition 5.5 and Proposition 5.8. As for the case (i), the result is certainly true if the extension A/K is Galois (by Proposition 5.5 and Proposition 5.8 again). If A/K is not necessarily Galois, let E be a normal closure for the finite separable extension A/K in some algebraic closure for A, so that E/K is finite and Galois. By the Galois case of part (i), we have

$$\mathrm{rad}_{E \otimes_K B}(E \otimes_K N) = E \otimes_K \mathrm{rad}_B(N).$$

Since E/A is finite, by Proposition 5.5, we also have

$$\iota_{E,N}^{-1}(\mathrm{rad}_{E \otimes_A (A \otimes_K B)}(E \otimes_A (A \otimes_K N))) = \mathrm{rad}_{A \otimes_K B}(A \otimes_K N)$$

Identifying the functors $E \otimes_K (-)$ and $E \otimes_A (A \otimes_K (-))$, we see that

$$\mathrm{rad}_{A\otimes_K B}(A \otimes_K N) = \iota_{E,N}^{-1}(\mathrm{rad}_{E\otimes_K B}(E \otimes_K N)) = \iota_{E,N}^{-1}(E \otimes_K \mathrm{rad}_B(N)) = A \otimes_K \mathrm{rad}_B(N).$$

5.2 Tensor product of K-fields

In this section, K is a field. A K-**field** is a field E which is a K-algebra, so the data is equivalent to that of a field extension E/K.

Proposition 5.11. Let E, F be two K-fields. Then $\mathrm{Jac}(E \otimes_K F) = \mathrm{Nil}(E \otimes_K F)$.

Proof. Note that if A is any commutative ring, we have

$$\mathrm{Nil}(A) = \bigcap_{\mathfrak{p}\in\mathrm{Spec}(A)} \mathfrak{p} \subseteq \bigcap_{\mathfrak{m}\in\mathrm{MaxSpec}(A)} \mathfrak{m} = \mathrm{rad}(A).$$

For the reverse inclusion, let Ω be an algebraic closure for E and recall that $K^{p^{-\infty}}$ is the perfect closure of K in Ω. Suppose $\mathrm{ch}(K) = p > 0$ for the moment. Note that by applying Proposition 5.5 (iii) by replacing (A, K, B) by $(\Omega, E, E \otimes_K F)$, we obtain

$$\iota_{\Omega,E\otimes_K F}^{-1}(\mathrm{Jac}(\Omega \otimes_K F)) = \mathrm{Jac}(E \otimes_K F)$$

hence

$$\Omega \otimes_E \mathrm{Jac}(E \otimes_K F) \subseteq \mathrm{Jac}(\Omega \otimes_E (E \otimes_K F)) = \mathrm{Jac}(\Omega \otimes_K F).$$

By Proposition 5.8 applied by replacing (A, K, B) by $(\Omega, K^{p^{-\infty}}, K^{p^{-\infty}} \otimes_K F)$, since $\Omega^{\mathrm{Aut}(\Omega/K)} = K^{p^{-\infty}}$ (c.f. [Commutative Algebra, Theorem 13.16 (iv)]), we obtain

$$\Omega \otimes_E \mathrm{Jac}(E \otimes_K F) \subseteq \mathrm{Jac}(\Omega \otimes_K F) \subseteq (\mathrm{Jac}(K^{p^{-\infty}} \otimes_K F))_{\Omega\otimes_K F}.$$

If $\mathrm{Jac}(K^{p^{-\infty}} \otimes_K F) \subseteq \mathrm{Nil}(K^{p^{-\infty}} \otimes_K F)$, this will imply the nilpotency of every element of $\mathrm{Jac}(E \otimes_K F)$. Therefore, without loss of generality, it suffices to prove the result when $E = K^{p^{-\infty}}$. By repeating the argument with F instead of E, it suffices to show that $\mathrm{Jac}(K^{p^{-\infty}} \otimes_K K^{p^{-\infty}}) \subseteq \mathrm{Nil}(K^{p^{-\infty}} \otimes_K K^{p^{-\infty}})$.

Let $x = \sum_{i=1}^n a_i \otimes b_i \in \mathrm{Jac}(K^{p^{-\infty}} \otimes_K K^{p^{-\infty}})$ where $a_i, b_i \in K^{p^{-\infty}} = \bigcup_{m\geq 1} K^{p^{-m}}$. Fix m large enough so that $a_i, b_i \in K^{p^{-m}}$ for all $1 \leq i \leq n$. It follows that

$$x^{p^m} = \sum_{i=1}^n a_i^{p^m} \otimes b_i^{p^m} \in K.$$

It follows that $x^{p^m} \in K \setminus K^\times = \{0\}$ because no element of the Jacobson radical can be a unit, hence x is nilpotent.

(When $\mathrm{ch}(F) = 0$, the same proof works but one replaces $K^{p^{-\infty}}$ by K and the ring $K^{p^{-\infty}} \otimes_K K^{p^{-\infty}}$ just becomes K, so the result is trivial.)

Theorem 5.12. Let K be a field and E, F be two K-fields. The following are equivalent :

(i) The field extension E/K is separable, i.e. if L is a K-field containing E and $K^{p^{-1}}$, the map

$$E \otimes_K K^{p^{-1}} \to L,$$

given by multiplication, is injective

(ii) For every K-field F, $\mathrm{Jac}(E \otimes_K F) = 0$

(iii) For every K-field F, $\mathrm{Nil}(E \otimes_K F) = 0$

(iv)* $\mathrm{Nil}(E \otimes_K K^{p^{-1}}) = 0$.

(*) This statement only makes sense in characteristic p. For characteristic zero, the statements (i) to (iii) are always true.

Proof. ((i) $\Rightarrow$ (ii)) This follows by Corollary 5.9 since it implies

$$\mathrm{Jac}(E \otimes_K F) \subseteq E \otimes_K \mathrm{Jac}(F) = E \otimes_K 0 = 0.$$

((ii) $\iff$ (iii)) This is clear by Proposition 5.11.

((iii) $\Rightarrow$ (iv)) This is obvious.

((iv) $\Rightarrow$ (i)) Suppose that there exists $x_1, \cdots, x_n \in E$ and $a_1, \cdots, a_n \in K^{p^{-1}}$ such that $\sum_{i=1}^n x_i a_i = 0$ in L. Raising to the p^{th} power gives $\sum_{i=1}^n x_i^p a_i^p = 0$, an equation in E since $a_i^p \in K$. This implies

$$\left(\sum_{i=1}^n x_i \otimes a_i \right)^p = \sum_{i=1}^n x_i^p \otimes a_i^p = \left(\sum_{i=1}^n x_i^p a_i^p \right) \otimes 1 = 0,$$

hence $\sum_{i=1}^n x_i \otimes a_i \in \mathrm{Nil}(E \otimes_K K^{p^{-1}}) = \{0\}$, i.e. E and $K^{p^{-1}}$ are linearly disjoint over K, so that E/K is separable.

Corollary 5.13. Let $E_1, \cdots, E_n$ be K-fields. Assume that $n-1$ of those fields are separable over K and that $n-1$ of them are finite over K (possibly different ones). Then $\bigotimes_{i=1}^n E_i \stackrel{\text{def}}{=} E_1 \otimes_K E_2 \otimes_K \cdots \otimes_K E_n$ is isomorphic to a direct product of a finite number of K-fields. Furthermore, if $E_1, \cdots, E_n$ are finite extensions of K, the K-fields appearing in the product are also finite extensions of K.

Proof. We argue by induction on $n \geq 2$. For $n = 2$, if E_1 is separable, we know that $\mathrm{Jac}(E_1 \otimes_K E_2) = 0$. One of those fields is a finite extension, hence $E_1 \otimes_K E_2$ is a finite algebra over a field. By Corollary 4.40, since $E_1 \otimes_K E_2$ is radical-free, it is a direct product of fields which are finite over either E_1 or E_2 (depending on of E_2 or E_1 is a finite extension of K). If both are finite extensions of K, so do the direct factors.

If $n > 2$, we can assume that $E_3, \cdots, E_n$ are finite separable extensions of K, so by induction on n, we see that $\bigotimes_{i=2}^n E_i$ is a direct product of a finite number of K-fields. Since tensor products and direct products commute, we conclude by the case where $n = 2$ on each direct factor.

Example 5.14. (Some separable field theory) Let E/K be a field extension, $f(t) \in K[t]$ be an irreducible polynomial and $F \stackrel{\text{def}}{=} K[t]/(f(t))$. When E or F is separable over K, the K-algebra $E \otimes_K F \simeq E[t]/(f(t))$ is isomorphic to a direct product of fields by Corollary 5.13. If $f(t) = \prod_{i=1}^n f_i(t)$ is the factorization of $f(t)$ over $E[t]$ into distinct irreducible factors, then the isomorphism of Corollary 5.13 gives

$$E[t]/(f(t)) \simeq \prod_{i=1}^n E[t]/(f_i(t)).$$

To see this, note that if $E[t]/(f(t)) \simeq \prod_{i=1}^n F_i$ are the fields appearing in Corollary 5.13, the projection to F_i gives a surjective morphism $E[t] \to F_i$, so $F_i \simeq E[t]/(f_i(t))$ for some irreducible polynomial $f_i(t) \in E[t]$.

This gives the equality $(f(t))_{E[t]} = \bigcap_{i=1}^n (f_i(t))_{E[t]}$ between ideals of $E[t]$. Note that $f(t)$ divides $\prod_{i=1}^n f_i(t)$ since the latter annihilates $E[t]/(f(t))$, hence $\prod_{i=1}^n f_i(t) \in (f(t))_{E[t]}$. Since $\deg f = \sum_{i=1}^n \deg f_i$ by the isomorphism $E[t]/(f(t)) \simeq \prod_{i=1}^n E[t]/(f_i(t))$, this means $f(t) = \prod_{i=1}^n f_i(t)$ (by assuming that $f(t)$ and each $f_i(t)$ are monic polynomials).

Note that we already knew this when F/K was separable (i.e. when $f(t)$ was an irreducible separable polynomial). The new statement here is that this is also true when E is separable, regardless of whether $f(t)$ is separable or not ; in other words, to factor an irreducible inseparable polynomial into inseparable factors, you need to use an inseparable field extension, otherwise the irreducible factors you will obtain will appear with multiplicity 1.

5.3 Tensor product of completely reducible modules

In this section, K is a field, A, B are two K-algebras, M is a left A-module and N is a right B-module.

Definition 5.15. For a left (resp. right) A-module M, let $\mathrm{Lsubmod}_A(M)$ (resp. $\mathrm{Rsubmod}_A(M)$) denote the set of left (resp. right) A-submodules of M. Let B be a ring and N a left B-module.

(i) A map $\Phi : \mathrm{Lsubmod}_A(M) \to \mathrm{Lsubmod}_B(N)$ is said to **preserve the radical** if $\Phi(\mathrm{rad}_A(M)) = \mathrm{rad}_B(N)$.

(ii) A map $\Phi : \mathrm{Lsubmod}_A(M) \to \mathrm{Lsubmod}_B(N)$ is said to **preserve direct sums** if for two submodules $M_1, M_2 \in \mathrm{Lsubmod}_A(M)$, we have $\Phi(M_1 \oplus M_2) = \Phi(M_1) \oplus \Phi(M_2)$.

(iii) A map $\Phi : \mathrm{Lsubmod}_A(M) \to \mathrm{Lsubmod}_B(N)$ is said to be **inclusion-preserving** if for two submodules $M_1, M_2 \in \mathrm{Lsubmod}_A(M)$ with $M_1 \subseteq M_2$, we have $\Phi(M_1) \subseteq \Phi(M_2)$.

Analogous definitions apply if we replace $\mathrm{Lsubmod}_A(M)$ or $\mathrm{Lsubmod}_B(N)$ by their right counterparts $\mathrm{Rsubmod}_A(M)$ and $\mathrm{Rsubmod}_B(N)$.

Lemma 5.16. Let A and B be K-algebras and N a simple left B-module. Interpret the right $C_B(N)$-module $C_B(N)_r$ as a $(C_B(N)^{\mathrm{opp}}, C_B(N))$-bimodule. For every left A-module M, consider the isomorphism of $A \otimes_K B$-modules

$$\varphi_N : M \otimes_K C_B(N)_r \otimes_{C_B(N)} N \to M \otimes_K N, \qquad m \otimes \varphi \otimes n \mapsto m \otimes \varphi(n).$$

The following map is a bijection between the set of left $(A \otimes_K C_B(N)^{\mathrm{opp}})$-submodules of $M \otimes_K C_B(N)_r$ and the set of left $(A \otimes_K B)$-submodules of $M \otimes_K N$:

$$\Phi : \mathrm{Lsubmod}_{A\otimes_K C_B(N)^{\mathrm{opp}}}(M \otimes_K C_B(N)_r) \to \mathrm{Lsubmod}_{A\otimes_K B}(M \otimes_K N),$$
$$P \mapsto \varphi_N(P \otimes_{C_B(N)} N).$$

Furthermore, this map preserves direct sums, inclusions and the radical.

Proof. We wish to apply Corollary 3.15. In this result, make the following substitutions :

$$(P, A, D, V, N) \mapsto (N, B, C_B(N), M \otimes_{C_B(N)} C_B(N)_r, P).$$

Furthermore, replace the subset $S \subseteq \mathrm{End}_D(V) = \mathrm{End}_{C_B(N)}(M \otimes_{C_B(N)} C_B(N)_r)$ in the result by the set of homotheties of the left A-module $M \otimes_{C_B(N)} C_B(N)_r$, which are right $C_B(N)$-linear since this is a left $A \otimes_K C_B(N)^{\mathrm{opp}}$-module. It follows that there is a bijection between the set of right $C_B(N)^{\mathrm{opp}}$-submodules of $M \otimes_{C_B(N)} C_B(N)_r$ stable under left multiplication by elements of A and the set of B-submodules of $M \otimes_{C_B(N)} C_B(N)^{\mathrm{opp}} \otimes_K N$ stable under those same multiplications. In other words, the application

$$P \mapsto P \otimes_{C_B(N)} N$$

puts in bijection the $(A \otimes_K C_B(N)^{\text{opp}})$-submodules of $M \otimes_{C_B(N)} C_B(N)_r$ and the $(A \otimes_K B)$-submodules of $M \otimes_{C_B(N)} C_B(N)^{\text{opp}} \otimes_K N$. Since φ_N is an isomorphism, the first part of the proof follows. The second part is obvious by properties of the functor $(-) \otimes_{C_B(N)} N$ and Remark 5.17.

Remark 5.17.

- In Definition 5.15, if Φ is an inclusion-preserving bijection where Φ^{-1} is also inclusion-preserving, then it preserves the radical ; this is because it puts in correspondence the set of maximal submodules too, so $\Phi(\text{rad}_A(M)) \subseteq \text{rad}_B(N)$; the reverse inclusion comes from applying the same reasoning to Φ^{-1}. It also preserves direct summands ; we have $M = M' \oplus M''$ if and only if the only submodule $M_0 \subseteq M', M''$ is zero and the only submodule $M', M'' \subseteq M_1$ is $M_1 = M$, and this property is preserved under inclusion-preserving bijections. It follows that it also preserves direct sums by applying the result to $M' \oplus M'' \subseteq M$, i.e. by restricting Φ to those submodules of $M' \oplus M''$.

- We have the equality $\text{Lsubmod}_A(M) = \text{Rsubmod}_{A^{\text{opp}}}(M^{\text{opp}})$ by definition of the opposite ring/module. This implies

$$\text{Lsubmod}_{A \otimes_K B}(M \otimes_K N) \simeq \text{Rsubmod}_{B^{\text{opp}} \otimes_K A^{\text{opp}}}(N^{\text{opp}} \otimes_K M^{\text{opp}}).$$

  defined by using the isomorphism $(M \otimes_K N)^{\text{opp}} \simeq N^{\text{opp}} \otimes_K M^{\text{opp}}$.

- Using the fact that left $(A \otimes_K B)$-submodules of $M \otimes_K N$ are the same as right $A^{\text{opp}} \otimes_K B^{\text{opp}}$-submodules of $M^{\text{opp}} \otimes_K N^{\text{opp}}$, we also have a bijection

$$\text{Lsubmod}_{A \otimes_K B}(M \otimes_K N) \simeq \text{Rsubmod}_{A^{\text{opp}} \otimes_K B^{\text{opp}}}(M^{\text{opp}} \otimes_K N^{\text{opp}}).$$

- If M is a (A, B)-bimodule, then M^{opp} is a $(B^{\text{opp}}, A^{\text{opp}})$-bimodule. Seeing this when $A = B$ and the left A-module M is given its canonical (A, A^{opp})-bimodule structure, we see that M^{opp} is an $((A^{\text{opp}})^{\text{opp}}, A^{\text{opp}})$-bimodule, i.e. $M^{\text{opp}} = M$ as (A, A^{opp})-bimodules. Similar remarks apply to the case when M is a right A-module, and we can apply this to the (A, A^{opp})-bimodule A_ℓ or the (A^{opp}, A)-bimodule A_r.

- If M is a left A-module, then $C_{A^{\text{opp}}}(M^{\text{opp}}) = C_A(M)^{\text{opp}}$ (this can be checked trivially ; the reason why it is equal to $C_A(M)^{\text{opp}}$ and not $C_A(M)$ is because in the computation of $C_{A^{\text{opp}}}(M^{\text{opp}})$, we must see M^{opp} as a right A^{opp}-module, hence a right $C_{A^{\text{opp}}}(M^{\text{opp}})$-module, which means composition is in the reverse order). It follows that the (A, A^{opp})-bimodule A_ℓ is such that $(A_\ell)^{\text{opp}} = A_\ell = (A^{\text{opp}})_\ell$ as (A, A^{opp})-bimodules. Similar remarks apply to A_r.

Corollary 5.18. Let A and B be rings and M a simple left A-module. Interpret the right $C_A(M)$-module $C_A(M)_r$ as a $(C_A(M)^{\text{opp}}, C_A(M))$-bimodule and the left $C_A(M)$-module M as a $(C_A(M), C_A(M)^{\text{opp}})$-bimodule. For every left B-module N, consider the isomorphism of $A \otimes_K B$-modules

$$\psi_M : M \otimes_{C_A(M)^{\text{opp}}} C_A(M)_r \otimes_K N \to M \otimes_K N, \qquad m \otimes \psi \otimes n \mapsto \psi(m) \otimes n.$$

The following map is a bijection between the set of left $(C_A(M)^{\text{opp}} \otimes_K B)$-submodules of $C_A(M)_r \otimes_K N$ and the set of left $(A \otimes_K B)$-submodules of $M \otimes_K N$:

$$\Phi : \text{Lsubmod}_{C_A(M)^{\text{opp}} \otimes_K B}(C_A(M)_r \otimes_K N) \to \text{Lsubmod}_{A \otimes_K B}(M \otimes_K N),$$
$$Q \mapsto \psi_N(M \otimes_{C_A(M)^{\text{opp}}} Q).$$

Furthermore, this map preserves direct sums, inclusions and the radical.

Proof. Apply Lemma 5.16 by substituting the following data

$$(A, M, B, N) \mapsto (B, N, A, M).$$

By Remark 5.17, this gives us a bijection

$$\begin{aligned}\Phi : \mathrm{Lsubmod}_{B\otimes_K C_A(M)^{\mathrm{opp}}}(N \otimes_K C_A(M)_r) &\to \mathrm{Lsubmod}_{B\otimes_K A}(N \otimes_K M),\\ P &\mapsto \varphi_M(P \otimes_{C_A(M)} M)\end{aligned}$$

where φ_M is obtained by applying $\psi \in C_A(M)$ to $m \in M$ as in Lemma 5.16. Using Remark 5.17 again, we get

$$\begin{aligned}\mathrm{Lsubmod}_{C_A(M)^{\mathrm{opp}}\otimes_K B}(C_A(M)_r \otimes_K N) &= \mathrm{Rsubmod}_{C_A(M)\otimes_K B^{\mathrm{opp}}}(C_A(M)_r \otimes_K N^{\mathrm{opp}})\\ &\simeq \mathrm{Lsubmod}_{B\otimes_K C_A(M)^{\mathrm{opp}}}(N \otimes_K C_A(M)_r)\\ &\simeq \mathrm{Lsubmod}_{B\otimes_K A}(N \otimes_K M)\\ &\simeq \mathrm{Rsubmod}_{A^{\mathrm{opp}}\otimes_K B^{\mathrm{opp}}}(M^{\mathrm{opp}} \otimes_K N^{\mathrm{opp}})\\ &\simeq \mathrm{Lsubmod}_{A\otimes_K B}(M \otimes_K N).\end{aligned}$$

We merely flipped the tensor factors in each of those bijections by using the $(-)^{\mathrm{opp}}$ operation, so the composition of all of them still amounts to applying $\psi \in C_A(M)$ to $m \in M$.

Corollary 5.19. Let A, B be rings, M a simple left A-module and N a simple left B-module. Consider the K-algebra $C_A(M) \otimes_K C_B(N)$, a tensor product of two division K-algebras. The $(A \otimes_K B)$-module $M \otimes_K N$ is canonically a $C_A(M) \otimes_K C_B(N)$-module by the definition $(\varphi \otimes \psi)(m \otimes n) \overset{\mathrm{def}}{=} \varphi(m) \otimes \psi(n)$. This gives an isomorphism

$$(C_A(M) \otimes_K C_B(N))_r \otimes_{C_A(M)\otimes C_B(N)} (M \otimes_K N) \simeq M \otimes_K N$$

given by multiplication. For a right ideal $\mathfrak{a} \trianglelefteq C_A(M) \otimes_K C_B(N)$, we let $\mathfrak{a}(M \otimes_K N)$ be the image of $\mathfrak{a} \otimes (M \otimes_K N)$ under this map. The application

$$\mathfrak{a} \mapsto \mathfrak{a}(M \otimes_K N)$$

is a bijection between the set of right ideals of $C_A(M) \otimes_K C_B(N)$ and the set of left $(A \otimes_K B)$-submodules of $M \otimes_K N$, i.e.

$$\mathrm{Rsubmod}_{C_A(M)\otimes_K C_B(M)}(C_A(M) \otimes_K C_B(N)) \simeq \mathrm{Lsubmod}_{A\otimes_K B}(M \otimes_K N).$$

Proof. It suffices to apply Lemma 5.16 and Corollary 5.18 successively on the right and left tensor factors of $M \otimes_K N$:

$$\begin{aligned}\mathrm{Lsubmod}_{A\otimes_K B}(M \otimes_K N) &\simeq \mathrm{Lsubmod}_{A\otimes_K C_B(N)^{\mathrm{opp}}}(M \otimes_K C_B(N)_r)\\ &\simeq \mathrm{Lsubmod}_{C_A(M)^{\mathrm{opp}}\otimes_K C_B(N)^{\mathrm{opp}}}(C_A(M)_r \otimes_K C_B(N)_r)\end{aligned}$$

since the latter is easily seen to be $\mathrm{Rsubmod}_{C_A(M)\otimes_K C_B(N)}(C_A(M)_r \otimes_K C_B(N)_r)$, i.e. the set of right ideals of $C_A(M) \otimes_K C_B(M)$. Up to permuting the tensor factors, this map was obtained by tensoring the two operations

$$\begin{aligned}C_A(M) \otimes_K M \to M, &\quad \psi \otimes m \mapsto \psi(m)\\ C_B(N) \otimes_K N \to N, &\quad \varphi \otimes n \mapsto \varphi(n),\end{aligned}$$

so the result is clear.

Theorem 5.20. Let K be a field, A, B two K-algebras, M a left A-module and N a left B-module.

(i) If M, N are non-zero and $M \otimes_K N$ is a completely reducible (resp. simple) left $(A \otimes_K B)$-module, then M and N are completely reducible (resp. simple).

(ii) Assume M and N are simple modules. The following are equivalent :

- The $(A \otimes_K B)$-module $M \otimes_K N$ is radical-free
- The K-algebra $C_A(M) \otimes_K C_B(N)$ is radical-free
- The K-algebra $Z(C_A(M)) \otimes_K Z(C_B(N))$ is radical-free.

(iii) Assume M and N are simple modules. The following are equivalent :

- The $(A \otimes_K B)$-module $M \otimes_K N$ is simple (resp. completely reducible)
- The K-algebra $C_A(M) \otimes_K C_B(N)$ is simple (resp. semisimple).

Proof. (i) Let $N' \leq N$ be a B-submodule. It follows that $M \otimes_K N'$ is a submodule of $M \otimes_K N$ by flatness (because M is a K-vector space), so there exists an $(A \otimes_K B)$-linear projection $\pi : M \otimes_K N \to M \otimes_K N'$. Since $M \neq 0$, there exists $x \in M$ and $\alpha \in \mathrm{Hom}_K(M, K)$ such that $\alpha(x) = 1$. The map $\alpha : M \to K$ can be extended to an endomorphism $\widetilde{\alpha} : M \otimes_K N \to M \otimes_K N$; explicitly, we have $\widetilde{\alpha}(m \otimes n) \overset{\text{def}}{=} \alpha(m) x \otimes n$. Note that the map $n \mapsto x \otimes n$ gives an isomorphism of N with $\langle x \rangle_K \otimes N \simeq K \otimes_K N \simeq N$ which also maps N' isomorphically onto $\langle x \rangle_K \otimes_K N'$. Because K is a field, we can fix K-bases for M and N (where the basis of M contains x) and deduce

$$\pi(\langle x \rangle_K \otimes_K N) \subseteq (M \otimes_K N') \cap (\langle x \rangle \otimes_K N) = \langle x \rangle_k \otimes_K N',$$

so $\pi|_{\langle x \rangle_K \otimes_K N}$ is a projection of $\langle x \rangle_K \otimes_K N$. Since $\pi|_{M \otimes_K N'} = \mathrm{id}_{M \otimes_K N'}$, it follows that $\mathrm{im}\, \pi|_{\langle x \rangle_K \otimes_K N} = \langle x \rangle_K \otimes_K N'$, hence $\langle x \rangle_K \otimes_K N'$ is a direct summand of $\langle x \rangle_K \otimes_K N$, meaning that N' is a direct summand of N.

If $M \otimes_K N$ is simple but N is not, it is still semisimple, so we can find two direct summands $N = N' \oplus N'$, which implies $M \otimes_K N = (M \otimes_K N') \oplus (M \otimes_K N'')$, a contradiction. Therefore, N is simple ; similarly, M is simple.

(ii),(iii) The entire result is clear except the equivalence between the radical-freeness of $C_A(M) \otimes_K C_B(N)$ and that of $Z(C_A(M)) \otimes_K Z(C_B(N))$ (because the first two points are obviously equivalent). In fact, we can show that

$$\mathrm{Jac}(C_A(M) \otimes_K C_B(N)) = \mathrm{Jac}(Z(C_A(M)) \otimes_K Z(C_B(M))) \Big(C_A(M) \otimes_K C_B(N) \Big).$$

$(\subseteq)$ Consider the isomorphism

$$C_A(M) \otimes_K C_B(N) \simeq C_A(M) \otimes_{Z(C_A(M))} \big(C_B(N) \otimes_{Z(C_B(N))} (Z(C_A(M)) \otimes_K Z(C_B(N))) \big),$$
$$\varphi \otimes \psi \mapsto \varphi \otimes (\psi \otimes (1 \otimes 1)).$$

It then suffices to apply Corollary 5.9 twice (c.f. Remark 5.7) and the multiplication map twice to deduce the inclusion since the right-hand side is a two-sided ideal in $C_A(M) \otimes_K C_B(N)$ because

$$\mathrm{Jac}(Z(C_A(M)) \otimes_K Z(C_B(M))) \Big(C_A(M) \otimes_K C_B(N) \Big)$$
$$=$$
$$\Big(C_A(M) \otimes_K C_B(N) \Big) \mathrm{Jac}(Z(C_A(M)) \otimes_K Z(C_B(M)))$$

follows from the fact that $\mathrm{Jac}(Z(C_A(M)) \otimes_K Z(C_B(M))) \subseteq Z(C_A(M) \otimes_K C_B(N))$.

($\supseteq$) The elements of $\mathrm{Jac}(Z(C_A(M)) \otimes_K Z(C_B(M)))$ are nilpotent and contained in the center of $C_A(M) \otimes_K C_B(N)$, which means that the right-hand side of the statement is a nilideal of $C_A(M) \otimes_K C_B(N)$; it is therefore contained in the Jacobson radical of $C_A(M) \otimes_K C_B(N)$ (c.f. Corollary 4.23 (iv)), i.e. the left-hand side.

Theorem 5.21. Let K be a field, A, B be K-algebras, M a left A-module and N a left B-module. Suppose M and N are isotypically simple and that one of the two is finite-dimensional over K. If $C_B(N)$ is a central K-algebra (meaning that $Z(C_B(N)) = K$), then $M \otimes_K N$ is an isotypically simple $(A \otimes_K B)$-module.

Proof. Suppose M is isotypically simple of type P and N is isotypically simple of type Q. We reduce to the case where $M = P$ and $N = Q$. If $M \simeq P^{\oplus I}$ and $N \simeq Q^{\oplus I}$, we have an isomorphism of $(A \otimes_K B)$-modules

$$M \otimes_K N \simeq P^{\oplus I} \otimes_K Q^{\oplus J} \simeq (P \otimes_K Q)^{\oplus (I \times J)}.$$

It suffices to show that the hypotheses on N carry to Q. The ring $C_B(Q)$ is a division ring, so $\mathrm{Hom}_B(Q, N)$ is a right $C_B(Q)$-vector space ; this means it is free. By Corollary 1.38 and Proposition 3.14 (ii), this implies

$$Z(C_B(Q)) = Z(\mathrm{End}_{C_B(Q)}(\mathrm{Hom}_B(Q, N))) = Z(C_B(N)) = K$$

by the assumption on $C_B(N)$.

Assume that M and N are simple. The K-algebra

$$Z(C_A(M)) \otimes_K Z(C_B(N)) = Z(C_A(M)) \otimes_K K \simeq Z(C_A(M))$$

is a field (and in particular radical-free), so $M \otimes_K N$ is a radical-free $(A \otimes_K B)$-module by Theorem 5.20 (ii). If M (resp. N) is finite-dimensional over K, then $M \otimes_K N$ is a B-module (resp. A-module) of finite length, and thus an $(A \otimes_K B)$-module of finite length. This implies that it is a radical-free artinian $(A \otimes_K B)$-module, hence is completely reducible by Theorem 4.29. By Theorem 5.20 applied again, we deduce that $C_A(M) \otimes_K C_B(N)$ is semisimple ; by this result applied a third time, it now suffices to show that $C_A(M) \otimes_K C_B(N)$ is iso simple to finish the proof.

Let $\mathfrak{a} \trianglelefteq C_A(M) \otimes_K C_B(N)$ be a non-zero two-sided ideal. It is a right $C_B(N)$-vector subspace stable under the subgroup G of automorphisms of the form $1 \otimes \varphi_a$ where $\varphi_a \in \mathrm{Aut}(C_B(N))$ is given by $\varphi_a(x) = axa^{-1}$, so since $C_B(N)^G = Z(C_B(N)) = K$, we deduce by Corollary 3.16 that $\mathfrak{a} = V \otimes_K C_B(N)$ where $V \leq C_A(M)$ is a K-vector subspace of $C_A(M)$. Since $\mathfrak{a}$ is a two-sided ideal, V is a left ideal of $C_A(M)$ which is non-zero (because $\mathfrak{a} \neq 0$), hence $V = C_A(M)$, i.e. $\mathfrak{a} = C_A(M) \otimes_K C_B(N)$.

Corollary 5.22. Let A, B be two simple K-algebras, one of the two being finite-dimensional over K and one of the two being a central K-algebra. Then $A \otimes_K B$ is a simple K-algebra.

Proof. Theorem 5.21 proves that $(A \otimes_K B)_\ell$ is isotypically simple, hence $A \otimes_K B$ is a simple K-algebra by definition.

Corollary 5.23. Let A be a CSA over K of dimension $m \geq 1$ and Ω an algebraic closure for K. Then $m = n^2$ is a perfect square (i.e. $n \in \mathbb{N}$) and we have an isomorphism of Ω-algebras $\Omega \otimes_K A \simeq \mathrm{Mat}_{n \times n}(\Omega)$.

Proof. By the previous corollary, $\Omega \otimes_K A$ is simple and has center isomorphic to $Z(\Omega) \otimes_K Z(A) = \Omega \otimes_K K \simeq \Omega$, i.e. it is a CSA over the algebraically closed field Ω. The result follows by Corollary 3.40 (ii).

5.4 Separable algebras and modules over a field

In this section, K is a field. Note that in characteristic zero, every K-algebra A and every A-module M is separable over K, so the results of this section give strong statements about algebras and modules.

Definition 5.24. Let K be a field, A a K-algebra and M a left A-module.

(i) The A-module M is said to be **separable over** K if for every field extension E/K, the left $(E \otimes_K A)$-module $E \otimes_K M$ is radical-free.

(ii) The K-algebra A is said to be **separable over** K if A_ℓ is a separable module over K, i.e. if $\mathrm{Jac}(E \otimes_K A) = 0$ for all field extensions E/K.

Proof. Let K be a field, A a K-algebra and M a left A-module.

(i) If M is separable over K, then every A-submodule of a M is separable over K.

(ii) If $\{M_i\}_{i\in I}$ is a family of separable A-modules over K, then $\bigoplus_{i\in I} M_i$ is separable over K.

(iii) If M is separable over K, then for every field extension E/K, the $(E \otimes_K A)$-module $E \otimes_K M$ is separable over E.

Proof. Consider a field extension E/K.

(i) Let $M' \leq M$ be such an A-submodule. By Proposition 4.8 applied to the inclusion map $E \otimes_K M' \to E \otimes_K M$,
$$\mathrm{rad}_{E\otimes_K A}(E \otimes_K M') \subseteq \mathrm{rad}_{E\otimes_K A}(E \otimes_K M) = 0.$$

(ii) Recalling that $E \otimes_K \bigoplus_{i\in I} M_i \simeq \bigoplus_{i\in I} E \otimes_K M_i$, by Proposition 4.9, we obtain
$$\mathrm{rad}_{E\otimes_K A}(E \otimes_K \bigoplus_{i\in I} M_i) \simeq \mathrm{rad}_{E\otimes_K A}(\bigoplus_{i\in I} E \otimes_K M_i) = \bigoplus_{i\in I} \mathrm{rad}_{E\otimes_K A}(E \otimes_K M_i) = 0.$$

(iii) This follows since for every field extension E'/E, we have an isomorphism of rings/modules
$$E' \otimes_E (E \otimes_K A) \simeq E' \otimes_K A, \quad E' \otimes_E (E \otimes_K M) \simeq E' \otimes_K M$$
and the module structures correspond, so the separability of $E \otimes_K M$ over E follows from that of M over K.

Proposition 5.25. Let K be a field, A a K-algebra and M a finitely generated A-module. Suppose there exists an algebraic field extension F/K with F perfect such that $P \otimes_K M$ is a radical-free $(P \otimes_K A)$-module. Then M is separable over K.

Proof. Let E/K be a field extension and Ω be an algebraic closure of E. Since P/K is algebraic, we can assume without loss of generality that $P \subseteq \Omega$, which implies that Ω/P is a separable extension. We are in the conditions of Corollary 5.9 (M is a finitely generated A-module and Ω/P is separable), which means that

$$\mathrm{rad}_{\Omega\otimes_K A}(\Omega \otimes_K M) \subseteq \Omega \otimes_P \mathrm{rad}_{P\otimes_K A}(P \otimes_K M) = \Omega \otimes_K 0 = 0.$$

Considering the isomorphism $\Omega \otimes_K M \simeq \Omega \otimes_E (E \otimes_K M)$, letting $\iota : E \otimes_K M \to \Omega \otimes_E (E \otimes_K M) \simeq \Omega \otimes_K M$ denote the canonical map (which is injective because Ω/E is a field extension, e.g. Ω is an E-vector space), Proposition 5.5 (ii) gives

$$\iota(\mathrm{rad}_{E\otimes_K A}(E \otimes_K M)) \subseteq \mathrm{rad}_{\Omega\otimes_K A}(\Omega \otimes_K M) = 0 \quad \Longrightarrow \quad \mathrm{rad}_{E\otimes_K A}(E \otimes_K M) = 0.$$

Corollary 5.26. Let K be a field and A a K-algebra. Consider the two following statements :

(i) There exists a field extension P/K such that P is perfect and $\mathrm{Jac}(P \otimes_K A) = 0$

(ii) A is a separable K-algebra.

Then (i) implies (ii), and if A is finite-dimensional over K, (i) and (ii) are equivalent.

Proof. The first part of the statement follows directly from Proposition 5.25.

For the second part of the statement, apply the proof of Proposition 5.25 to the case where $M = A_\ell$, but instead of using Proposition 5.5 (ii) (which is where we need the fact that Ω/E is algebraic), we pick an arbitrary field Ω containing both E and P as K-subfields (it could be a residue field of some $\mathfrak{p} \in \mathrm{Spec}\,(E \otimes_K P)$ for instance, c.f. Definition 10.28) ; this preserves the fact that Ω/P is separable and since $E \otimes_K A$ is finite-dimensional over E, Proposition 5.5 (iii) applies (because $E \otimes_K A$ is left-artinian by Example 2.27) and gives us the same result.

Proposition 5.27. Let K be a field, A a K-algebra and M a completely reducible A-module. The following are equivalent :

(i) M is separable over K

(ii) For each simple A-submodule P of M, $Z(C_A(P))/K$ is a separable field extension.

Proof. Recall (c.f. Definition 2.56) that if P is a simple A-module, the isotypical component of M is denoted by M_P. By writing

$$M \simeq \bigoplus_{P \,|\, M_P \neq 0} M_P,$$

Definition 5.4 (i) and (ii) implies that we can assume without loss of generality that $M = P$ where I is a set and P is a simple A-module. Consider a field extension E/K and note that E is a simple E-module satisfying $Z(E) = E$. By Theorem 5.20 (ii), the following are equivalent :

- M is separable over K
- For every field extension E/K, $E \otimes_K M$ is radical-free
- For every field extension E/K, $E \otimes_K Z(C_A(P))$ is radical-free
- The K-algebra $Z(C_A(P))$ is separable
- The field extension $Z(C_A(P))/K$ is separable.

This completes the proof.

Corollary 5.28. Let K be a field and A a semisimple K-algebra. The following are equivalent :

(i) A is separable over K

(ii) $Z(A)$ is separable over K

(iii) Write $A = \prod_{i=1}^{n} A_i$ where the A_i are simple K-algebras (c.f. Theorem 3.38). Then $Z(A_i)/K$ is a separable field extension for $i = 1, \cdots, n$.

Proof. This follows from Theorem 3.38 and Proposition 5.27.

Definition 5.29. Let K be a field, A a K-algebra and M an A-module.

(i) We say that M is **absolutely completely reducible over** K if for every field extension E/K, the $(E \otimes_K A)$-module $E \otimes_K M$ is completely reducible.

(ii) We say that A is **absolutely semisimple over** K if A_ℓ is an absolutely completely reducible A-module over K.

Proposition 5.30. Let K be a field, A a K-algebra and M a left A-module.

(i) If M is absolutely completely reducible over K, then every A-submodule of M is absolutely completely reducible over K.

(ii) If $\{M_i\}_{i \in I}$ is a family of absolutely completely reducible A-modules over K, then $\bigoplus_{i \in I} M_i$ is absolutely completely reducible over K.

(iii) If M is absolutely completely reducible over K, then for every field extension E/K, the $(E \otimes_K A)$-module $E \otimes_K M$ is absolutely completely reducible over E.

Proof. Consider a field extension E/K.

(i) Let $M' \leq M$ be such an A-submodule. Since $E \otimes_K M'$ is an $(E \otimes_K A)$-submodule of $E \otimes_K M$ which is completely reducible, $E \otimes_K M'$ is also completely reducible.

(ii) Since $E \otimes_K \bigoplus_{i \in I} M_i \simeq \bigoplus_{i \in I} E \otimes_K M_i$ can be written as a direct sum of completely reducible $(E \otimes_K A)$-submodules, it is completely reducible by definition.

(iii) This follows since for every field extension E'/E, we have an isomorphism of rings/modules

$$E' \otimes_E (E \otimes_K A) \simeq E' \otimes_K A, \quad E' \otimes_E (E \otimes_K M) \simeq E' \otimes_K M$$

and the module structures correspond, so the absolute complete reducibility of $E \otimes_K M$ over E follows from that of M over K.

Theorem 5.31. Let K be a field, A a K-algebra and M an A-module. Consider the following statements :

(i) M is absolutely completely reducible over K.

(ii) M is separable over K

Then (i) implies (ii), and if M is finite-dimensional over K, both statements are equivalent.

Proof. Completely reducible modules are radical-free by Proposition 4.9 (and the fact that the radical of a simple module is zero), so absolute complete reducibility implies separability. Conversely, in the case where M is finite-dimensional over K, let E/K be a field extension. The $(E \otimes_K A)$-module $E \otimes_K M$ is finite-dimensional over E, hence is left-artinian by Example 2.27 ; since it is radical-free, it is completely reducible by Theorem 4.29. This implies that M is absolutely completely reducible over K.

Corollary 5.32. Let K be a field and A a K-algebra. Consider the following statements :

(i) A is absolutely completely reducible over K.

(ii) A is separable over K

Then (i) implies (ii), and if A is finite-dimensional over K, both statements are equivalent.

Proof. This is straightforward from Theorem 5.31 applied to the case where $M = A_\ell$.

Theorem 5.33. Let A, B be K-algebras, M be a separable left A-module over K and N a left B-module. Then

$$\mathrm{rad}_{A\otimes_K B}(M \otimes_K N) \subseteq M \otimes_K \mathrm{rad}_B(N).$$

In particular, the tensor product of a radical-free module with a module which is separable over K gives a radical-free module.

Proof. First, we treat the case where N is simple, so that $\mathrm{rad}_B(N) = 0$. By Lemma 5.16, it suffices to show that the left $(A \otimes_K C_B(N)^{\mathrm{opp}})$-module $M \otimes_K C_B(N)_r$ is radical-free. We have an isomorphism of $(A \otimes_K C_B(N)^{\mathrm{opp}})$-modules

$$M \otimes_K C_B(N)_r \simeq (M \otimes_K Z(C_B(N))) \otimes_{Z(C_B(N))} C_B(N)_r.$$

Since M is separable over K and N is simple, considering the field extension $Z(C_B(N))/K$ implies that $M \otimes_K Z(C_B(N))$ is radical-free. By Corollary 5.9 (i), we deduce that $M \otimes_K C_B(N)_r$ is radical-free.

Onto the general case. Let $z = \sum_{i=1}^n m_i \otimes n_i \in \mathrm{rad}_{A\otimes_K B}(M \otimes_K N)$ where $m_i \in M$ and $n_i \in N$. Without loss of generality, we can suppose that the m_i are linearly independent over K. Let Q be a simple B-module ; to show that $n_i \in \mathrm{rad}_B(N)$, we have to show that whenever $f : N \to Q$ is a morphism of B-modules, we have $f(n_i) = 0$. Extend this morphism to M, so that $\mathrm{id}_M \otimes f : M \otimes_K N \to M \otimes_K Q$ satisfies

$$(\mathrm{id}_M \otimes f)(\mathrm{rad}_{A\otimes_K B}(M \otimes_K N)) \subseteq \mathrm{rad}_{A\otimes_K B}(M \otimes_K Q) = 0$$

by Proposition 4.8 and the first part of this proof. This means

$$\sum_{i=1}^n m_i \otimes f(n_i) = (\mathrm{id}_M \otimes f)(z) = 0 \quad \Longrightarrow \quad f(n_i) = 0$$

by the linear independence of the m_i over K. Therefore $n_i \in \mathrm{rad}_B(N)$, which completes the argument.

Corollary 5.34. Let A be a separable K-algebra and B a K-algebra. For every left B-module N, we have $\mathrm{rad}_{A\otimes_K B}(A \otimes_K N) \subseteq A \otimes_K \mathrm{rad}_B(N)$.

Proof. This is Theorem 5.33 in the case where $M = A_\ell$.

Corollary 5.35. Let A, B be K-algebras, M a left A-module and N a left B-module, both modules being separable over K. Then then $(A \otimes_K B)$-module $M \otimes_K N$ is separable over K.

Proof. Let E/K be a field extension. By separability of N, we see that the $(B \otimes_K E)$-module $N \otimes_K E$ is radical-free. By separability of M and Theorem 5.33,

$$\mathrm{rad}_{A\otimes_K(B\otimes_K E)}(M \otimes_K (N \otimes_K E)) \subseteq M \otimes_K \mathrm{rad}_{B\otimes_K E}(N \otimes_K E) = 0.$$

Since the $A \otimes_K (B \otimes_K E)$-module $M \otimes_K (N \otimes_K E)$ can be identified with the $E \otimes_K (A \otimes_K B)$-module $E \otimes_K (M \otimes_K N)$ (via $m \otimes (n \otimes e) \mapsto e \otimes (m \otimes n)$), we see that the latter is radical-free, which implies that $M \otimes_K N$ is separable over K.

Corollary 5.36. Let A and B be two K-algebras. If A is separable over K and $\mathrm{Jac}(B) = 0$ (i.e. if B is radical-free), then $\mathrm{Jac}(A \otimes_K B) = 0$ (i.e. $A \otimes_K B$ is radical-free).

Proof. It suffices to set $M = A_\ell$ and $N = B_\ell$ in the previous corollary.

Corollary 5.37. Let K be a field and A, B two K-algebras.

(i) If $A \otimes_K B$ is semisimple, then A and B are semisimple.

(ii) If A and B are semisimple, A is separable over K and one of A or B is finite-dimensional over K, then $A \otimes_K B$ is semisimple. In particular, if K is a perfect field (which is the case when $\mathrm{ch}(K) = 0$), the tensor product of finite-dimensional semisimple K-algebras is semisimple.

Proof. Part (i) follows by applying Theorem 5.20 (i) to $M = A_\ell$ and $N = B_\ell$. For part (ii), since A (resp. B) is finite-dimensional over K, $A \otimes_K B$ is a free left A-module (resp. right B-module) of finite rank. The semisimplicity of A and B implies that both are left-artinian, right-artinian and radical-free (c.f. Theorem 4.29), so by Proposition 2.28, $A \otimes_K B$ is left-artinian (resp. right-artinian). Since one algebra is separable and the other is radical-free, $A \otimes_K B$ is radical-free by Corollary 5.36, so that it is semisimple by Theorem 4.29.

Theorem 5.38. Let K be a field, A, B be two K-algebras and write $\mathscr{C}(A)$ for the set of isomorphism classes of all simple left A-modules which are finite-dimensional over K ; given $\alpha \in \mathscr{C}(A)$, write $\alpha = [P]$ for a representative P of this class, i.e. P is a simple left A-module in the isomorphism class.

For each isomorphism class $[R] \in \mathscr{C}(A \otimes_K B)$ represented by, there exist $[P] \in \mathscr{C}(A)$ and $[Q] \in \mathscr{C}(B)$ such that the $(A \otimes_K B)$-module R is isomorphic to a quotient of $P \otimes_K Q$. Furthermore, $[P]$ and $[Q]$ are unique with this property, giving a well-defined map $\mathscr{C}(A \otimes_K B) \to \mathscr{C}(A) \times \mathscr{C}(B)$ defined by $[R] \mapsto ([P], [Q])$.

Proof. Let $R \in C(A \otimes_K B)$ be a simple left $(A \otimes_K B)$-module. Since R is finite-dimensional over K, it is a left-artinian B-module, so there exists a simple B-submodule ; call it Q. Instead of seeing R as an $(A \otimes_K B)$-module, we interpret it as a left A-module and a left B-module such that the two module structures are compatible. This gives $M \stackrel{\text{def}}{=} \mathrm{Hom}_B(Q, R)$ the structure of a left A-module (c.f. Remark 1.47). Consider the map $\varphi : M \otimes_K Q \to R$ defined by evaluation, i.e. $\mu \otimes q \mapsto \varphi(\mu \otimes q) \stackrel{\text{def}}{=} \mu(q)$. This is a morphism of $(A \otimes_K B)$-modules since for $a \in A, b \in B, \mu \in \mathrm{Hom}_B(Q, R) = M$ and $q \in Q$, we have

$$\varphi((a \otimes b)(\mu \otimes q)) = \varphi(a\mu \otimes bq) = a\mu(bq) = a(b\mu(q)) = (a \otimes b)\varphi(\mu \otimes q).$$

The left A-module $\mathrm{Hom}_B(Q, R)$ is finite-dimensional over K (because Q and R are), so it is left-artinian ; let P be a simple left A-submodule of $\mathrm{Hom}_B(Q, R)$. We have a canonical inclusion of $(A \otimes_K B)$-submodules $P \otimes_K Q \subseteq \mathrm{Hom}_B(Q, R) \otimes_K Q$ (tensor up with Q over K), and the restriction of φ to $P \otimes_K Q$ is not identically zero (for any $\varphi \in \mathrm{Hom}_B(Q, R) \setminus \{0\}$, there exists at least one

$q \in Q$ such that $\varphi(q) \neq 0$). This implies that $\varphi|_{P \otimes_K Q}$ is surjective by simplicity of R, which means that φ induces an isomorphism $P \otimes_K Q/S \simeq R$ where $S \leq P \otimes_K Q$ is an $(A \otimes_K B)$-submodule of $P \otimes_K Q$.

Because Q is a K-vector space, the left A-module $P \otimes_K Q$ is isotypically simple of type P ; symetrically, it is an isotypically simple left B-module of type Q. It follows by the $(A \otimes_K B)$-linearity of φ that the same is true for R, i.e. it is an isotypically simple A-module of type P and an isotypically simple B-module of type Q). It follows that $[P]$ and $[Q]$ are the unique isomorphism classes with the property that a quotient map $P \otimes_K Q \to R$ exists.

Corollary 5.39. Let K be an algebraically closed field, A, B be two K-algebras and write $\mathscr{C}(A)$ for the set of all simple left A-modules which are finite-dimensional over K. The map

$$\Phi : \mathscr{C}(A) \times \mathscr{C}(B) \to \mathscr{C}(A \otimes_K B), \quad (P, Q) \mapsto P \otimes_K Q$$

is a well-defined map (i.e. the tensor product of two simple modules becomes simple) which is a bijection.

Proof. By Corollary 5.19, it suffices to show that if $[P] \in \mathscr{C}(A)$, then $C_A(P) \simeq K$ as K-algebras. This is clear by Lemma 2.66.