Chapter 6

Approximating the Jacobson radical of a finite ring

When trying to answer questions about left-artinian rings and modules over them, it is often convenient to reduce the problem at hand to the semisimple case, where structures are much more manageable, and then "lift". However, this approach requires the computation of the Jacobson radical of the ring, which we cannot efficiently carry out in general. But how "close" can we get to semisimplicity with a deterministic polynomial-time algorithm in the case of finite rings?

In this chapter, we give two deterministic polynomial-time algorithms that, given a finite ring A, produce two-sided nilpotent ideals $\mathfrak{j}_A$, such that $A/\mathfrak{j}_A$ is "almost semisimple". We think of such ideals $\mathfrak{j}_A$ as approximations to the Jacobson radical.

6.1 Introduction

When considering the module isomorphism problem for finite rings, not being able to compute Jacobson radicals was the main obstacle in the way of generalising methods that had worked in the case of finite-dimensional algebras over finite fields (cf. [15]). The side-exit algorithm of Theorem 4.1.3 was designed to construct an approximation of the Jacobson radical which was good enough for the purpose at hand, namely determining the minimum number of generators of a module. Motivated by this, we design deterministic polynomial-time algorithms that compute good working approximations of the Jacobson radical of a finite ring, that is, two-sided nilpotent ideals such that when we quotient the ring by them, we are left with something that is "almost" semisimple.

The notion we will use to approximate semisimplicity is that of separability. Given a commutative ring R, an R-algebra S is said to be *separable* over R if S is projective as an $S \otimes_R S^{\mathrm{o}}$-module, where S^{o} denotes the opposite ring of S. A ring is said to be separable if it is separable as a $\mathbb{Z}$-algebra. Section 6.2 explores the structure and properties of separable algebras and attempts to make an argument for why they

are a good "approximation" to semisimple algebras. Section 6.2.6 gives a complete classification of finite rings that are separable over $\mathbb{Z}$, as finite products of matrix rings over certain commutative rings.

It turns out that finite separable rings are automatically projective over a certain subring, which we will refer to as the *generalised prime subring* (see Section 6.2.5). With this in mind, we make the following definition.

Definition 6.1.1. *Let A be a finite ring. We say an ideal $\mathfrak{j}_A \subset A$ is an* approximation of the Jacobson radical of A *if it satisfies the following conditions:*

(A1) *$\mathfrak{j}_A$ is a nilpotent two-sided ideal of A,*
(A2) *$A/\mathfrak{j}_A$ is separable,*
(A3) *The prime subring and generalised prime subring of $A/\mathfrak{j}_A$ coincide.*

If $\mathfrak{j}_A$ is an approximation of the Jacobson radical of A, then the ring $A/\mathfrak{j}_A$ has many of the good properties that semisimple rings have: it has "many" projective and injective modules, it is quasi-Frobenius, it is a symmetric algebra over its prime subring and it is isomorphic to a product of matrix rings over commutative local rings. However, as opposed to semisimplicity, which can be neither tested nor enforced (see Note 3.4.2), separability is a much friendlier notion in algorithmic contexts. In Sections 6.3 and 6.4, we prove the following results.

Theorem 6.1.2. *There exists a deterministic polynomial-time algorithm that, given a finite ring A, computes an approximation of the Jacobson radical of A.*

We prove Theorem 6.1.2 by exhibiting two algorithms that produce approximations of Jacobson radicals of finite rings.

Proposition 6.1.3. *Let $\mathcal{F}$ be the class of finite rings. The two families of ideals $(\mathfrak{j}_A)_{A\in\mathcal{F}}$ and $(\mathfrak{j}'_A)_{A\in\mathcal{F}}$, produced by the two algorithms described in the proof of Theorem 6.1.2 are functorial under isomorphisms, i.e. if $\phi : A \to B$ is an isomorphism of finite rings, then $\phi(\mathfrak{j}_A) = \mathfrak{j}_B$ and $\phi(\mathfrak{j}'_A) = \mathfrak{j}'_B$.*

Theorem 6.1.4. *There exists a deterministic polynomial-time algorithm that, given a finite ring A, computes the generalised prime subring of A.*

In Section 6.3.6, we look at some basic examples of the running of these algorithms.

6.2 Separability

6.2.1 Separable algebras

We begin with a study of separable algebras and some of their basic properties. We argue that the notion of separability is a good starting point in our quest to approximate semisimplicity. The main references for this section are [20, 54].

Definition 6.2.1. *Let R be a commutative ring and S an R-algebra. We say S is* separable *over R if S is projective as a module over $S^{\mathrm{e}} := S \otimes_R S^{\mathrm{o}}$, where S^{o} denotes the opposite ring of S and the module structure is given by $(s \otimes s')t = sts'$, for $s, s', t \in S$.*

Note 6.2.2. For any R-algebra S, the ring S^{e} is called the *enveloping algebra* of S, which justifies the choice of notation. A left S^{e}-module is the same as an S-S-bimodule whose induced R-structures coincide.

Let $\phi : S^{\mathrm{e}} \to S$ be the S^{e}-module homomorphism given by $a \otimes a' \mapsto aa'$. Note that $\ker(\phi)$ is then generated as an S^{e}-module by elements of the form $s \otimes 1 - 1 \otimes s$.

Theorem 6.2.3 ([20], Chapter II, Proposition 1.1)**.** *Let R be a commutative ring and S an R-algebra. Then the following are equivalent:*

(i) *S is separable over R.*
(ii) *The exact sequence of S^{e}-modules $0 \to \ker(\phi) \to S^{\mathrm{e}} \xrightarrow{\phi} S \to 0$ splits.*
(iii) *There exists an element $e \in S^{\mathrm{e}}$ such that $\phi(e) = 1$ and $\forall s \in S$, $(s \otimes 1)e = (1 \otimes s)e$.*

Note 6.2.4. The element e in (iii) is necessarily an idempotent, since $e^2 - e = (e - (1 \otimes 1))e \in \ker(\phi)e = 0$, and it is referred to as a *separability idempotent*. It arises as the image of $1 \in S$ under a splitting of ϕ and is in general not unique.

Note 6.2.5.

(i) Let $\tau : S^{\mathrm{e}} \to (S^{\mathrm{o}})^{\mathrm{e}}$ be the map given by $x \otimes y \mapsto y \otimes x$. Then τ is a ring isomorphism. For this, note that for all $x_1, x_1, y_1, y_2 \in S$:

$$\tau((x_1 \otimes y_1)(x_2 \otimes y_2)) = \tau(x_1x_2 \otimes y_2y_1) = y_2y_1 \otimes x_1x_2$$

and

$$\tau(x_1 \otimes y_1)\tau(x_2 \otimes y_2) = (y_1 \otimes x_1)(y_2 \otimes x_2) = y_2y_1 \otimes x_1x_2.$$

(ii) The map $\tau' : S^{\mathrm{e}} \to S^{\mathrm{e}}$ given by $x \otimes y \mapsto y \otimes x$ is an involutive ring anti-automorphism, since $(\tau')^2 = \mathrm{id}$ and $\tau'((x_1 \otimes y_1)(x_2 \otimes y_2)) = y_2y_1 \otimes x_1x_2 = (y_2 \otimes x_2)(y_1 \otimes x_1) = \tau'(x_2 \otimes y_2)\tau'(x_1 \otimes y_1)$. A separability idempotent that satisfies $\tau'(e) = e$ is called a *symmetric separability idempotent*.

Proposition 6.2.6. *Let R be a commutative ring and S be a separable R-algebra. Then S^{o} is a separable R-algebra.*

Proof. Let $S^{\mathrm{e}} = S \otimes_R S^{\mathrm{o}}$ and $(S^{\mathrm{o}})^{\mathrm{e}} = S^{\mathrm{o}} \otimes_R S$. Consider the two exact sequences

$$\begin{array}{ccccccccc} 0 & \longrightarrow & S^{\mathrm{e}} & \underset{\phi}{\overset{\sigma}{\leftrightarrows}} & S & \longrightarrow & 0 \\ & & \tau\downarrow & & \downarrow\mathrm{id} & & \\ 0 & \longrightarrow & (S^{\mathrm{o}})^{\mathrm{e}} & \xrightarrow{\psi} & S^{\mathrm{o}} & \longrightarrow & 0, \end{array}$$

where $\phi : S^{\mathrm{e}} \to S$ is given by $\phi(s \otimes s') = ss'$, $\psi : (S^{\mathrm{o}})^{\mathrm{e}} \to S^{\mathrm{o}}$ is given by $\psi(s' \otimes s) = ss'$ and τ is the ring isomorphism described in Note 6.2.5. Let σ be a splitting of ϕ, which exists since S is a separable algebra over R. It is easy to see that the above diagram commutes and since σ is S^{e}-linear, $\tau \circ \sigma$ is $(S^{\mathrm{o}})^{\mathrm{e}}$-linear. Hence $\tau \circ \sigma$ gives a splitting of ψ, showing that S^{o} is separable over R. □

Note 6.2.7. If e is a separability idempotent of S over R, then $\tau(e)$ is a separability idempotent of S^{o} over R.

The following proposition describes separability over fields.

Theorem 6.2.8.

(i) ([54], Chapter III, Proposition 3.4). *Let $R \subset S$ be a finite field extension. Then S is separable over R if and only if for all $s \in S$, the minimal polynomial of s over R has distinct roots in a splitting field over R.*

(ii) ([20], Chapter II, Theorem 2.5). *Let R be a field and S an R-algebra. Then S is separable over R if and only if S is finite-dimensional over R and for every field extension $R \subset K$, we have that $S \otimes_R K$ is semisimple.*

(iii) ([54], Chapter III, Theorem 3.1). *Let R be a field and S an R-algebra. Then S is separable over R if and only if S is isomorphic to an algebra of the form $\prod_{i=1}^{n} \mathcal{M}_{n_i}(D_i)$, for some $n \in \mathbb{Z}_{\geq 0}$ and $n_i \in \mathbb{Z}_{>0}$, with D_i finite-dimensional division algebras over R and $\mathrm{Z}(D_i) \supset R$ finite-dimensional separable field extensions.*

Corollary 6.2.9. *A separable algebra over a field is semisimple.*

Proof. Put $K = R$ in Proposition 6.2.8, part (ii). □

Since finite extensions of perfect fields are separable, semisimplicity and separability are equivalent notions for finite-dimensional algebras over perfect fields.

Corollary 6.2.10. *Let R be a perfect field and S a finite-dimensional R-algebra. Then S is a separable R-algebra if and only if S is semisimple.*

Example 6.2.11. Let R be a commutative ring and let $n \in \mathbb{Z}_{\geq 0}$. Then the matrix ring $\mathcal{M}_n(R)$ is a separable R-algebra. To see this, let E_{ij} denote the matrix with $(i,j)^{\text{th}}$ entry equal to 1 and all other entries equal to 0. Then for any fixed i, the element $e_i = \sum_{j=1}^{n} E_{ij} \otimes E_{ji}$ is a separability idempotent.

Example 6.2.12. Let R be a commutative ring and let G be a finite group such that $|G|$ is a unit in R. Then the group algebra $R[G]$ is a separable R-algebra. To see that, note that $e := |G|^{-1} \sum_{g \in G} g \otimes g^{-1}$ is a separability idempotent.

Parts (i) and (ii) of Proposition 6.2.8 establish that the definition of separability is compatible with the classical definitions of separability in the cases of finite field extensions and finite-dimensional algebras over a field. The reason the extra finiteness condition is required is that separable algebras, as we have defined them, turn out to have a lot of structure, as shown in the following series of results.

Proposition 6.2.13 ([20], Chapter II, Proposition 2.1)**.** *Let R be a commutative ring and S a separable R-algebra. Suppose that S is projective as an R-module. Then S is finitely generated as an R-module.*

Proposition 6.2.14 ([20], Chapter II, Proposition 1.12, Theorem 3.8)**.** *Let R be a commutative ring.*

(i) *Let A be a separable commutative algebra over R. Suppose S is a separable A-algebra. Then S is an R-algebra and it is separable over R.*
(ii) *Let S be a separable R-algebra and A be any R-subalgebra of the centre of S. Then S is separable over A.*
(iii) *Suppose S is an R-algebra. Then S is separable over R if and only if S is separable over its centre, and its centre is separable over R.*

Proposition 6.2.15 ([54], Chapter III, Theorem 5.1)**.** *Let S be a ring. If S is separable over its centre, then S is projective as a module over its centre.*

Proposition 6.2.16 ([54], Chapter III, Proposition 1.7)**.**

(i) *Let R be a commutative ring and R_1, R_2 be two commutative R-algebras. Let S_1 be a separable R_1-algebra and S_2 a separable R_2-algebra. Then $S_1 \otimes_R S_2$ is a separable $R_1 \otimes_R R_2$-algebra, with $(r_1 \otimes r_2)(s_1 \otimes s_2) = r_1 s_1 \otimes r_2 s_2$. Moreover, $\mathrm{Z}(S_1 \otimes S_2) = \mathrm{Z}(S_1) \otimes \mathrm{Z}(S_2)$.*
(ii) *Let R_1, R_2 be two commutative rings. Let S_1 be an R_1-algebra and S_2 an R_2-algebra. Then $S_1 \times S_2$ is separable over $R_1 \times R_2$ if and only if S_1 is separable over R_1 and S_2 is separable over R_2.*
(iii) *Let R be a commutative ring and S_1, S_2 two R-algebras. Then $S_1 \times S_2$ is separable over R if and only if both S_1 and S_2 are separable over R.*

Corollary 6.2.17. *Let R be a commutative ring, R' a commutative R-algebra and S a separable R-algebra. Then $S \otimes_R R'$ is separable over over R'.*

Proof. In Proposition 6.2.16, part (i), take $R_1 := R$, $R_2 := R'$, $S_1 := S$ and $S_2 := R'$. □

Theorem 6.2.18 ([20], Chapter II, Theorem 7.1)**.** *Let R be a commutative ring and S an R-algebra that is finitely generated as an R-module. Then the following are equivalent:*

(i) *S is separable over R.*
(ii) *For every maximal ideal $\mathfrak{m}$ of R, we have that $S \otimes_R R_{\mathfrak{m}}$ is separable over $R_{\mathfrak{m}}$.*
(iii) *For every maximal ideal $\mathfrak{m}$ of R, the quotient $S/\mathfrak{m}S$ is separable over $R/\mathfrak{m}$.*

Separability is testable deterministically in polynomial time (cf. Note 3.4.2).

Theorem 6.2.19. *There exists a deterministic polynomial-time algorithm that, given a finite commutative ring R and a finite R-algebra S, decides whether or not S is separable over R.*

Proof. Using Proposition 2.4.1, we compute the enveloping algebra $S^{\mathrm{e}} = S \otimes_R S^{\mathrm{o}}$, after which we test projectivity of S over S^{e} using Theorem 5.4.1. □

6.2.2 Azumaya and finite-étale algebras

There are two distinguished classes of separable algebras that deserve special attention: Azumaya and finite-étale algebras.

Recall the definition of a progenerator (Definition 1.8.6).

Theorem 6.2.20 ([54], Chapter III, Theorem 6.1, [20], Chapter II, Theorem 3.4)**.** *Let R be a commutative ring and S an R-algebra. Then the following are equivalent.*

(i) *S is separable over R and $\mathrm{Z}(S) = R$.*
(ii) *S is an R-progenerator and the map $\alpha : S^{\mathrm{e}} \to \mathrm{End}_R(S)$, given by $s \otimes s' \mapsto (f : t \mapsto sts')$, is an isomorphism of R-algebras.*
(iii) *S is an S^{e}-progenerator and $\mathrm{Z}(S) = R$.*
(iv) *There exist an R-algebra T and an R-progenerator P such that $S \otimes_R T \cong \mathrm{End}_R(P)$ as R-algebras.*

Definition 6.2.21. *An R-algebra S satisfying the conditions of Theorem 6.2.20 is called an* Azumaya algebra *over R.*

Note 6.2.22. From Theorem 6.2.20, part (ii), it is easy to see that if S is Azumaya over R, then S^{o} is also Azumaya over R. This gives another, more conceptual way of showing that separability is stable under taking opposites. Suppose S is separable as an algebra over a commutative ring R. Then S is Azumaya over $\mathrm{Z}(S)$ and $\mathrm{Z}(S)$ is separable over R. Now $R^{\mathrm{o}} = R$ and $\mathrm{Z}(S) = \mathrm{Z}(S^{\mathrm{o}})$. So $\mathrm{Z}(S^{\mathrm{o}})$ is separable over R^{o} and S^{o} is Azumaya over $\mathrm{Z}(S^{\mathrm{o}})$. Hence S^{o} is separable over R, by Theorem 6.2.14, part (iii).

Example 6.2.23 ([26], §8)**.** Over a field, an algebra is Azumaya if and only if it is central simple.

Example 6.2.24 ([20], Chapter II, Proposition 4.1)**.** Let R be a commutative ring. Then the endomorphism ring of any R-progenerator is Azumaya over R.

Proposition 6.2.25 ([80], Proposition 3.9)**.** *Let R be a commutative ring and A an R-algebra that is Azumaya of constant rank over R. Then there exists a faithfully flat ring extension S of R, and $n \in \mathbb{Z}_{>0}$ such that $A \otimes_R S \cong \mathcal{M}_n(S)$.*

Corollary 6.2.26. *Let R be a commutative ring and A an Azumaya R-algebra. Then the rank of A over R, as a function on $\mathrm{Spec}(R)$, is a square.*

Proof. This follows from Proposition 6.2.25 and the fact that extension of scalars does not change the rank.

□

In the commutative setting, the notion we are interested in is that of a *finite-étale* algebra.

Definition 6.2.27. *Let R be a commutative ring. An R-algebra S is* finite-étale *over R if S is commutative, separable as an R-algebra and projective as an R-module.*

We state a couple of results describing the behaviour of finite-étale algebras and Azumaya algebras with respect to tensor products and direct products. These are consequences of Proposition 6.2.16.

Proposition 6.2.28. *Let R be a commutative ring and let R_1, R_2 be two commutative R-algebras.*

(i) *Let S_1 be an Azumaya R_1-algebra and S_2 an Azumaya R_2-algebra. Then $S_1 \otimes_R S_2$ is Azumaya over $R_1 \otimes_R R_2$.*
(ii) *Let S_1 be a finite-étale R_1-algebra and S_2 a finite-étale R_2-algebra. Then $S_1 \otimes_R S_2$ is finite-étale over $R_1 \otimes_R R_2$.*

Corollary 6.2.29. *Let R be a commutative ring and R' a commutative R-algebra.*

(i) *Let S be an Azumaya R-algebra. Then $S \otimes_R R'$ is Azumaya over R'.*
(ii) *Let S be a finite-étale R-algebra. Then $S \otimes_R R'$ is finite-étale over R'.*

Proposition 6.2.30. *Let R_1, R_2 be two commutative rings. Let S_1 be an R_1-algebra and S_2 an R_2-algebra. Then*

(i) *$S_1 \times S_2$ is Azumaya over $R_1 \times R_2$ if and only if S_1 is Azumaya over R_1 and S_2 is Azumaya over R_2.*
(ii) *$S_1 \times S_2$ is finite étale over $R_1 \times R_2$ if and only if S_1 is finite-étale over R_1 and S_2 is finite-étale over R_2.*

Moreover, if $R := R_1 = R_2$, then $S_1 \times S_2$ is finite étale over R if and only if S_1 and S_2 are both finite-étale over R.

Note 6.2.31. If $R := R_1 = R_2 \neq 0$ and S_1, S_2 are Azumaya R-algebras, then $S_1 \times S_2$ is not Azumaya over R.

6.2.3 The Brauer group

For a commutative ring R, we can define an equivalence relation on the collection of Azumaya R-algebras such that the equivalence classes form an abelian group with binary operation given by taking tensor products over R.

Definition 6.2.32. *Let R be a commutative ring. Let $\mathcal{B}(R)$ be a collection of Azumaya R-algebras such that every Azumaya R-algebra is isomorphic to exactly one element of $\mathcal{B}(R)$. Let*

$$\mathcal{B}^{\mathrm{o}}(R) = \{A \in \mathcal{B} \mid A \cong \mathrm{End}_R(P) \text{ as } R\text{-algebras, for some } R\text{-progenerator } P\}.$$

Define an equivalence relation $\sim$ on $\mathcal{B}(R)$ by:

$$A \sim B \iff \text{there exist } Y, Z \in \mathcal{B}^{\mathrm{o}}(R) \text{ such that } A \otimes_R Y \cong B \otimes_R Z \text{ as } R\text{-algebras.}$$

Denote by $[A]$ the equivalence class of $A \in \mathcal{B}(R)$ under $\sim$. The set of all such equivalence classes, denoted by $\mathrm{Br}(R)$, together with binary operation given by $[A] \cdot [B] = [A \otimes_R B]$ is an abelian group called the Brauer group *of R. The identity is given by $[R]$ and inverses are given by $[A]^{-1} = [A^{\mathrm{o}}]$.*

Note 6.2.33. Since all Azumaya R-algebras are finitely generated projective as R-modules, $\mathcal{B}(R)$ is indeed a set. It is also easy to check that $\sim$ is an equivalence relation and that $\mathrm{Br}(R)$ is an abelian group.

Example 6.2.34. (Brauer groups)

1. If k is a finite field, $\mathrm{Br}(k)$ is trivial (see [82], Chapter X, §7).
2. $\mathrm{Br}(\mathbb{Z})$ is trivial (see [26], page 196).
3. If k is a finite commutative ring, then $\mathrm{Br}(k)$ is trivial (see [87], Proposition 4.1).

For more on Brauer groups, see [20], Chapter III, Section 5.

6.2.4 Separable projective algebras

It is often convenient to look at algebras that are both finitely generated projective as modules and separable as algebras over the underlying commutative ring.

Definition 6.2.35. *Let R be a commutative ring. An R-algebra S that is separable as an R-algebra and projective as an R-module is said to be* separable projective *over R.*

This notion can be linked to the notions of Azumaya and finite-étale.

Theorem 6.2.36. *Let k be a commutative ring and S a k-algebra. Let $R := \mathrm{Z}(S)$. Then the following are equivalent:*

(i) *S is Azumaya over R and R is finite-étale over k.*
(ii) *S is separable projective over k.*

Proof. (i)⇒(ii) By Theorem 6.2.20, part (i), Definition 6.2.27 and Proposition 6.2.14, part (iii), we have that S is separable as a k-algebra. From Corollary 6.2.15 we know that S is projective as an R-module and so by transitivity of projectivity, S is projective as a k-module.

(ii)⇒(i) By Proposition 6.2.14, part (ii), we have that S is separable over R so it is Azumaya over R, and R is separable over k. All that remains to be established is that R is projective as a k-module.

From Theorem 6.2.20 we know that S is an R-progenerator, so

$$R = \sum_{f \in \mathrm{Hom}_R(S,R)} f(S).$$

Since S is finitely generated and projective as an R-module, $\mathrm{Hom}_R(S, R)$ is finitely generated as an R-module, so we can restrict the sum to a finite set of generators. In particular, there exists a surjective R-homomorphism $S^n \twoheadrightarrow R$ for some $n \in \mathbb{Z}_{>0}$. But R is R-projective, so this map splits, giving $S^n \cong R \oplus Q$ for some R-module Q. Now S is k-projective by hypothesis, so S^n is also k-projective and since R is a direct summand of S^n, we have that R is also k-projective.

□

Over a semisimple ring, every module is projective. The following proposition says that a separable projective algebra over a commutative ring has "many" projective modules.

Theorem 6.2.37 ([31], Proposition 2.3)**.** *Let R be a commutative ring, S a separable R-algebra and M a finitely generated S-module. Then any exact sequence of S-modules $0 \to M_1 \to M_2 \to M \to 0$ that splits over R, splits over S.*

Proposition 6.2.38. *Let R be a commutative ring and S a separable R-algebra that is projective as an R-module. Let M be an S-module. Then*

$$M \text{ is projective as an } S\text{-module} \iff M \text{ is projective as an } R\text{-module.} \tag{6.1}$$

Proof. ($\Rightarrow$) This direction is easy and follows by transitivity of projectivity: M is S-projective and S is R-projective, so M is R-projective.

($\Leftarrow$) This direction follows from Theorem 6.2.37, Proposition 5.6.1 and Note 5.6.2. □

Note 6.2.39. The "if" direction of (6.1) is a strong statement and only requires S to be separable over R. We will refer to this property as "projectivity lift". Another proof of this fact is also given in [20], Chapter II, Proposition 2.3, which uses the existence and properties of the separability idempotent. We sketch it here. Suppose M is an R-projective S-module. Let $f : N \to M$ be an S-module epimorphism. Since M is R-projective, there exists R-homomorphism $g : M \to N$ such that $fg = \mathrm{id}_M$. Note that $\mathrm{Hom}_R(M, N)$ is an S^{e}-module via $(a \otimes b) \cdot \phi(m) = a\phi(bm)$. Suppose e is a separability idempotent for S. Then $e \cdot g$ is an S-module homomorphism and $f(e \cdot g) = \mathrm{id}_M$. Hence M is S-projective.

Proposition 6.2.40. *Let R be a commutative ring and S a separable R-algebra that is projective as an R-module. Let M be an S-module. Then*

$$M \text{ is injective as an } S\text{-module} \iff M \text{ is injective as an } R\text{-module.} \tag{6.2}$$

Proof. ($\Rightarrow$) Recall from Proposition 1.6.20 that $\mathrm{Hom}_S({}_SS_R, {}_SM_R) \cong {}_RM_R$, so it is enough to show that $\mathrm{Hom}_S(S, M)$ is injective as an R-module. By tensor-hom adjunction (see Section 1.6.6), we have

$$\mathrm{Hom}_R(-, \mathrm{Hom}_S(S, M)) \cong \mathrm{Hom}_S(S \otimes_R -, M).$$

Since S is projective over R, the functor $S \otimes_R -$ is exact, and since M is injective over S, the functor $\mathrm{Hom}_S(-, M)$ is exact. Hence $\mathrm{Hom}_R(-, \mathrm{Hom}_S(S, M))$ is exact, i.e. $\mathrm{Hom}_S(S, M)$ is an injective R-module.

($\Leftarrow$) Consider an exact sequence of S-modules $0 \to I \to M \to C \to 0$, where M is an S-module and C is a cyclic S-module. Since I is R-injective the sequence is R-split, so because C is cyclic over S, the sequence is S-split by Theorem 6.2.37. The result now follows from Theorem 1.6.12, part (iv), which states that I is an injective S-module if and only if every short exact sequence $0 \to I \to M \to C \to 0$, where M is an S-module and C is a cyclic S-module, is S-split. □

Note 6.2.41. We will refer to the property induced by the "if" direction as "injectivity lift".

Corollary 6.2.42. *Let S be a finite ring that is separable projective over its prime subring. Then S is a quasi-Frobenius ring.*

Proof. Since S is finite, its prime subring is isomorphic to $R = \mathbb{Z}/n\mathbb{Z}$, where $n = \mathrm{char}(S) \in \mathbb{Z}_{>0}$. Since R is quasi-Frobenius (see Example 1.7.3), an R-module is injective if and only if it is projective. Since S admits both projectivity and injectivity lift from R by Propositions 6.2.38 and 6.2.40, it follows that S itself is quasi-Frobenius. □

We record some other properties of separable projective algebras.

Proposition 6.2.43. *Let A be a finite semisimple ring. Then A is separable projective over its prime subring.*

Proof. Since A is semisimple, the characteristic of A is squarefree. By Proposition 6.2.16, part (ii), Proposition 1.6.9 and the fact that A is semisimple, we may assume that A has prime subring $\mathbb{F}_p$, for some prime p, and that $A \cong \mathcal{M}_n(D)$, for some $n \in \mathbb{Z}_{>0}$, where D is a finite field extension of $\mathbb{F}_p$. Now A is separable projective over D by Example 6.2.23 and D is separable projective over $\mathbb{F}_p$, since finite extensions of perfect fields are separable. Hence A is separable projective over $\mathbb{F}_p$. □

Theorem 6.2.44. *Let A be a nonzero finite ring. Then A is semisimple if and only if A is separable projective over its prime subring and* $\mathrm{char}(A)$ *is squarefree.*

Proof. Let $n := \mathrm{char}(A)$. The "if" direction follows from Proposition 6.2.43 and the fact that for any $d \in \mathbb{Z}_{>0}$ such that $d^2 \mid n$, we have $0 \neq \frac{n}{d}A \subseteq \mathrm{J}(A)$. The other direction follows from Theorem 6.2.18, part (iii) and Proposition 6.2.16, part (ii). □

Moreover, separable projective algebras that are faithful as modules over the base ring, are symmetric (see Definition 1.8.1 and Theorem 1.8.2).

Theorem 6.2.45 ([24], Theorem 4.2)**.** *Let k be a commutative ring and A a separable projective k-algebra that is faithful as a module over k. Then A is a symmetric k-algebra.*

6.2.5 Separable rings

Let A be a ring. Then A is a $\mathbb{Z}$-algebra, as well as an algebra over its prime subring. By Proposition 6.2.14, parts (i) and (ii), we have that A is separable over $\mathbb{Z}$ if and only if A is separable over its prime subring.

Definition 6.2.46. *We say a ring is* separable *if it is separable as a $\mathbb{Z}$-algebra.*

Theorem 6.2.47. *There exists a deterministic polynomial-time algorithm that, given a finite ring A, decides whether or not it is separable.*

Proof. We begin by computing the prime subring of A using Theorem 3.3.1, and then use Theorem 5.4.1 to test separability over the prime subring. □

Suppose A_1, A_2 are two finite rings that are separable projective over their prime subrings. Then it is not necessarily true that $A_1 \times A_2$ will also be separable projective over its prime subring. However, the class of separable rings is closed under taking products by Proposition 6.2.16, part (iii). Being closed under taking products is also an important property of the class of semisimple rings. For a finite ring A, we would like to identify a subring $S \subset A$ such that A is separable over $\mathbb{Z}$ if and only if A is separable projective over S. That is the aim of this section.

Let A be a finite ring. Then A has a unique block decomposition, $A = \prod_{i \in I} A_i$, where I is the set of centrally primitive idempotents of A and each A_i is connected (see Definition 1.5.3, Theorem 1.5.5), and hence has prime power characteristic (see Theorem 1.5.5). We group together the A_i according to their characteristics to get

$$A = \prod_{i \in I} A_i = \prod_{\substack{p \text{ prime} \\ e \in \mathbb{Z}_{>0}}} \left(\prod_{\substack{i \\ \mathrm{char}(A_i) = p^e}} A_i \right). \tag{6.3}$$

Let

$$B_{p,e} := \prod_{\substack{i \\ \mathrm{char}(A_i) = p^e}} A_i.$$

Definition 6.2.48. *Let A be a finite ring. We define the* generalised prime subring *of A, denoted by $\mathcal{P}_A$, to be the product of the prime subrings of $B_{p,e}$.*

Proposition 6.2.49. *Let A be a finite ring and let k be its prime subring. Then $\mathcal{P}_A$ is separable as a k-algebra.*

Proof. The ring $\mathcal{P}_A$ is a product of rings, each of which is separable over k by Proposition 6.2.16, part (ii). The result now follows from Proposition 6.2.16, part (iii). □

Lemma 6.2.50. *Let A be a finite ring. Then $\mathcal{P}_A = \mathcal{P}_{\mathrm{Z}(A)}$.*

Proof. This follows since a block decomposition of A induces a block decomposition of $\mathrm{Z}(A)$ (see Theorem 1.5.6), together with the fact that any ring has the same prime subring as its centre. □

Proposition 6.2.51. *Let A be a finite separable ring. Then A is projective as a module over $\mathcal{P}_A$.*

Proof. By Proposition 6.2.16 we may assume that A is connected. Further, by Proposition 6.2.13 and Proposition 6.2.14, part (iii), we may assume that A is commutative. Hence A is local. Suppose A has prime subring $\mathbb{Z}/p^n\mathbb{Z}$, for some prime p and some $n \in \mathbb{Z}_{>0}$. Then A/pA is a separable $\mathbb{F}_p$-algebra. By Corollary 6.2.9, we have that A/pA is semisimple, so it must be a finite field extension of $\mathbb{F}_p$. Suppose the degree of this extension is d. We are left with showing that $A^+ \cong (\mathbb{Z}/p^n\mathbb{Z})^d$.

Consider the map $A \to p^{n-1}A$, given by $f : a \mapsto p^{n-1}a$. This map is surjective. Moreover, $pA \subseteq \ker(f)$. Since A/pA is a field, pA is a maximal ideal of A, so it must be the case that $pA = \ker(f)$. Hence $|A/pA| = |p^{n-1}A| = p^d$.

Since $A/pA \cong \mathbb{F}_p^d$ as $\mathbb{F}_p$-vector spaces, we may choose a basis $\{a_1, \ldots, a_d\} \subset A$ of A/pA over $\mathbb{F}_p$. Since $p^n A = 0$, it follows that $\{a_1, \ldots, a_d\}$ generate A over $\mathbb{Z}/p^n\mathbb{Z}$. Then the map $(\mathbb{Z}/p^n\mathbb{Z})^d \twoheadrightarrow A$, given by sending the generator of the i^{th} copy of $\mathbb{Z}/p^n\mathbb{Z}$ to a_i, is surjective. To see that it is also injective it is enough to show that the cardinalities agree. Consider the chain of ideals $A \supset pA \supset \ldots \supset p^{n-1}A \supset \{0\}$. Since $|p^i A/p^{i+1}A| = p^d$, for all $0 \leq i \leq n-1$, we have that $|A| = p^{nd}$. Hence $(\mathbb{Z}/p^n\mathbb{Z})^d \cong A$. □

Theorem 6.2.52. *Let A be a finite ring. Then A is separable if and only if A is separable projective over $\mathcal{P}_A$.*

Proof. Let k be the prime subring of A. The "only if" direction follows from Proposition 6.2.49 and the fact that A is separable over $\mathbb{Z}$ if and only if it is separable over k. The "if" direction follows from Proposition 6.2.14, parts (i), (ii) and Proposition 6.2.51. □

Note 6.2.53. If A is separable, but not finite, it is not necessarily projective over any proper subring. To see this, consider the $\mathbb{Z}$-algebra $\mathbb{Q}$. Then $\mathbb{Q}$ is certainly separable over $\mathbb{Z}$, since $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q} \cong \mathbb{Q}$, but it cannot be projective over any proper subring, since then it would have to be finitely generated over it (see Proposition 6.2.13).

Suppose $R \subseteq \mathbb{Q}$ is a subring such that $\mathbb{Q}$ is finitely generated as a module over R. Then $\mathbb{Q}$ is integral over R, i.e. for every $q \in \mathbb{Q}$, there exists a monic polynomial $f \in R[X]$ such that $f(q) = 0$. But then it is easy to see that $\mathbb{Q}^* \cap R = R^*$, where R^* denotes the unit group of R. Hence $R^* = R \backslash \{0\}$, so R is a field and then it must be the case that $R = \mathbb{Q}$.

6.2.6 Classification of finite separable rings

For finite-dimensional semisimple algebras over a field and separable algebras over a field, we have explicit descriptions in terms of matrix rings over certain division rings (see Theorem 1.4.5 and Theorem 6.2.8, part (iii), respectively). The aim of this section is to provide a similar classification result for finite separable rings. It turns out that finite separable rings are isomorphic to products of finitely many matrix algebras over certain special commutative rings, called *Witt rings*.

Recall that a ring C is said to be *connected* (or *indecomposable*) if C has exactly two central idempotents, namely 0 and 1. Note that a connected ring is nonzero.

Here, we develop the theory concerning Witt rings that we require. We restrict our attention to *truncated Witt rings over finite fields*, as this is a sufficient level of generality for our purposes. For more on Witt rings, see Chapter II: §6 of [82] or Chapter VI: Exercises 46-51 of [60].

Let p be a prime and $e \in \mathbb{Z}_{>0}$. Let

$$\underline{\mathbf{C}} = \text{category of finite local commutative } \mathbb{Z}/p^e\mathbb{Z}\text{-algebras},$$
$$\underline{\mathbf{D}} = \text{category of finite fields of characteristic } p,$$

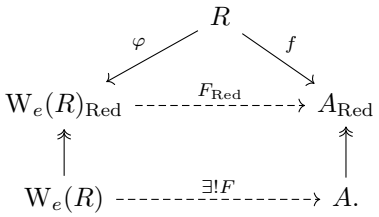
and consider the covariant functor

$$\begin{aligned} \mathrm{Red} : \underline{\mathbf{C}} &\longrightarrow \underline{\mathbf{D}} \\ A &\longmapsto A_{\mathrm{Red}} := A/\sqrt{0_A}, \end{aligned} \tag{6.4}$$

where $\sqrt{0_A}$ denotes the nilradical of A (which equals the maximal ideal of A).

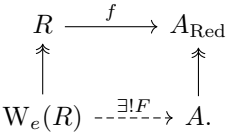
Theorem 6.2.54. *The functor* Red *has a left adjoint.*

Proof. We will show that if $R \in \underline{\mathbf{D}}$, then there exists a pair $(\mathrm{W}_e(R), \varphi)$, with $\mathrm{W}_e(R) \in \underline{\mathbf{C}}$ and $\varphi : R \to \mathrm{W}_e(R)_{\mathrm{Red}}$ a ring homomorphism, such that for every $A \in \underline{\mathbf{C}}$ and every ring homomorphism $R \xrightarrow{f} A_{\mathrm{Red}}$, there exists a unique ring homomorphism $F : \mathrm{W}_e(R) \xrightarrow{F} A$ such that $f = F_{\mathrm{Red}} \circ \varphi$, i.e. such that the following diagram commutes:



Moreover, φ is an isomorphism, and the pair $(\mathrm{W}_e(R), \varphi)$ is unique up to unique isomorphism.

We may assume that $R = \mathbb{F}_p[X]/(\overline{g}(X))$, where $g(X) \in \mathbb{Z}/p^e\mathbb{Z}$ is a monic polynomial of degree d, for some $d \in \mathbb{Z}_{>0}$, and $\overline{g}(X) := (g(X) \mod p) \in \mathbb{F}_p[X]$ is irreducible. Let $\mathrm{W}_e(R) = (\mathbb{Z}/p^e\mathbb{Z})[X]/(g(X))$. Then $\mathrm{W}_e(R)_{\mathrm{Red}} \cong R$. Let $\varphi : R \xrightarrow{\sim} \mathrm{W}_e(R)_{\mathrm{Red}}$ be the natural isomorphism. We are left with showing that for all $A \in \underline{\mathbf{D}}$ and $f : R \to A_{\mathrm{Red}}$, there is a unique $F : \mathrm{W}_e(R) \to A$, making the following diagram commute:



This follows from Hensel's lemma. The last part follows by properties of universal objects.

This shows that there is a functor

$$\begin{aligned} \mathrm{W}_e : \underline{\mathbf{D}} &\longrightarrow \underline{\mathbf{C}} \\ R &\longmapsto \mathrm{W}_e(R) \end{aligned}$$

that is left adjoint to Red. □

Definition 6.2.55. *Let p be a prime and $d, e \in \mathbb{Z}_{>0}$. The* e-truncated Witt ring *of $\mathbb{F}_{p^d}$ is defined to be $\mathrm{W}_e(\mathbb{F}_{p^d})$.*

Note 6.2.56. The ring $\mathrm{W}_e(\mathbb{F}_{p^d})$ has cardinality p^{de}.

Example 6.2.57. We have $\mathrm{W}_1(\mathbb{F}_{p^d}) = \mathbb{F}_{p^d}$ and $\mathrm{W}_e(\mathbb{F}_p) = \mathbb{Z}/p^e\mathbb{Z}$.

From the above construction, we have the following result.

Proposition 6.2.58. *Let p be a prime and $e, d \in \mathbb{Z}_{>0}$. Then the ring $\mathrm{W}_e(\mathbb{F}_{p^d})$ is local, with maximal ideal $p\,\mathrm{W}_e(\mathbb{F}_{p^d})$, which has cardinality $p^{d(e-1)}$. Moreover, the set of ideals of $\mathrm{W}_e(\mathbb{F}_{p^d})$ is $\{p^i\,\mathrm{W}_e(\mathbb{F}_{p^d}) \mid 0 \leq i \leq e\}$.*

Note 6.2.59. Another way of constructing Witt rings is via Galois theory for commutative rings. In the case of finite rings, the notion of a Witt ring is then replaced by that of a *Galois ring*. This is the more common terminology in literature on separability (see [9, 20]).

Proposition 6.2.60. *Let R be a finite commutative ring. Then R is local separable if and only if $R \cong \mathrm{W}_e(\mathbb{F}_{p^d})$, for some prime p and some $e, d \in \mathbb{Z}_{>0}$.*

Proof. For the "only if" direction, suppose that R is local separable. Then it has prime power characteristic, p^e, for some prime p and some $e \in \mathbb{Z}_{>0}$. By Theorem 6.2.18, part (iii), we have that R is separable over $\mathbb{Z}/p^e\mathbb{Z}$ if and only if R/pR is separable over $\mathbb{F}_p$. By Corollary 6.2.9, we have that R/pR is semisimple. Hence $R/pR \cong \mathbb{F}_{p^d}$. We have the following commutative diagram:

$$\begin{array}{ccc} R & \twoheadrightarrow & \mathbb{F}_{p^d} \\ \uparrow & & \uparrow \\ \mathbb{Z}/p^e\mathbb{Z} & \twoheadrightarrow & \mathbb{F}_p. \end{array}$$

By the proof of Theorem 6.2.54, we have that $R \cong \mathrm{W}_e(\mathbb{F}_{p^d})$.

The "if" direction follows by construction of truncated Witt rings. □

We can now turn to the classification of finite separable rings. By Proposition 6.2.16, part (ii) it suffices to classify finite connected separable rings.

Proposition 6.2.61. *Let $\mathcal{P}$ be the set of primes. There is a bijection between the sets*

$$\{\text{finite commutative local separable rings}\}/\cong \quad \longleftrightarrow \quad \mathcal{P} \times \mathbb{Z}_{>0} \times \mathbb{Z}_{>0},$$

where

$$[A] \longmapsto (p, d, e), \tag{6.5}$$

if for $\mathfrak{m}$, the maximal ideal of A, we have

$$\begin{aligned} \mathrm{char}(A/\mathfrak{m}) &= p, \\ [A/\mathfrak{m} : \mathbb{F}_p] &= d, \\ \mathrm{char}(A) &= p^e. \end{aligned}$$

The inverse of the map in (6.5) is given by

$$\mathrm{W}_e(\mathbb{F}_{p^d}) \longleftarrow\!\shortmid (p, d, e). \tag{6.6}$$

Proof. This is a consequence of Theorem 6.2.54, Definition 6.2.55 and Proposition 6.2.60. □

Theorem 6.2.62. *Let $\mathcal{P}$ denote the set of primes. Then there is a bijection between the sets*

$$\{\text{finite connected separable rings}\}/\cong \quad \longleftrightarrow \quad \mathcal{P} \times \mathbb{Z}_{>0} \times \mathbb{Z}_{>0} \times \mathbb{Z}_{>0},$$

where

$$[A] \longmapsto (p, d, e, n), \tag{6.7}$$

if

$$\begin{aligned} |A| &= p^{den^2}, \\ |\operatorname{Z}(A)| &= p^{de}, \\ |\operatorname{Z}(A)/p\operatorname{Z}(A)| &= p^d. \end{aligned}$$

The inverse of the map in (6.7) is given by

$$\mathcal{M}_n(\mathrm{W}_e(\mathbb{F}_{p^d})) \longleftarrow\!\shortmid (p, d, e, n). \tag{6.8}$$

Proof. By Theorem 6.2.52, a finite connected ring is separable if and only if it is separable projective over its prime subring, which by Theorem 6.2.36 is equivalent to being Azumaya over its centre and its centre being separable over its prime subring. Given Proposition 6.2.61, we are thus left with classifying Azumaya algebras over truncated Witt rings.

The map given in (6.7) is well-defined, since $\mathrm{W}_e(\mathbb{F}_{p^d})$ is a local ring, and hence the degree of any Azumaya $\mathrm{W}_e(\mathbb{F}_{p^d})$-algebra is well-defined and is a square (Corollary 6.2.26). Injectivity follows from Example 6.2.34, part 3. Surjectivity follows from the fact that matrix rings over commutative rings are separable (Example 6.2.11).

Note that an Azumaya algebra over a commutative local ring is free as a module over that ring (since projective modules over local rings are free). The fact that the maps (6.7) and (6.8) are mutual inverses now follows from Proposition 6.2.61, Theorem 6.2.20, part (ii), and Example 6.2.34, part 3. □

Corollary 6.2.63. *Let A be a finite separable ring. Then $A \cong A^{\mathrm{o}}$ as rings.*

We know from Theorem 1.2.11 that for R a commutative ring, $n \in \mathbb{Z}_{>0}$ and $S = \mathcal{M}_n(R)$, every two-sided ideal of S is of the form $\mathcal{M}_n(I)$, for some two-sided ideal I of R. Conversely, if I is a two-sided ideal of R, then $\mathcal{M}_n(I)$ is a two-sided ideal of S.

Corollary 6.2.64. *The set of two-sided ideals of a finite connected separable ring is in bijection with the set of ideals of its prime subring.*

Proof. Recall from Proposition 6.2.58 that all ideals of $\mathrm{W}_e(\mathbb{F}_{p^d})$, where p is a prime, are generated by powers of p. In particular, there are exactly $e+1$ ideals, with maximal ideal generated by p. The result now follows from Theorem 6.2.62. □

6.2.7 The trace map and the trace radical

In this section we introduce the notions of trace map and trace ideal, which are closely related to separability.

Let k be a commutative ring and P a finitely generated k-module. Consider the map

$$\mathrm{Hom}_k(P,k) \otimes_k P \xrightarrow{\varphi} \mathrm{End}_k(P), \quad f \otimes x \mapsto (y \mapsto f(y)x). \tag{6.9}$$

Then φ induces a map

$$\begin{aligned} \square : (\mathrm{Hom}_k(P,k) \otimes_k P) \times (\mathrm{Hom}_k(P,k) \otimes_k P) &\longrightarrow \mathrm{Hom}_k(P,k) \otimes_k P, \\ (f \otimes x, g \otimes y) &\longmapsto f(y)g \otimes x, \end{aligned} \tag{6.10}$$

which makes the following diagram commute:

$$\begin{array}{ccc} \mathrm{End}_k(P) \times \mathrm{End}_k(P) & \xrightarrow{\text{composition}} & \mathrm{End}_k(P) \\ {\scriptstyle \varphi\times\varphi}\uparrow & & \uparrow{\scriptstyle \varphi} \\ (\mathrm{Hom}_k(P,k) \otimes_k P) \times (\mathrm{Hom}_k(P,k) \otimes_k P) & \xrightarrow{\square} & \mathrm{Hom}_k(P,k) \otimes_k P. \end{array} \tag{6.11}$$

Recall the definition of a dual basis.

Lemma 6.2.65 ([57], Lemma 2.9, Remark 2.11)**.** (Dual Basis Lemma) *Let k be a ring and let P be a k-module. Then*

(i) *P is projective if and only if there exists a collection $\{x_i, f_i\}_{i\in I}$ for some index set I, with $x_i \in P$ and $f_i \in \mathrm{Hom}_k(P,k)$ such that*

$$\forall x \in P: \ f_i(x) = 0 \text{ for almost all } i, \text{ and } x = \sum_{i=1}^{n} f_i(x)x_i.$$

(ii) *P is finitely generated projective if and only if there exist $n \in \mathbb{Z}_{>0}$ and a collection $\{x_i, f_i\}_{i=1}^n$ with $x_i \in P$ and $f_i \in \mathrm{Hom}_k(P,k)$ such that*

$$\forall x \in P: \quad x = \sum_{i=1}^{n} f_i(x)x_i,$$

i.e.

$$\varphi\left(\sum_{i=1}^{n} f_i \otimes x_i\right) = \mathrm{id}_P,$$

where φ is the map defined in (6.9).

Note 6.2.66. Part (ii) above is equivalent to requiring $1 \in \mathrm{im}(\varphi)$, where φ is the map defined in (6.9).

Definition 6.2.67. *Let k be a ring and P a projective k-module. A collection $\{x_i, f_i\}_i$ as described in the previous lemma is called a* dual basis *of P.*

Lemma 6.2.68. *Let k be a commutative ring, M a k-module and N a finitely generated projective k-module. Then*

$$\begin{aligned}\psi : \mathrm{Hom}_k(M,k) \otimes_k N &\to \mathrm{Hom}_k(M,N),\\ f \otimes x &\mapsto (y \mapsto f(y)x)\end{aligned}$$

is a k-module isomorphism.

Proof. If $N = k$, then ψ is clearly an isomorphism. Then, by properties of tensor products and Hom's, for any $n \in \mathbb{Z}_{>0}$, we have that $N = k^n$ also gives an isomorphism. But then ψ remains an isomorphism for N a finitely generated projective k-module, since then N is a direct summand of some multiple of k. □

Note 6.2.69. Lemma 6.2.68 remains true if it is M that is finitely generated projective as a k-module (the proof of this follows the same lines).

Now let P be a finitely generated projective k-module. Then the map φ as defined in (6.9) is an isomorphism. Further, if we consider the map

$$\mathrm{Hom}_k(P,k) \otimes_k P \xrightarrow{\psi} k, \quad f \otimes x \mapsto f(x), \tag{6.12}$$

then we get an induced map $\mathrm{tr}_{P/k} := \psi\varphi^{-1}$:

$$\begin{array}{ccc} \mathrm{Hom}_k(P,k) \otimes_k P & \xrightarrow{\sim} & \mathrm{End}_k(P). \\ \downarrow & \swarrow_{\mathrm{tr}_{P/k}} & \\ k & & \end{array} \tag{6.13}$$

Definition 6.2.70. *Let k be a commutative ring and P a finitely generated projective k-module. Then the map $\mathrm{tr}_{P/k}$ of diagram (6.13) is called the* trace *of P over k. The quantity $\mathrm{rk}_{P/k} := \mathrm{tr}_{P/k}(\mathrm{id})$ is called the* Hattori-Stallings rank *of P over k.*

Proposition 6.2.71. *Let k be a commutative ring and P a finitely generated k-module. Then P is projective if and only if $\mathrm{Hom}_k(P,k) \otimes_k P$ is a ring with multiplication given by $\square$, as defined in (6.10).*

Proof. If P is finitely generated projective, then $\mathrm{Hom}_k(P,k) \otimes_k P \cong \mathrm{End}_k(P)$, so it is a ring and the map $\square$ is simply composition of maps by diagram (6.11).

For the other direction, note that $\mathrm{Hom}_k(P,k) \otimes_k P$ being a ring implies the existence of an element $\alpha = \sum_{i=1}^n f_i \otimes x_i \in \mathrm{Hom}_k(P,k) \otimes_k P$ such that for all $\beta \in \mathrm{Hom}_k(P,k) \otimes_k P$, we have $\square(\alpha, \beta) = \beta$. But then for any $x \in P$,

$$\mathrm{id} \otimes x = \square(\sum_{i=1}^n f_i \otimes x_i, \mathrm{id} \otimes x) = \sum_{i=1}^n f_i(x)\, \mathrm{id} \otimes x_i,$$

Applying ψ (as defined in (6.12))to both sides, we get

$$x = \sum_{i=1}^{n} f_i(x)x_i.$$

Hence $\{x_i, f_i\}_{i=1}^n$ is a dual basis of P and so P is finitely generated projective by Lemma 6.2.65. □

The following result says that the trace map $\mathrm{tr}_{P/k}$ behaves "as expected".

Proposition 6.2.72 ([7], Section 1)**.** *Let k be a commutative ring and P a finitely generated projective k-module.*

(i) *Let $e_1, e_2 \in \mathrm{End}_k(P)$. Then $\mathrm{tr}_{P/k}(e_1 + e_2) = \mathrm{tr}_{P/k}(e_1) + \mathrm{tr}_{P/k}(e_2)$.*
(ii) *Let $e \in \mathrm{End}_k(P)$ and $c \in k$. Then $\mathrm{tr}_{P/k}(ce) = c\,\mathrm{tr}_{P/k}(e)$.*
(iii) *Let $e_1, e_2 \in \mathrm{End}_k(P)$. Then $\mathrm{tr}_{P/k}(e_1 \circ e_2) = \mathrm{tr}_{P/k}(e_2 \circ e_1)$.*
(iv) (The trace is compatible with base change) *Let k' be a commutative ring and $\alpha : k \to k'$ a ring homomorphism. Let $P' = P \otimes_k k'$ and $e \in \mathrm{End}_k(P)$. Then*

$$\mathrm{tr}_{P'/k'}(e \otimes_k 1_{k'}) = \alpha(\mathrm{tr}_{P/k}(e)).$$

Let us now consider the case when P is in fact a k-algebra.

Definition 6.2.73. *Let k be a commutative ring and let A be a k-algebra that is finitely generated and projective as a k-module. Then the map $A \to \mathrm{End}_k(A)$ given by $a \mapsto (x \mapsto ax)$ induces a map $\mathrm{Tr}_{A/k} : A \to k$ in the following diagram:*

$$\begin{array}{ccccc} \mathrm{Hom}_k(A,k) \otimes_k A & \xrightarrow{\sim} & \mathrm{End}_k(A) & \longleftarrow & A. \\ \downarrow & & \nearrow_{\mathrm{tr}_{A/k}} & \swarrow_{\mathrm{Tr}_{A/k}} & \\ k & & & & \end{array}$$

We call $\mathrm{Tr}_{A/k}$ the trace map *of A over k.*

Note 6.2.74. It is easy to see that $\mathrm{Tr}_{A/k}$ is a k-module homomorphism. Moreover, by Proposition 6.2.72, part (iii), for all $a, b \in A$, we have $\mathrm{Tr}_{A/k}(ab) = \mathrm{Tr}_{A/k}(ba)$.

We give a second definition of the trace map, using a more element-oriented approach.

Definition 6.2.75. *Let k be a commutative ring and A a k-algebra that is finitely generated projective as a k-module. Let $\{x_i, f_i\}$ be a dual basis of A over k. We define*

$$\mathrm{tr}_{A/k} : \mathrm{End}_k(A) \to k, \quad g \mapsto \sum_{i=1}^{n} f_i(g(x_i))$$

and

$$\mathrm{Tr}_{A/k} : A \to k, \quad r \mapsto \sum_{i=1}^{n} f_i(rx_i).$$

Note 6.2.76. The above definition is independent of the choice of dual basis. One way to see this is the following proposition.

Proposition 6.2.77. *The two definitions of* $\mathrm{Tr}_{A/k}$ *agree.*

Proof. Let $\{a_i, f_i\}_{i=1}^n$ be a dual basis of A as a finitely generated projective module over k. Let $\mathrm{Tr}^{(1)}_{A/k}$ be the trace map as in Definition 6.2.73 and $\mathrm{Tr}^{(2)}_{A/k}$, the trace map as in Definition 6.2.75. For any $a \in A$, consider the two trace maps:

$$A \longrightarrow \mathrm{End}_k(A) \longrightarrow k$$

$$\mathrm{Tr}^{(1)}_{A/k}: \qquad a \longmapsto e_a := (x \mapsto ax) \longmapsto \mathrm{tr}_{A/k}(e_a)$$

$$\mathrm{Tr}^{(2)}_{A_k}: \qquad a \longmapsto \sum_{i=1}^n f_i(aa_i).$$

Consider the element $\sum_{i=1}^n f_i \otimes aa_i \in \mathrm{Hom}_k(A,k) \otimes_k A$. This maps to

$$(y \mapsto \sum_{i=1}^n f_i(y)aa_i = \sum_{i=1}^n af_i(y)a_i = ay) = e_a$$

under the isomorphism $\varphi : \mathrm{Hom}_k(A,k) \otimes_k A \xrightarrow{\sim} \mathrm{End}_k(A)$, which in turn maps to $\mathrm{tr}_{A/k}(a) = \mathrm{Tr}^{(1)}_{A/k}(a) \in k$. Also, it maps to $\sum_{i=1}^n f_i(aa_i) \in k$ under $\psi : \mathrm{Hom}_k(A,k) \otimes_k A \to k$. Hence $\mathrm{Tr}^{(1)}_{A/k}(a) = \mathrm{tr}_{A/k}(e_a) = \sum_{i=1}^n f_i(aa_i) = \mathrm{Tr}^{(2)}_{A/k}(a)$. □

Example 6.2.78. Let k be a commutative ring and let A be a k-algebra such that $A \cong k^n$ as k-modules, for some $n \in \mathbb{Z}_{>0}$. Let $\mathcal{B} = \{b_i \mid 1 \le i \le n\}$ be a basis of A over k. Then a dual basis of A over k is given by $\{b_i, f_i\}_{i=1}^n$, where $f_j : \sum_{i=1}^n a_i b_i \mapsto a_j$. It is easy to see that $\mathrm{Tr}_{A/k}(1) = n \cdot 1$.

Example 6.2.79. Let k be a commutative ring and let $A = \mathcal{M}_n(k)$. Then

$$\mathrm{Tr}_{A/k} = n \cdot (\text{usual trace}).$$

Example 6.2.80. Let A be a finite-dimensional algebra over a field k. Then nilpotent elements of A have trace zero. This is because nilpotent matrices over a field have trace zero.

Example 6.2.81. Let A be a finite-dimensional algebra over a field $\mathbb{F}_p$, where p is a prime and let S be a finite A-module. Since S is a vector space over $\mathbb{F}_p$, we have a ring homomorphism $\rho : A \to \mathrm{End}_{\mathbb{F}_p}(S)$ given by sending an element $a \in A$ to the endomorphism of S corresponding to the action of a on S. Define $\mathrm{Tr}^{(S)} : A \to \mathbb{F}_p$ to be the map $\mathrm{tr}_{S/\mathbb{F}_p} \circ \rho$, where $\mathrm{tr}_{S/\mathbb{F}_p}$ is the trace of S over $\mathbb{F}_p$. Note that $\mathrm{Tr}^{(A)} = \mathrm{Tr}_{A/\mathbb{F}_p}$

is the usual trace map, as defined in 6.2.73. If $0 \to S \to T \to U \to 0$ is an exact sequence of A-modules, then

$$\mathrm{Tr}^{(T)} = \mathrm{Tr}^{(S)} + \mathrm{Tr}^{(U)}.$$

To see this, suppose C_1, C_2 are bases for S and U respectively. Then the matrix of $\mathrm{Tr}^{(T)}$ can be represented as an upper triangular block matrix, where the two diagonal blocks are the matrices of $\mathrm{Tr}^{(S)}$ and $\mathrm{Tr}^{(U)}$ with respect to C_1 and C_2 respectively. Moreover, if a basis of T contains a basis of S, then the rest is a basis of U.

Definition 6.2.82. *Let k be a commutative ring and A a k-algebra that is finitely generated projective as a k-module. The* trace radical *of A over k is the kernel of the right A-module homomorphism:*

$$\psi : A \to \mathrm{Hom}_k(A, k), \quad a \mapsto \mathrm{Tr}_{A/k} \cdot a := (x \mapsto \mathrm{Tr}_{A/k}(ax)). \tag{6.14}$$

In other words,

$$I_{A/k} := \{a \in A \mid \mathrm{Tr}_{A/k}(aA) = 0\}.$$

Note 6.2.83.

(i) By Proposition 6.2.72, part (iii), the trace radical is a two-sided ideal.
(ii) By Proposition 6.2.72, part (iii), if $\mathrm{Tr}_{A/k}$ generates $\mathrm{Hom}_k(A, k)$ as a right A-module, then it generates it as a left A-module.
(iii) Suppose k is a field. Since $\dim_k(A) = \dim_k(\mathrm{Hom}_k(A, k))$, we have that $A \cdot \mathrm{Tr}_{A/k} = \mathrm{Hom}_k(A, k)$ if and only if $I_{A/k} = 0$.

Lemma 6.2.84. *Let A be a finite ring. Suppose $A = \prod_{i=1}^{l} A_i$, for some $l \in \mathbb{Z}_{>0}$ and A_i finite rings. Let $n_i := \mathrm{char}(A_i)$ and suppose that for all $i \neq j$ we have* $\gcd(n_i, n_j) = 1$ *and that each A_i is free as a module over $\mathbb{Z}/n_i\mathbb{Z}$. Then*

$$I_{A/(\mathbb{Z}/\mathrm{char}(A)\mathbb{Z})} = \prod_i I_{A/(\mathbb{Z}/n_i\mathbb{Z})}.$$

Proof. Write $k := \mathbb{Z}/\mathrm{char}(A)\mathbb{Z}$. First note that $\mathrm{char}(A) = \prod_i n_i$ and that A is indeed projective over k, so that $I_{A/k}$ is well-defined. The result now follows from Proposition 6.2.72, part (iv). □

Theorem 6.2.85. *There exists a deterministic polynomial-time algorithm that, given a finite commutative ring k and a finite k-algebra A that is projective as a k-module, computes the trace radical $I_{A/k}$.*

Proof. We begin by computing $\mathrm{Hom}_k(A, k)$, using Proposition 2.4.1. Then $I_{A/k}$ is computed as the kernel of the map ψ from Definition 6.2.82. □

6.2.8 Strongly separable algebras

We now study the connections between the trace radical and separability.

Proposition 6.2.86 ([64], Proposition 6.11)**.** *Let k be a commutative ring and R a commutative k-algebra. Then R is finite-étale over k if and only if R is finitely generated projective as a module over k and $\mathrm{Tr}_{R/k}$ generates $\mathrm{Hom}_k(R,k)$.*

Note 6.2.87. This is usually taken to be the definition of finite-étale.

Let k be a commutative ring. We would like to characterise k-algebras A that are finitely generated and projective as k-modules and have the property that $\mathrm{Tr}_{A/k}$ generates $\mathrm{Hom}_k(A,k)$ as a right A-module, but are not necessarily commutative.

Theorem 6.2.88 ([21], Theorem 1, [49], Theorem 3.4)**.** *Let k be a commutative ring and let A be a k-algebra with centre $R := \mathrm{Z}(A)$ such that A is a finitely generated projective k-module. Then the following are equivalent:*

(i) *The trace map $\mathrm{Tr}_{A/k}$ generates $\mathrm{Hom}_k(A,k)$ as a right A-module.*
(ii) *A is k-separable and $A = R \oplus [A,A]$ as R-modules, where $[A,A]$ is the R-submodule of A generated by elements of the form $ab - ba$, with $a, b \in A$.*
(iii) *A is k-separable and $\mathrm{Tr}_{A/R}(1)$ is a unit in $k \cdot 1_A$, the image of k in R.*
(iv) *A has a symmetric separability idempotent over k.*

Definition 6.2.89. *An algebra satisfying any of the conditions of Theorem 6.2.88 is called a* strongly separable *algebra.*

Note 6.2.90. We see that strongly separable algebras are a special kind of symmetric algebras, namely ones for which a nonsingular, symmetric, associative bilinear map $B : A \times A \to k$ is given by $B(a,b) = \mathrm{Tr}_{A/k}(ba)$. We have seen in Theorem 6.2.45 that any separable algebra that is finitely generated, projective and faithful as a module over its base ring is symmetric, but the trace map need not be nonsingular, and thus may not give rise to such a map B.

Example 6.2.91. Let k be a finite field and let $A = \mathcal{M}_n(k)$. Suppose $\mathrm{char}\, k$ divides n. Then A is separable (and symmetric) over k, but $\mathrm{Tr}_{A/k} = n \cdot (\text{the usual trace}) = 0$, so A is not strongly separable over k. To see that A is a symmetric k-algebra, we must look at the usual trace map, which we denote by tr_0. Consider the map $B : A \times A \to k$ given by $B(a,b) = \mathrm{tr}_0(ab)$. This is now bilinear, symmetric, associative and nonsingular, as required for it to witness the fact that A is symmetric as a k-algebra.

Example 6.2.92. (Strongly separable algebras)

1. Let $n \in \mathbb{Z}_{>0}$ and k be a commutative ring. If $n \cdot 1$ is a unit in k, then $\mathcal{M}_n(k)$ is strongly separable over k with symmetric separability idempotent $n^{-1} \sum_{i,j=1}^{n} E_{ij} \otimes E_{ji}$, where E_{ij} denotes the $n \times n$ matrix whose $(i,j)^{\text{th}}$ entry is equal to 1 and all other entries are equal to 0.

2. Let $n \in \mathbb{Z}_{>0}$ and k be a finite commutative ring. Put $A = \mathcal{M}_n(k)$. If $n \cdot 1$ is not a unit in k, then $n \cdot 1$ is a zero-divisor. Since $\mathrm{Tr}_{A/k} = n \cdot$ (usual trace), we have that $I_{A/k} \neq 0$ and hence A is not strongly separable.
3. Let G be a finite group, k a commutative ring, and put $A := kG$. If $|G|$ is a unit in k, then A is strongly separable over k, with symmetric separability idempotent $|G|^{-1} \sum_{g \in G} g \otimes g^{-1}$.
4. ([3], Corollary 3.1) Let k be a field with $\mathrm{char}(k) = 0$ and A a k-algebra. Then A is strongly separable if and only if it is finite-dimensional and semisimple.

6.3 An approximation of the Jacobson radical

We have seen in Sections 6.2.4 and 6.2.5 that separable projective algebras and separable rings have many nice properties. Until now, however, we have mainly stayed on theoretical ground. We would now like to be able to algorithmically reduce any finite ring to this "state". In other words, given a finite ring, we would like to quotient out by some two-sided ideal and obtain a ring that is separable. Our goal in a perfect world would have been to quotient out by the Jacobson radical and obtain a semisimple ring. Since computing the Jacobson radical is in general out of our reach (see Note 3.4.2), we will have to content ourselves with quotienting out by something that is *almost* the Jacobson radical and obtaining something that is *almost* semisimple, more precisely, something that is separable.

6.3.1 Defining an approximation

Definition 6.3.1. *Let A be a finite ring and $\mathfrak{j}_A \subset A$ an ideal. We say $\mathfrak{j}_A$ is an* approximation of the Jacobson radical *of A if*

(A1) *$\mathfrak{j}_A$ is a two-sided nilpotent ideal of A.*
(A2) *$A/\mathfrak{j}_A$ is finite separable.*
(A3) *The prime subring and generalised prime subring of $A/\mathfrak{j}_A$ coincide.*

Note 6.3.2. Let A be a finite ring. Then by Theorem 1.4.9, Proposition 6.2.43 and Theorem 6.2.52, the Jacobson radical is an approximation of itself.

Note 6.3.3. Approximations of Jacobson radicals are not unique. Let p be a prime and let $A = \mathbb{Z}/p^2\mathbb{Z}$. Then A is finite separable with prime subring and generalised prime subring equal to $\mathbb{Z}/p^2\mathbb{Z}$. Hence 0 and $\mathrm{J}(A) = p\mathbb{Z}/p^2\mathbb{Z}$ are both approximations of the Jacobson radical of A.

Theorem 6.3.4. *Let A be a finite ring and $\mathfrak{j}_A$ a two-sided ideal of A such that $\mathfrak{j}_A$ is nilpotent and $A/\mathfrak{j}_A$ is separable projective over its prime subring. Suppose, moreover, that the characteristic of A is a power of some prime p. Then*

$$(A/\mathfrak{j}_A)/(p(A/\mathfrak{j}_A)) = A/\mathrm{J}(A),$$

and

$$(A/\mathfrak{j}_A)^+ \cong (\mathbb{Z}/p^e\mathbb{Z})^r,$$

where $r = \dim_{\mathbb{F}_p}(A/\operatorname{J}(A))$ *and* $e \in \mathbb{Z}_{>0}$ *is such that* $p^e = \operatorname{char}(A/\mathfrak{j}_A)$.

Proof. Let $e \in \mathbb{Z}_{>0}$ and p be a prime such that $\operatorname{char}(A/\mathfrak{j}_A) = p^e$. First note that, since $A/\mathfrak{j}_A$ is separable over $\mathbb{Z}/p^e\mathbb{Z}$, we have that $(A/pA)/((\mathfrak{j}_A + pA)/pA)$ is semisimple by Corollary 6.2.10 and Theorem 6.2.18, part (iii). This implies that $(\mathfrak{j}_A + pA)/pA \supseteq \operatorname{J}(A/pA)$. Moreover, $\mathfrak{j}_A$ is nilpotent. We thus have that $(\mathfrak{j}_A + pA)/pA = \operatorname{J}(A/pA)$. Hence

$$\begin{aligned}(A/\mathfrak{j}_A)/(p(A/\mathfrak{j}_A)) &= (A/pA)/((\mathfrak{j}_A + pA)/pA)\\ &= (A/pA)/\operatorname{J}(A/pA)\\ &= A/\operatorname{J}(A).\end{aligned}$$

By Nakayama's Lemma, the minimum number of generators of $A/\mathfrak{j}_A$ as a $\mathbb{Z}/p^e\mathbb{Z}$-module is equal to the dimension of $A/\operatorname{J}(A)$ over $\mathbb{F}_p$. But $A/\mathfrak{j}_A$ is projective over $\mathbb{Z}/p^e\mathbb{Z}$, so it is free of finite rank. Thus the rank of $A/\mathfrak{j}_A$ as a $\mathbb{Z}/p^e\mathbb{Z}$-module is equal to $\dim_{\mathbb{F}_p}(A/\operatorname{J}(A))$.

□

Example 6.3.5. Let p be a prime and M an $\mathbb{F}_p$-vector space of dimension 1. Let

$$A = \mathbb{Z}/p^2\mathbb{Z} \oplus M$$

be the ring with componentwise addition and multiplication given by

$$(a, x) \cdot (b, y) = (ab, ay + bx).$$

In particular, A is a commutative ring with $M^2 = 0$. Moreover, $\operatorname{J}(A) = p\mathbb{Z}/p^2\mathbb{Z} \oplus M$.

For any approximation $\mathfrak{j}$ of the Jacobson radical of A we must have $A/\mathfrak{j} \cong \mathbb{Z}/p^2\mathbb{Z}$ or $A/\mathfrak{j} \cong \mathbb{F}_p$. If $A/\mathfrak{j} \cong \mathbb{F}_p$, then it must be the case that $\mathfrak{j} = \operatorname{J}(A)$.

Let S be the set of all approximations of the Jacobson radical of A. We have bijections between the following sets

$$\begin{aligned}S\backslash\{\operatorname{J}(A)\} &\longleftrightarrow \{\text{ring homomorphisms } A \to \mathbb{Z}/p^2\mathbb{Z}\}\\ &\longleftrightarrow \{\text{group homomorphisms } M \to p\mathbb{Z}/p^2\mathbb{Z}\}.\end{aligned}$$

The latter set has p elements and each of these gives rise to an approximation of the Jacobson radical of A of the same size.

Note 6.3.6. Example 6.3.5 shows that, even though the set of all approximations of the Jacobson radical of a finite ring always has a maximal element with respect to inclusion, given by the Jacobson radical, it does not necessarily have a minimal element.

The aim of this section is to describe deterministic polynomial-time algorithms that produce approximations of the Jacobson radical of a finite ring. We are interested in algorithms that have the additional property that, when run on two isomorphic rings, they output isomorphic approximations of their Jacobson radicals (induced by the same isomorphism), even when the ring isomorphism is unknown (cf. Section 3.5).

We will treat rings in a differentiated manner, depending on the size of the primes dividing their characteristic. We define convenient notions of "small" and "large" primes that allow us to split the ring into two parts and deal with them separately. The case of small primes is easy to deal with, since we can actually compute the Jacobson radical and thus arrange for genuine semisimplicity. The case of large primes requires more work and what allows us to deal with them is Theorem 6.2.88, part (iii).

6.3.2 Trace radical vs. Jacobson radical

We start by proving a series of results about the trace ideal (see Definition 6.2.73) that we will make use of within our algorithms.

Proposition 6.3.7. *Let A be a finite-dimensional algebra over a field k. Then the trace ideal $I_{A/k}$ contains the Jacobson radical $\mathrm{J}(A)$.*

Proof. Since A is left-artinian, its Jacobson radical is nilpotent and so by Example 6.2.80, all its elements lie in $I_{A/k}$. □

Theorem 6.3.8. *Let A be a finite-dimensional algebra over the finite field $\mathbb{F}_p$, where p is a prime and $p > \dim_{\mathbb{F}_p}(A)$. Then $I_{A/\mathbb{F}_p} = \mathrm{J}(A)$.*

Proof. The inclusion $\mathrm{J}(A) \subseteq I_{A/\mathbb{F}_p}$ is given by Proposition 6.3.7. For the other inclusion, use Example 6.2.81 and induction to write

$$\mathrm{Tr}_{A/\mathbb{F}_p} = \sum_{\substack{S \text{ simple} \\ \text{up to } \cong}} \mathrm{length}_S(A) \cdot \mathrm{Tr}^{(S)}, \tag{6.15}$$

where the sum is taken over isomorphism classes of simple A-modules and $\mathrm{length}_S(A)$ is the number of times that S occurs in a composition series of A.

Recall from Note 1.4.6 that

$$A/\mathrm{J}(A) \cong \prod_{\substack{S \text{ simple} \\ \text{up to } \cong}} \mathrm{End}_{\mathrm{End}_A(S)}(S) \tag{6.16}$$

as $\mathbb{F}_p$-algebras. Since $I_{A/\mathbb{F}_p}$ is a two-sided ideal of A (by Note 6.2.83) and $I_{A/\mathbb{F}_p} \supseteq \mathrm{J}(A)$, we have that $I_{A/\mathbb{F}_p}/\mathrm{J}(A)$ is a two-sided ideal of $A/\mathrm{J}(A)$, and so it is a subproduct of (6.16).

Suppose $I_{A/\mathbb{F}_p} \neq \mathrm{J}(A)$. Then there is at least one simple S_0 occurring in this subproduct. Then $I_{A/\mathbb{F}_p}$ contains all elements of A that act as 0 on all simple A-modules not isomorphic to S_0. Consider such an element that acts as 1 on S_0 and as 0 on all other simples. Since it lies in the product of (6.16), it is represented by an element $r \in A$. Then by (6.15), the trace of r is $\mathrm{length}_{S_0}(A) \cdot \dim_{\mathbb{F}_p}(S_0)$. This quantity is strictly positive and less than or equal to $\dim_{\mathbb{F}_p}(A)$, so, for $p > \dim_{\mathbb{F}_p}(A)$, it is nonzero in $\mathbb{F}_p$. Hence $r \notin I_{A/\mathbb{F}_p}$, giving a contradiction.

□

Corollary 6.3.9. *There exists a deterministic polynomial-time algorithm that, given a finite algebra over a finite field $\mathbb{F}_p$, where p is a prime satisfying $p > \dim_{\mathbb{F}_p}(A)$, computes the Jacobson radical* $\mathrm{J}(A)$.

Proof. From Theorem 6.3.8 we have $I_{A/\mathbb{F}_p} = \mathrm{J}(A)$, and the trace ideal can be computed deterministically in polynomial time by Theorem 6.2.85. □

Note 6.3.10. We already knew this ([18, 27]).

Definition 6.3.11. *Let A be a finite ring and let $n := \mathrm{char}(A)$. We say a prime $p \mid n$ is* a small prime for A *if $p \leq \dim_{\mathbb{F}_p}(A/pA)$. We say a prime $p \mid n$ is* a large prime for A *if $p > \dim_{\mathbb{F}_p}(A/pA)$.*

Note 6.3.12. When it is clear what ring we are referring to, we will simply refer to a prime as being large or small.

Note 6.3.13. Let A be a finite ring. Then a prime $p \mid \mathrm{char}(A)$ is large if the number of cyclic direct summands of A^+ of size divisible by p (a quantity which is independent of the decomposition), is larger than p.

Proposition 6.3.14. *Let A be a finite ring and let m be its characteristic. Suppose m is divisible only by large primes and that A is projective as a $\mathbb{Z}/m\mathbb{Z}$-module. Let*

$$n' = \mathrm{rad}(m) := \prod_{\substack{p \mid m \\ p \text{ prime}}} p.$$

Then $n'A \subseteq \mathrm{J}(A)$ and

$$\begin{aligned} \mathrm{J}(A)/n'A &= \mathrm{J}(A/n'A) \\ &= I_{(A/n'A)/(\mathbb{Z}/n'\mathbb{Z})} \\ &= \left(I_{A/(\mathbb{Z}/m\mathbb{Z})} : \frac{m}{n'}A\right)/n'A, \end{aligned} \tag{6.17}$$

where $I_{A/(\mathbb{Z}/m\mathbb{Z})}$ is the trace radical of A over $\mathbb{Z}/m\mathbb{Z}$, as before, and

$$\left(I_{A/(\mathbb{Z}/m\mathbb{Z})} : \frac{m}{n'}A\right) := \{x \in A \mid \frac{m}{n'}x \in I_{A/(\mathbb{Z}/m\mathbb{Z})}\}.$$

Proof. To simplify notation, we write $I_A := I_{A/(\mathbb{Z}/m\mathbb{Z})}$ and $I_{A/n'A} := I_{(A/n'A)/(\mathbb{Z}/n'\mathbb{Z})}$. We will use similar abbreviations for the trace maps. Note that $A/n'A$ is projective as a module over $\mathbb{Z}/n'\mathbb{Z}$, so the trace map and the trace radical are well-defined.

It is easy to see that $n'A$ is nilpotent in A, since some power of n' is divisible by m. The first equality of (6.17) follows since $n'A$ is nilpotent and the second equality follows by Proposition 1.4.11, Theorem 6.3.8 and Lemma 6.2.84. For the last part,

note that by Proposition 6.2.72, part (iv), we have $\mathrm{Tr}_{A/n'A} \equiv \mathrm{Tr}_A \mod n'$. Hence

$$\begin{aligned} x + n'A \in I_{A/n'A} &\iff \mathrm{Tr}_{A/n'A}((A/n'A)(x + n'A)) = 0 \\ &\iff \mathrm{Tr}_{A/n'A}(Ax + n'A) = 0 \\ &\iff \mathrm{Tr}_A(Ax) \subset n'\mathbb{Z}/m\mathbb{Z} \\ &\iff \frac{m}{n'}\,\mathrm{Tr}_A(Ax) = 0 \\ &\iff \frac{m}{n'}x \in I_A \\ &\iff x + n'A \in \left(I_A : \frac{m}{n'}A\right)/n'A. \end{aligned}$$

□

Proposition 6.3.15. *Let A be a finite ring and let $\mathrm{char}(A) := p^e$, for some prime p and some $e \in \mathbb{Z}_{>0}$. Suppose that A is free as a $\mathbb{Z}/p^e\mathbb{Z}$-module and p is a large prime. Let $B := A/I_{A/(\mathbb{Z}/p^e\mathbb{Z})}$ and let $0 < e' \leq e$. Then*

(i) *if B is free as a $\mathbb{Z}/p^e\mathbb{Z}$-module, then B is separable over $\mathbb{Z}/p^e\mathbb{Z}$.*
(ii) *if $B/B[p^{e-e'}]$ is free as a $\mathbb{Z}/p^{e'}\mathbb{Z}$-module, then $B/B[p^{e-e'}]$ is separable over $\mathbb{Z}/p^{e'}\mathbb{Z}$, where $B[p^{e-e'}] = \ker(B \to B, b \mapsto p^{e-e'}b)$.*

Proof. (i) Since B is free over $\mathbb{Z}/p^e\mathbb{Z}$, by Theorem 6.2.18, part (iii), we have that B is separable over $\mathbb{Z}/p^e\mathbb{Z}$ if and only if B/pB is separable over $\mathbb{F}_p$. By Theorem 6.3.8, since $p > \dim_{\mathbb{F}_p}(A/pA)$, we have

$$B/pB = (A/pA)/I_{(A/pA)/\mathbb{F}_p} = (A/pA)/\,\mathrm{J}(A/pA),$$

so B/pB is semisimple, and thus B is separable over $\mathbb{Z}/p^e\mathbb{Z}$ (see Corollary 6.2.9).

(ii) Let $C := B/B[p^{e-e'}]$ and consider the canonical map $\pi : A \twoheadrightarrow C$. First note that

$$\begin{aligned} \ker(\pi) &:= \ker(A \twoheadrightarrow B := A/I_{A/(\mathbb{Z}/p^e\mathbb{Z})} \twoheadrightarrow C := B/B[p^{e-e'}]) \\ &= (I_{A/(\mathbb{Z}/p^e\mathbb{Z})} : p^{e-e'}A), \end{aligned}$$

where

$$(I_{A/(\mathbb{Z}/p^e\mathbb{Z})} : p^{e-e'}A) := \{x \in A \mid p^{e-e'}x \in I_{A/(\mathbb{Z}/p^e\mathbb{Z})}\}.$$

Further,

$$\begin{aligned} \pi^{-1}C[p^{e'-1}] &= \{x \in A \mid p^{e'-1}x \in (I_{A/(\mathbb{Z}/p^e\mathbb{Z})} : p^{e-e'}A)\} \\ &= (I_{A/(\mathbb{Z}/p^e\mathbb{Z})} : p^{e-1}A). \end{aligned}$$

Since C is free as a $\mathbb{Z}/p^{e'}\mathbb{Z}$-module, we have that $C[p^{e'-1}] = pC$, so

$$\pi^{-1}C[p^{e'-1}] = pA + \ker(\pi).$$

Hence

$$(I_{A/(\mathbb{Z}/p^e\mathbb{Z})} : p^{e-e'}A) + pA = (I_{A/(\mathbb{Z}/p^e\mathbb{Z})} : p^{e-1}A). \tag{6.18}$$

Since C is free as a $\mathbb{Z}/p^{e'}\mathbb{Z}$-module, by Theorem 6.2.18, part (iii), we have that C is separable over $\mathbb{Z}/p^{e'}\mathbb{Z}$ if and only if C/pC is semisimple. But, since p is large,

$$\begin{aligned} C/pC &= (A/pA)/((I_{A/(\mathbb{Z}/p^e\mathbb{Z})} : p^{e-e'}A) + pA)/pA) \\ &= (A/pA)/(I_{A/(\mathbb{Z}/p^e\mathbb{Z})} : p^{e-1}A)/pA), \quad \text{by (6.18)} \\ &= (A/pA)/I_{(A/pA)/\mathbb{F}_p}, \quad \text{by (6.17)} \\ &= (A/pA)/\operatorname{J}(A/pA), \quad \text{by Theorem 6.3.8.} \end{aligned}$$

□

Proposition 6.3.16. *Let A be a finite ring and let $n := \operatorname{char}(A)$. Suppose that A is projective as a $\mathbb{Z}/n\mathbb{Z}$-module. If all primes p dividing n are large, then $I_{A/(\mathbb{Z}/n\mathbb{Z})} \subseteq J(A)$.*

Proof. Let S be a simple A-module. Then S has exponent p for some prime $p \mid n$. So S is a simple module over A/pA. By Proposition 6.2.72, part (iv), the following diagram commutes:

$$\begin{array}{ccc} A & \longrightarrow & A/pA \\ \Big\downarrow{\scriptstyle \operatorname{Tr}_{A/(\mathbb{Z}/n\mathbb{Z})}} & & \Big\downarrow{\scriptstyle \operatorname{Tr}_{(A/pA)/\mathbb{F}_p}} \\ \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \mathbb{F}_p. \end{array}$$

Since p is large, by Theorem 6.3.8 we have

$$(I_{A/(\mathbb{Z}/n\mathbb{Z})} + pA)/pA \subseteq \operatorname{J}(A/pA). \tag{6.19}$$

Let $i \in I_{A/(\mathbb{Z}/n\mathbb{Z})}$. By (6.19), the image of i in A/pA lies in $\operatorname{J}(A/pA)$, so it annihilates all simple A/pA-modules. In particular, it annihilates S. Hence i annihilates all simple A-modules. So $i \in \operatorname{J}(A)$. □

Proposition 6.3.17. *Let A be a finite ring and let $m := \operatorname{char}(A)$. Suppose A is projective over $\mathbb{Z}/m\mathbb{Z}$ and that all primes dividing m are large. Then $\operatorname{char}(A) = \operatorname{char}(A/I_{A/(\mathbb{Z}/m\mathbb{Z})})$.*

Proof. Write $I := I_{A/(\mathbb{Z}/m\mathbb{Z})}$. By Proposition 6.2.72, for all primes $p \mid m$, we have that $\operatorname{Tr}_{A/(\mathbb{Z}/m\mathbb{Z})}(1) \equiv \dim_{\mathbb{F}_p}(A/pA) \mod p$. Since all primes dividing m are large, we have $p > \dim_{\mathbb{F}_p}(A/pA)$, and so $p \nmid \operatorname{Tr}_{A/(\mathbb{Z}/m\mathbb{Z})}(1)$ for all $p \mid m$. Hence $\operatorname{Tr}_{A/(\mathbb{Z}/m\mathbb{Z})}(1)$ is a unit in A. Now by Proposition 6.3.16 we have $I \subseteq \operatorname{J}(A)$, so $\operatorname{Tr}_{A/(\mathbb{Z}/m\mathbb{Z})}(1) \notin I$, otherwise it would be a nilpotent element of A. Hence $\operatorname{Tr}_{A/(\mathbb{Z}/m\mathbb{Z})}(1)$ is an element of additive order m in A/I. □

6.3.3 Separating small primes from large primes

To develop algorithms from the theory in the previous sections, we first need to address the problem of separating small primes from large primes.

Proposition 6.3.18. *There exists a deterministic polynomial-time algorithm that, given a finite ring A of characteristic n, outputs two positive integers n_1 and n_2, such that:*

(i) $n_1 \cdot n_2 = n$,
(ii) $\gcd(n_1, n_2) = 1$,
(iii) *all primes dividing n_1 are small and all primes dividing n_2 are large.*

Moreover, the algorithm produces a prime factorisation of n_1.

Proof. Suppose the finite abelian group A^+ is given to the algorithm as the direct sum of cyclic groups $A^+ \cong \bigoplus_{i=1}^{t} \mathbb{Z}/d_i\mathbb{Z}$, where for all $1 \leq i \leq t$, we have $d_i \in \mathbb{Z}_{>1}$. Let $S := \{p \mid p \text{ prime}, p \leq t\}$. Note that if a prime p is small, then certainly $p \leq t$, since $\dim_{\mathbb{F}_p}(A/pA) = \#\{i \mid p \mid d_i\} \leq t$. So the set S will certainly contain all small primes. Now we decide which of the primes which occur in the factorisation of the d_i are actually small, by checking the condition $p \leq \dim_{\mathbb{F}_p}(A/pA)$. Finally, we gather all small primes, with their exponents, into n_1.

To see that the algorithm is polynomial-time, note that $t \leq \log_2(|A|)$. □

Note 6.3.19. In the process of running the algorithm of Proposition 6.3.18, we have obtained a complete factorisation of n_1, i.e. we know what all the small primes dividing n are, and what their multiplicities are. Note that any two isomorphic rings have the same small primes, with the same multiplicities.

Lemma 6.3.20. *There exists a deterministic polynomial-time algorithm that, given a finite ring A, computes a two-sided nilpotent ideal I of A and two positive integers n_1' and n_2' such that*

(i) $n_1' \cdot n_2' = \operatorname{char}(A/I)$,
(ii) $\gcd(n_1', n_2') = 1$,
(iii) *all primes dividing n_1' are small for A/I and all primes dividing n_2' are large for A/I,*
(iv) *n_1' is squarefree.*

Proof. We start by computing the characteristic of A using Theorem 3.3.1 and then apply Proposition 6.3.18 to compute n_1 and n_2, i.e. to separate small primes for A from large primes for A. This also gives a complete factorisation of n_1. Let $m \in \mathbb{Z}_{>1}$ be the largest integer such that $m^2 \mid n_1$ and write $n = m \cdot l$. Then $lA \neq 0$, but $(lA)^2 = 0$, so we have found a nilpotent two-sided ideal, $I = lA \subset A$. Put $n_1' = n_1/m$ and $n_2' = n_2$. Note also that the small (resp. large) primes for A are the same as the small (resp. large) primes for A/I. □

Theorem 6.3.21. *There exists a deterministic polynomial-time algorithm that, given a finite ring A, computes a two-sided nilpotent ideal $\mathfrak{i}$ such that*

$$A/\mathfrak{i} \cong A_1 \times A/n_2A,$$

where A_1 is semisimple and all primes dividing n_2 are large for $A/\mathfrak{i}$.

Proof. By Lemma 6.3.20, we may write

$$A/I \cong A/n_1A \times A/n_2A,$$

for some two-sided nilpotent ideal $I \subseteq A$, where n_2 is divisible only by large primes for A/I and n_1 is squarefree. For each prime $p \mid n_1$, the ring A/pA is an algebra over $\mathbb{F}_p$, so by Theorem 3.4.1 we may compute its Jacobson radical and factor it out of A, making the first component genuinely semisimple.

□

6.3.4 Algorithms

Theorem 6.3.22. *There exists a deterministic polynomial-time algorithm that, given a finite ring A, computes an approximation of the Jacobson radical of A.*

Proof. By Theorem 6.3.21, we may assume that $\mathrm{char}(A)$ is only divisible by large primes, i.e. for all primes $p \mid n$, we have $p > \dim_{\mathbb{F}_p}(A/pA)$. We proceed by building a sequence of rings that will terminate with a strongly separable ring (see Theorem 6.2.88 and Definition 6.2.89). We start by putting

$$A_0 := A.$$

To continue, we would like to make use of the trace and the trace radical and for this, we must ensure that we are working with a projective module. We thus quotient out by a multiple of A_0 to get

$$A_1 := A_0/mA_0,$$

where $m \mid \mathrm{char}(A)$ is such that mA_0 is a nilpotent two-sided ideal of A_0, and A_1 is projective as a module over $\mathbb{Z}/m\mathbb{Z}$. The way to do this deterministically in polynomial time has been described in Proposition 2.8.1.

We proceed by computing the trace radical $I := I_{A_1/(\mathbb{Z}/m\mathbb{Z})}$ using Theorem 6.2.85. By Proposition 6.3.8, we have $I \subseteq \mathrm{J}(A_1)$. The next term in our sequence is

$$A_2 := A_1/I.$$

If $I = 0$, then the map

$$\begin{aligned} \phi : A_1 &\to \mathrm{Hom}_{\mathbb{Z}/m\mathbb{Z}}(A_1, \mathbb{Z}/m\mathbb{Z}) \\ a &\mapsto (a \cdot \mathrm{Tr}_{A_1/(\mathbb{Z}/m\mathbb{Z})} : b \mapsto \mathrm{Tr}_{A_1/(\mathbb{Z}/m\mathbb{Z})}(ba)) \end{aligned}$$

is injective, and since A_1 is a finite projective $\mathbb{Z}/m\mathbb{Z}$-module, ϕ is an isomorphism of $\mathbb{Z}/m\mathbb{Z}$-modules, i.e. the trace map generates $\mathrm{Hom}_{\mathbb{Z}/m\mathbb{Z}}(A_1, \mathbb{Z}/m\mathbb{Z})$ as a left module, which is equivalent to A being strongly separable over $\mathbb{Z}/m\mathbb{Z}$ by Theorem 6.2.88.

If $I \neq 0$, then we treat A_2 as we did A_0, i.e. we make it projective as a module and calculate the trace radical of the resulting ring. We continue in this manner until the trace radical becomes equal to 0. In the end we will have produced a strongly separable algebra over its prime subring.

By Proposition 2.8.1, for every prime p dividing the characteristic of the final ring, a unique power of p occurs as an invariant of the underlying abelian group of the ring. Hence the generalised prime subring of the final ring is equal to its prime subring.

Set $\mathtt{j}_A$ to be the kernel of the map induced by the successive quotienting. Since $\mathrm{length}(A_i) < \mathrm{length}(A_{i-1})$, for all i, the algorithm terminates in polynomial time. □

Note 6.3.23. Suppose $\mathrm{char}(A) = n = \prod_{i=1}^{t} p_i^{e_i}$, for some $n \in \mathbb{Z}_{>0}$, p_i distinct primes and $e_i \in \mathbb{Z}_{>0}$. Then the number of iterations performed by the algorithm is bounded above by $\sum_{i=1}^{t} e_i - t$. This is because at each step we have to make the ring at hand projective over its prime subring in such a way that the radical of the characteristic is not changed.

Calculating the trace radical over and over again is a costly operation. There is a more economic way of proceeding, which we describe in the remaining part of this section. We begin with an auxiliary result.

Proposition 6.3.24. *Let A be a finite ring and let $\mathrm{char}(A) := m$, for some $m \in \mathbb{Z}_{>0}$. Suppose that A is projective as a $\mathbb{Z}/m\mathbb{Z}$-module and that all primes dividing m are large. Let $B := A/I_{A/(\mathbb{Z}/m\mathbb{Z})}$. Let $m' \mid m$ be such that $\mathrm{rad}(m) = \mathrm{rad}(m/m')$ and $B/B[m']$ is projective as a $\mathbb{Z}/\frac{m}{m'}\mathbb{Z}$-module. Then $B[m']$ is nilpotent and $B/B[m']$ is separable over $\mathbb{Z}/\frac{m}{m'}\mathbb{Z}$.*

Proof. Let p be a prime dividing m. Suppose its exponent in the prime factorisation of m is e, and its exponent in the prime factorisation of m' is $e - e' \geq 0$. Let $C := B/B[m']$ and $\varphi : A \to B := A/I_{A/(\mathbb{Z}/m\mathbb{Z})}$ be the canonical map. Then

$$\begin{aligned}\varphi^{-1}(B[p^{e-e'}]) &= \{x \in A \mid p^{e-e'}x \in I_{A/(\mathbb{Z}/p^e\mathbb{Z})}\} \\ &= \left(I_{A/(\mathbb{Z}/p^e\mathbb{Z})} : p^{e-e'}A\right).\end{aligned}$$

We have already seen in Propositions 6.3.15 and 6.3.14 that

$$(I_{A/(\mathbb{Z}/p^e\mathbb{Z})} : p^{e-e'}A) + pA = (I_{A/(\mathbb{Z}/p^e\mathbb{Z})} : p^{e-1}A). \tag{6.20}$$

and

$$(\varphi^{-1}(B[p^{e-e'}]) + pA)/pA = \mathrm{J}(A/pA),$$

so that $\varphi^{-1}(B[p^{e-e'}])$ is nilpotent, and hence $B[p^{e-e'}]$ is nilpotent.

Glueing along all primes (using Lemma 6.2.84), we get that

$$\left(\varphi^{-1}(B[m']) + n'A\right)/n'A = \mathrm{J}(A/n'A), \tag{6.21}$$

and $B[m']$ is nilpotent. Hence $C/n'C = (A/n'A)/\operatorname{J}(A/n'A)$ is semisimple. In particular, since n' is squarefree, $C/n'C$ is separable over $\mathbb{Z}/n'\mathbb{Z}$, by Theorem 6.2.44. Since $n' = \operatorname{rad}(m) = \operatorname{rad}(m/m')$, we have by Theorem 6.2.18, part (iii) and Proposition 6.2.16, part (ii), that C is separable over $\mathbb{Z}/\frac{m}{m'}\mathbb{Z}$.

□

Second proof of Theorem 6.3.22. By Theorem 6.3.21, we may assume that the characteristic of A is only divisible by large primes. We will construct a sequence of rings that terminates at a separable state. We begin as in the proof of Theorem 6.3.22:

$$A_0 := A, \quad A_1 := A_0/mA_0, \quad A_2 := A_1/I_{A_1/(\mathbb{Z}/m\mathbb{Z})},$$

where $m \mid \operatorname{char}(A_0)$ is such that mA_0 is a two-sided nilpotent ideal of A_0, and A_1 is projective over $\mathbb{Z}/m\mathbb{Z}$. We then proceed by putting

$$A_3 := A_2/A_2[m'],$$

where m' is computed using the deterministic polynomial-time algorithm described in Proposition 2.8.2. Then $m' \mid m$ is the least integer such that A_3 is projective over $\mathbb{Z}/\frac{m}{m'}\mathbb{Z}$. By Proposition 6.3.24 (taking $B := A_2$ and $C := A_3$), the ideal $A_2[m']$ is nilpotent and A_3 is separable over $\mathbb{Z}/\frac{m}{m'}\mathbb{Z}$.

By Propositions 2.8.1 and 2.8.2, for every prime p dividing the characteristic of the final ring, a unique power of p occurs as an invariant of the underlying abelian group of the ring. Hence the generalised prime subring of the final ring is equal to its prime subring.

Set $\mathfrak{j}_A = \ker(A \to A_3)$ under the map induced by the successive quotienting. □

Note 6.3.25. A natural question that arises is whether we have to compute any trace radical at all, i.e. whether given a finite ring A, the ideal given by $A[m']$ is not already an approximation of the Jacobson radical. The answer is no. To see this, consider the ring $A = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p^2\mathbb{Z}$, where p is a prime. Then $\operatorname{char} A = p^2$ and $m' = p$. Now $\dim_{\mathbb{F}_p}(A/\operatorname{J}(A)) = 2$, but $A/A[m'] \cong \mathbb{F}_p$ has rank $1 < 2$. This contradicts Theorem 6.3.4.

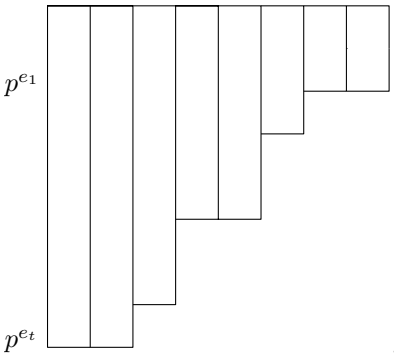
We can also produce a connected example of this type of failure. Let p be a prime and consider the ring $A = (\mathbb{Z}/p^2\mathbb{Z})[X]/(pX^2, X^3)$. Then $\operatorname{char}(A) = p^2$ and $m' = p$. Again, $\dim_{\mathbb{F}_p}(A/\operatorname{J}(A)) = 3$, but $\dim_{\mathbb{F}_p}(A/A[m']) = 2$.

6.3.5 An illustration

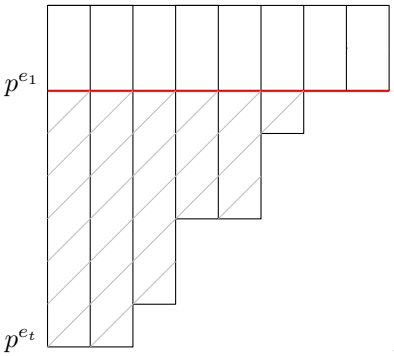
For more clarity, let us explore a graphical illustration of the above results. For simplicity, we restrict to the case that $m = p^e$ for some large prime p and some $e \in \mathbb{Z}_{>0}$. Suppose

$$A^+ \cong \bigoplus_{i=1}^{t} \mathbb{Z}/p^{e_i}\mathbb{Z},$$

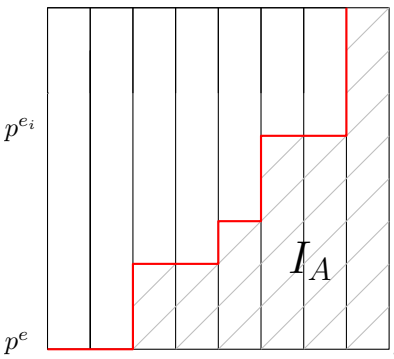
where $e_{i+1} \geq e_i$, $e_1 > 0$ and $e = e_t$. We will represent finite abelian p-groups by



where the number of vertical boxes is equal to the number of cyclic direct summands of A and the height of each such box is equal to the corresponding invariant. Now any finitely generated projective $\mathbb{Z}/p^e\mathbb{Z}$-module is free of finite rank, so is represented by a rectangle. To make A projective over its prime subring, we quotient out by $p^{e_1}A$, where p^{e_1} is the smallest nonzero invariant appearing in the decomposition of A^+ (or by $p^{e'}A$, for any $e' \leq e_1$).

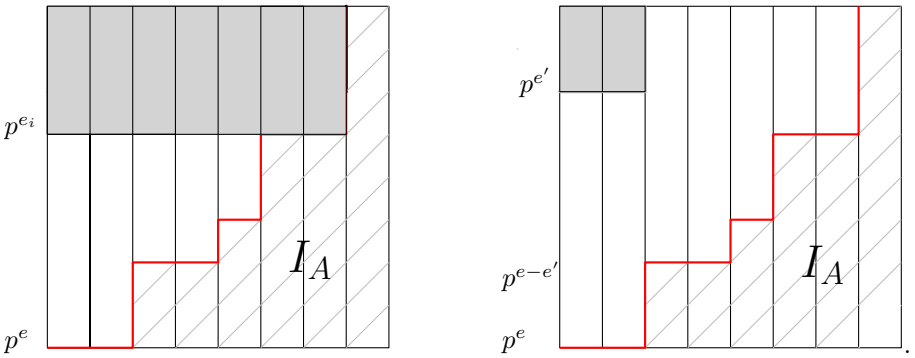


Suppose we have already made A projective as a module over $\mathbb{Z}/m\mathbb{Z}$, so that now $A^+ \cong (\mathbb{Z}/p^e\mathbb{Z})^t$. Then the next step in the algorithm is to quotient out by the trace radical to obtain $A_2 := A/I_A$ with quotient map $\varphi : A \to A_2$. We represent this graphically as:

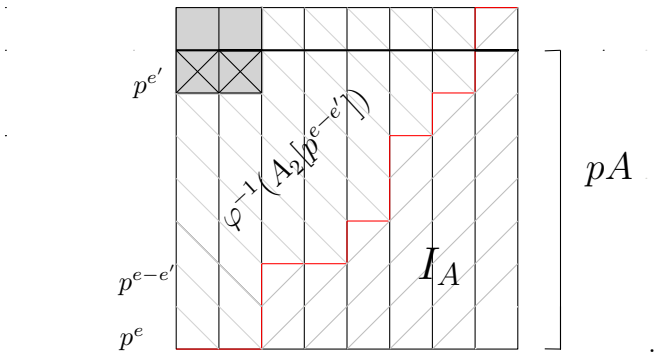


where the shaded lower-right part represents the trace radical. Note that the trace radical must touch the bottom line since when quotienting out by the trace radical, the characteristic remains unchanged (see Proposition 6.3.17). However, it may not touch the top line.

In the first algorithm, we proceed by making the remaining $A_2 := A/I_A$ projective over its prime subring, which we achieve by quotienting out by $p^{e_i}A_2$. This corresponds to looking at the upper-left grey rectangle in the first picture below, which we now treat as our initial box. In the second algorithm we proceed directly by quotienting out by $A_2[p^{e-e'}]$, where $p^{e-e'}$ is the second largest invariant in A_2 (or by quotienting out by $A_2[p^{e-f}]$, for any $0 < f \leq e'$). This leaves us looking at the upper-left grey rectangle in the second picture below, which is now separable projective over its prime subring by the second proof of Theorem 6.3.22.



Note 6.3.26. The equality in (6.20) can be easily seen from the following diagram, since both sides of the equality are represented by the upper-left grey area left unhatched:



6.3.6 Examples

In this section we look at some specific instances of trace computation and running of the algorithms given as proofs of Theorem 6.3.22. We will only consider examples where the characteristic of the given ring is divisible exclusively by large primes.

Note 6.3.27. If A is a finite ring of prime characteristic, then by Theorem 6.2.44, both our algorithms will output the Jacobson radical of A.

Note that rings that are finite products rings of the form $\mathbb{Z}/n\mathbb{Z}$, with $n \in \mathbb{Z}_{>0}$ and componentwise addition and multiplication, are separable over their prime subrings (see Proposition 6.2.16, part (iii)). Thus, if they are projective over their prime subring, they are strongly separable over their prime subring (see Proposition 6.2.86), so their trace ideal is trivial.

Example 6.3.28 (Integers modulo n)**.** Let $A = (\mathbb{Z}/5\mathbb{Z})^2 \times (\mathbb{Z}/3^2\mathbb{Z})$. Note that $5 > 2$ and $3 > 1$, so the primes occurring are large. The prime subring of A is $k = \mathbb{Z}/45\mathbb{Z}$ and A is projective as a k-module and hence A is strongly separable over k. Thus, if A is given to the algorithms proving Theorem 6.3.22, they will find that $I_{A/(\mathbb{Z}/45\mathbb{Z})} = 0$, and will therefore output $\mathfrak{j}_A = 0$.

It is easy to check that a projective basis of A over k is given by $\{F_i, x_i\}_{i=1}^3$, where

$$F_1 : (a, b, c) \mapsto 9a, \quad F_2 : (a, b, c) \mapsto 9b, \quad F_3 : (a, b, c) \mapsto 5c,$$

and

$$x_1 = (4, 0, 0), \quad x_2 = (0, 4, 0), \quad x_3 = (0, 0, 2).$$

Hence by Definition 6.2.75,

$$\mathrm{Tr}_{A/(\mathbb{Z}/45\mathbb{Z})}(a, b, c) = 9 \cdot 4a + 9 \cdot 4b + 5 \cdot 2c,$$

and so $\mathrm{Tr}_{A/(\mathbb{Z}/45\mathbb{Z})}(1) = 82$, which is indeed congruent to $(2 \mod 5)$ and to $(1 \mod 9)$, as predicted by Proposition 6.2.72. Moreover, $82 \equiv 37 \mod 45$, so that $\mathrm{Tr}_{A/(\mathbb{Z}/45\mathbb{Z})}(1)$ is a unit in $\mathbb{Z}/45\mathbb{Z}$ (cf. Theorem 6.2.88, part (iii)).

Example 6.3.29. Consider again the ring of Example 6.3.5,

$$A = \mathbb{Z}/p^2\mathbb{Z} \oplus M,$$

where $p > 2$ is a prime, M is a 1-dimensional $\mathbb{F}_p$-vector space, addition is componentwise and multiplication is given by

$$(a, x) \cdot (b, y) = (ab, ay + bx).$$

Then A is a commutative local ring with maximal ideal $p\mathbb{Z}/p^2\mathbb{Z} \oplus M$. The first step of our algorithms gives $A_1 := \mathbb{Z}/p\mathbb{Z} \oplus M$. Then $I_{A_1/\mathbb{F}_p} = M$ and $A_2 := \mathbb{Z}/p\mathbb{Z}$. Hence both algorithms output $\mathfrak{j}_A = pA + M$.

Example 6.3.30 (Group rings)**.** Let $k = \mathbb{Z}/n\mathbb{Z}$, for some $n \in \mathbb{Z}_{>0}$, and G a finite group. Let $A = k[G]$ be the group ring of G over k. We know from Example 6.2.92, part (3), that if $|G| \cdot 1$ is a unit in k, then A is strongly separable over k. Suppose all primes dividing n are large. Then $p > \dim_{\mathbb{F}_p}(A/pA) = \dim_{\mathbb{F}_p}(\mathbb{F}_p[G]) = |G|$, so $|G|$ is a unit in k and our algorithms output $\mathfrak{j}_A = 0$.

Let $k = \mathbb{Z}/n\mathbb{Z}$ and $A = \mathcal{M}_m(k)$, for some $m \in \mathbb{Z}_{>0}$. We know from Example 6.2.92, parts 1 and 2, that $\mathcal{M}_m(k)$ is strongly separable if and only if m is a unit in k. Moreover, $\mathrm{Tr}_{A/k} = m \cdot (\text{usual trace})$.

Example 6.3.31 (Matrix rings)**.** The smallest example of a matrix ring over a commutative ring whose characteristic is divisible only by large primes is $A = \mathcal{M}_2(\mathbb{F}_5)$. In this case, A is simple, but since the primes occurring are large, the algorithms will not be able to detect this. Since 2 is a unit in $\mathbb{F}_5$, the ring A is strongly separable, so the algorithms will output $\mathfrak{j}_A = 0$.

6.3.7 Remarks

Functoriality

Proposition 6.3.32. *Let $\mathcal{F}$ be the class of finite rings. The two families of ideals $(\mathfrak{j}_A)_{A\in\mathcal{F}}$ and $(\mathfrak{j}'_A)_{A\in\mathcal{F}}$, produced by the two algorithms described in the two proofs of Theorem 6.1.2 are functorial under isomorphisms, i.e. if $\phi : A \to B$ is an isomorphism of finite rings, then $\phi(\mathfrak{j}_A) = \mathfrak{j}_B$ and $\phi(\mathfrak{j}'_A) = \mathfrak{j}'_B$.*

Proof. It is clear by construction (Propositions 2.8.1 and 2.8.2) that two isomorphic rings will yield the same m and m'. Trace ideals are compatible with ring isomorphisms by Proposition 6.2.72, part (iv). □

Comparison between proofs of Theorem 6.3.22

We have already noted that the algorithm given in the second proof of Theorem 6.3.22 performs only 3 steps. But what can we say about the number of iterations (trace radical computations) needed in the first algorithm?

If A is a finite ring, let us write $\mathfrak{j}_1^A$ for the approximation of the Jacobson radical of A produced by the first proof of Theorem 6.3.22, and $\mathfrak{j}_2^A$ for the approximation of the Jacobson radical of A produced by the second proof. So far we have only seen examples where $\mathfrak{j}_1^A = \mathfrak{j}_2^A$. A natural question to ask is how $\mathfrak{j}_1$ and $\mathfrak{j}_2$ compare (with respect to inclusion), or indeed whether they are comparable at all.

We give partial answers to these questions in this section.

Let $e \in \mathbb{Z}_{>0}$ and let $p > 2$ be a prime. Let $e' \in \mathbb{Z}_{>0}$ be such that $2e' < e$. Set

$$A = (\mathbb{Z}/p^e\mathbb{Z})[X]/(X^2 - p^{e'}X).$$

Since A is already projective over its prime subring, in the notation of our algorithms, we have $A_0 := A = A_1$. Write $k := \mathbb{Z}/p^e\mathbb{Z}$, $\mathrm{Tr}_A := \mathrm{Tr}_{A/k}$ and $I_A := I_{A/k}$. Then

$$\mathrm{Tr}_A(1) = 2,$$
$$\mathrm{Tr}_A(X) = p^{e'}.$$

The matrix representing the map

$$A \to \mathrm{Hom}(A, \mathbb{Z}/p^e\mathbb{Z})$$

is then given by

$$F = \begin{pmatrix} 2 & p^{e'} \\ p^{e'} & p^{2e'} \end{pmatrix}.$$

Note that by Theorem 6.3.4, the rank of $A/\mathfrak{j}_1^A$ and that of $A/\mathfrak{j}_2^A$ must be equal to 1.

Suppose that $e = 2e'N + r$, for some $N \in \mathbb{Z}_{>0}$ and some $1 \leq r \leq 2e'$. Then

$$\mathfrak{j}_1^A = \left(p^r, X - \frac{p^{e'}}{2}\right) \tag{6.22}$$

and

$$\mathfrak{j}_2^A = \left(p^{2e'}, X - \frac{p^{e'}}{2}\right). \tag{6.23}$$

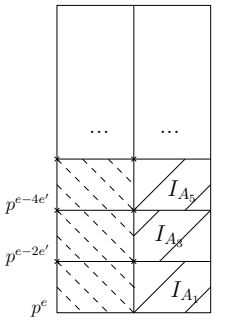
This example illustrates three remarks:

Remark I. The number of iterations performed by the first algorithm is unbounded.

To see this, note that

$$I_A = k \cdot p^{e-2e'}\left(X - \frac{p^{e'}}{2}\right)$$

and the rank of A/I_A is still 2. For the next trace radical computation, we simply replace e by $e-2e'$. Hence if $e > 2e'N$, then the first algorithm performs at least N trace radical computations. Graphically, the algorithm computing $\mathfrak{j}_1^A$ can be represented by the following diagram:



Algorithm 1

Remark II. The cardinality of $A/\mathfrak{j}_2^A$ may be larger than the cardinality of $A/\mathfrak{j}_1^A$.
Compare (6.22) with (6.23).
Remark III. It is possible that $\mathfrak{j}_2^A \subseteq \mathfrak{j}_1^A$.
Compare (6.22) with (6.23).

Good properties

We summarize the good properties of the ring $A/\mathfrak{j}_A$, where $\mathfrak{j}_A$ is an approximation of the Jacobson radical of A.

Theorem 6.3.33. *Let A be a finite ring and $\mathfrak{j}_A$ an approximation of the Jacobson radical of A. Then*

(i) *$A/\mathfrak{j}_A$ is separable,*
(ii) *the prime subring and the generalised prime subring of $A/\mathfrak{j}_A$ coincide,*
(iii) *$A/\mathfrak{j}_A$ admits projectivity and injectivity lift from its prime subring,*
(iv) *$A/\mathfrak{j}_A$ is a quasi-Frobenius ring,*
(v) *$A/\mathfrak{j}_A$ is a symmetric algebra over its prime subring.*

Applications and further questions

The exploration of possible applications of the computation of an approximation of the Jacobson radical of a finite ring is a problem for future research. We record here an application to testing simplicity of a finite module M over a finite ring R. More basic algorithms for this were given in Chapter 5, Section 5.3.

Third proof of Theorem 5.3.1. We begin by computing an approximation $\mathfrak{j}_R$ of the Jacobson radical of R using either of the proofs of Theorem 6.3.22. By Proposition 1.3.14, it is enough to test whether M is simple as an $R/\mathfrak{j}_R$-module, which by Theorem 1.6.4 reduces to testing whether $\mathrm{End}_{R/\mathfrak{j}_R}(M)$ is a field. This can be done by Theorem 5.1.2. □

It is also an interesting question to decide if for a finite ring A, we have $\mathfrak{j}_2^A \subseteq \mathfrak{j}_1^A$ in general. This has not been contradicted by the examples we have considered.

6.4 Computing the generalised prime subring

Let A be a finite ring and denote its generalised prime subring by $\mathcal{P}_A$ (see Definition 6.2.48). The two algorithms proving Theorem 6.3.22 each produce approximations $\mathfrak{j}_A$ of the Jacobson radical of A. In particular, the prime subring of the ring $A/\mathfrak{j}_A$ is equal to its generalised prime subring (see Definition 6.3.1). In what follows, we give a deterministic polynomial-time algorithm that, given a finite ring A, computes $\mathcal{P}_A$.

By Lemma 6.2.50, the generalised prime subring of a finite ring is equal to the generalised prime subring of its centre. Hence we may restrict to the case that A is a

finite commutative ring. Then

$$A = \prod_{\mathfrak{m} \text{ maximal}} A_{\mathfrak{m}},$$

where the product is taken over maximal ideals of A and $A_{\mathfrak{m}}$ denotes the localisation of A at $\mathfrak{m}$. Let $e_{\mathfrak{m}}$ be the primitive idempotent corresponding to $A_{\mathfrak{m}}$. Then $e_{\mathfrak{m}}$ has order a prime power, equal to $\exp(A_{\mathfrak{m}}^+)$.

Let $Q = \{\exp(A_{\mathfrak{m}}^+) \mid \mathfrak{m} \subseteq A \text{ maximal ideal}\}$. Define a map $\mathbb{Z}_{>0} \to A$, $q \mapsto e_q$, where

$$e_q = \sum_{\exp(A_{\mathfrak{m}}^+)=q} e_{\mathfrak{m}}. \tag{6.24}$$

Note that if $q \in \mathbb{Z}_{>0} \backslash Q$, then $e_q = 0$. Moreover,

$$\sum_{q \in Q} e_q = 1.$$

Let

$$B := \sum_{q \in Q} \mathbb{Z} e_q \cong \prod_{q \in Q} \mathbb{Z}/q\mathbb{Z}. \tag{6.25}$$

Then B is a subring of A, since the e_q are orthogonal idempotents of sum 1 (see Theorem 1.5.4). It is easy to see from Definition 6.2.48 that $B = \mathcal{P}_A$.

Proposition 6.4.1. *Let A be a finite commutative ring such that*

$$A^+ \cong \bigoplus_{d \in D} (\mathbb{Z}/d\mathbb{Z})^{n_d}.$$

where $n_d \in \mathbb{Z}_{>0}$ for all $d \in D$. For $d \in D$, let $A[d] = \ker(A \to A, a \mapsto da)$ and

$$I_d := \bigcap_n A[d]^n.$$

Then for all $d \in D$, there exists a unique element $f_d \in I_d$ such that for all $x \in I_d$, we have $f_d x = x$. Moreover,

$$\mathcal{P}_A = \sum_{d \in D} \mathbb{Z} f_d.$$

Proof. Let $d \in D$. First note that $A[d]$ is an ideal of A, and hence so is I_d. Note that

$$A[d] = \prod_{\mathfrak{m}} A_{\mathfrak{m}}[d] = \left(\prod_{\substack{\mathfrak{m} \\ \exp(A_{\mathfrak{m}}^+) \mid d}} A_{\mathfrak{m}} \right) \times \left(\prod_{\substack{\mathfrak{m} \\ \exp(A_{\mathfrak{m}}^+) \nmid d}} \mathfrak{a}_{d,\mathfrak{m}} \right),$$

for some ideal $\mathfrak{a}_{d,\mathfrak{m}} \subsetneq A_{\mathfrak{m}}$ contained in the maximal ideal of $A_{\mathfrak{m}}$. Then

$$I_d = \left(\prod_{\substack{\mathfrak{m} \\ \exp(A_{\mathfrak{m}}^+) | d}} A_{\mathfrak{m}} \right) \times 0,$$

and the identity in the first factor is $\sum_{\substack{q \in Q \\ q|d}} e_q$. Let

$$f_d := \sum_{\substack{q \in Q \\ q|d}} e_q. \tag{6.26}$$

For uniqueness, suppose $f'_d \in I_d$ is another element such that for all $x \in I_d$, we have $f'_d x = x$. Then $f_d = f'_d f_d = f_d$.

We claim that if $e_q \neq 0$, then there exists $d \in D$ such that d is exactly divisible by q, i.e. $q \mid d$ and $\gcd(q, d/q) = 1$. This is because if $e_q \neq 0$, then there exists $\mathfrak{m}$ such that $\exp(A_{\mathfrak{m}}^+) = q$ and $\mathbb{Z}/q\mathbb{Z}$ is a direct summand of $A_{\mathfrak{m}}^+$, and hence of A^+.

Further, we claim that for every $d \in D$ and every prime $p \mid d$, we have that

$$\sum_{\substack{i \\ p^i | d}} e_{p^i} \in \sum_{d \in D} \mathbb{Z} f_d.$$

To see this, let $d \in D$ and suppose $d = d_1 d_2$, where $d_1, d_2 \in \mathbb{Z}_{>0}$ and $(d_1, d_2) = 1$. Then $f_d = f_{d_1} + f_{d_2}$, so $\mathbb{Z} f_d \subseteq \mathbb{Z} f_{d_1} + \mathbb{Z} f_{d_2}$. Moreover, the additive orders of f_{d_1} and f_{d_2} are coprime, and so the additive order of $f_{d_1} + f_{d_2}$ is equal to the additive order of f_d. Hence $\mathbb{Z} f_d \subseteq \mathbb{Z} f_{d_1} + \mathbb{Z} f_{d_2}$. Suppose that for some prime p and some $r \in \mathbb{Z}_{>0}$, we have that p^r divides d exactly. Take $d_1 = p^r$. Then $f_{d_1} = \sum_{0 \leq i \leq r} e_{p^i} \in \mathbb{Z} f_d$, as required.

We now show that $\sum_{d \in D} \mathbb{Z} f_d = B$, where B is as in (6.25). That $\sum_{d \in D} \mathbb{Z} f_d \subseteq B$ follows from (6.26). For the other inclusion, we will show that for all $q = p^r$, with p a prime and $r \in \mathbb{Z}_{>0}$, we have $e_q \in \sum_{d \in D} \mathbb{Z} f_d$. Fix a prime p. If $e_q = 0$, then we are done. Otherwise, pick $d \in D$ that is exactly divisible by q. Then $e_{p^r} + \sum_{1 \leq i < r} e_{p^i} \in \sum_{d \in D} \mathbb{Z} f_d$. By induction on r, we have $e_q \in \sum_{d \in D} \mathbb{Z} f_d$.

□

Note 6.4.2. Proposition 6.4.1 is true for any choice of D. However, if we choose D such that $d_1 \mid d_2 \mid \ldots \mid d_t$, where $t = |D|$, then the relations between the f_{d_i} become simpler. First note that f_{d_i} is an idempotent for every $1 \leq i \leq t$. To make them orthogonal, put $f'_{d_i} := f_{d_i} - f_{d_{i-1}}$ for every $1 < i \leq t$. Let s_i be the order of f'_{d_i}. Then

$$\mathcal{P}_A = \sum_{i=1}^{t} \mathbb{Z} f'_{d_i} \cong \prod_{i=1}^{t} \mathbb{Z}/s_i\mathbb{Z}$$

as rings.

Theorem 6.4.3. *There exists a deterministic polynomial-time algorithm that, given a finite ring A, computes the generalised prime subring $\mathcal{P}_A$.*

Proof. Since $\mathcal{P}_{\mathrm{Z}(A)} = \mathcal{P}_A$, we may assume $A = \mathrm{Z}(A)$. Suppose A^+ is given to the algorithm as

$$A^+ \cong \bigoplus_{d \in D} (\mathbb{Z}/d\mathbb{Z})^{n_d},$$

where $n_d \in \mathbb{Z}_{>0}$. By computing the Smith normal form of the corresponding group presentation matrix, we can ensure that for $D = \{d_1, \ldots, d_t\}$, we have $d_1 \mid d_2 \mid \ldots \mid d_t$ and $d_1 \neq \pm 1$. For each $1 \leq i \leq t$, compute f_{d_i}, as in Proposition 6.4.1. Turn the set $\{f_{d_i}\}_{1 \leq i \leq t}$ into a set of orthogonal idempotents as in Note 6.4.2. Let s_i be the order of f'_{d_i}. The output of the algorithm consists of the set $\{s_i\}_{1 \leq i \leq t}$, together with a map $\prod_{1 \leq i \leq t} \mathbb{Z}/s_i\mathbb{Z} \to A$, given by $1_{(\mathbb{Z}/s_i\mathbb{Z})} \mapsto f_{d_i}$.

□

Note 6.4.4. If the elements of D are not assumed to divide each other, then the additive relations between the f_d can be computed by solving systems of linear equations over $\mathbb{Z}$.

The computation of the generalised prime subring gives another way of testing whether a finite ring is separable.

Second proof of Theorem 6.2.19. By Theorem 6.2.52, a finite ring is separable if and only if it is separable projective over its generalised prime subring. So compute $\mathcal{P}_A$ using Theorem 6.4.3 and then test projectivity of A over $\mathcal{P}_A$ using Theorem 5.4.1. □