Ludo Pulles

Finite Separable Rings

Master thesis

21st September 2021

Thesis supervisor: Prof. Dr. H.W. Lenstra Jr

Leiden University
Mathematical Institute

Contents

Conventions & notation

Throughout this thesis, all rings are understood to have a unit element with respect to multiplication, ring homomorphisms should map the unit element to the unit element and a subring must contain the unit element of the whole ring. Moreover, all the rings mentioned need not be commutative with respect to multiplication, except when this is mentioned explicitly.

The ring of $n \times n$ matrices over the ring A, is denoted by $\mathbf{M}_n(A)$, and $\mathbb{I}_n$ denotes the identity element of $\mathbf{M}_n(A)$. Moreover for any two-sided ideal $I \subseteq A$ we write $\mathbf{M}_n(I)$ for the two-sided ideal in $\mathbf{M}_n(A)$ that consists of all the matrices where all coefficients lie in I.

The logarithm of x taken with base 2 is denoted by $\lg(x)$.

1 Introduction

Separable field extensions play a crucial role in field theory. Auslander and Goldman generalized the notion of separability in [AG60] to algebras over commutative rings. The definition of separable algebras and elementary properties will be the content of section 3.1. Throughout this thesis, a *separable ring* is a ring that is separable as a $\mathbb{Z}$-algebra.

The merit of separable rings is that such rings have "a lot of projective modules", which is made precise in Proposition 3.13. Moreover, separability is a property that is computationally accessible, for example there is a deterministic polynomial-time algorithm that determines if a finite ring is separable. Hence separability is more suitable for computational problems than semisimplicity, because the ring $\mathbb{Z}/n\mathbb{Z}$ is semisimple if and only if n is a squarefree integer (for $n \in \mathbb{Z}_{>1}$) and there is no known polynomial-time test for squarefreeness.

In this thesis, we determine for a given finite ring R, the separable subrings of R that are maximal under inclusion. These maximal separable subrings possess the following remarkable property.

Theorem 1.1. *Let R be a finite ring and S a separable subring of R. Then, S is maximal as a separable subring of R under inclusion if and only if $S + \mathrm{rad}(R) = R$, where $\mathrm{rad}(R)$ is the Jacobson radical of R.*

Because any subring $S \subseteq R$ is isomorphic to uSu^{-1} for any unit $u \in R^*$, we say a subring $T \subseteq R$ is a subring of S *up to conjugation* if there is a unit $u \in R^*$ such that $uTu^{-1} \subseteq S$. This thesis contains a proof of the following theorem.

Theorem 1.2. *Let R be a finite ring. Then, there exists a separable subring $S \subseteq R$ such that any separable subring of R is a subring of S up to conjugation.*

In addition, we prove the following theorem.

Theorem 1.3. *There exists a deterministic polynomial-time algorithm that, given a finite ring R, outputs a separable subring $S \subseteq R$ having the properties in Theorem 1.2.*

Section 2 will introduce the reader to noncommutative ring theory that will be used in the rest of this thesis. Then section 3 covers the definition of separability and elementary properties and in section 3.2, we will focus on finite separable rings. Here we introduce truncated Witt rings and show in Theorem 3.21 that any finite separable ring is a finite product of matrix rings over truncated Witt rings, following the proof in [CT16]. Truncated Witt rings have applications in coding theory, where these rings are known as Galois rings (see [KDS20]).

Section 4 contains the proof of Theorem 1.2. The proof of Theorem 1.2 is very easy for commutative rings, and this will be the content of section 4.1. Then for the remainder of section 4, we will prove that there is a separable subring S of R such that the natural map $S \to R/\mathrm{rad}(R)$ is surjective, where $\mathrm{rad}(R)$ is the Jacobson radical of R. In section 4.5, we will show that two separable subrings S, T with a surjection onto $R/\mathrm{rad}(R)$ are conjugate by a unit in R^*. We will then prove Theorem 1.1 and Theorem 1.2 from this result.

In section 5 we will look at separable rings from a computational perspective. After defining how we represent a finite ring, it will be clear that there is a polynomial-time algorithm that given a finite ring R, decides if R is a separable ring or not. Moreover, we give a proof of Theorem 1.3.

Finally, we will prove in section 5.4 that Theorem 1.2 is efficiently computable in the following sense.

Theorem 1.4. *There exists a deterministic polynomial-time algorithm that given a finite ring R, a separable ring $S \subseteq R$ having the properties in Theorem 1.2 and a separable ring $T \subseteq R$, outputs some $u \in R^*$ such that $T \subseteq uSu^{-1}$.*

2 Ring theory

This thesis is primarily focused on finite rings. In this section, we will highlight some facts from [Lam01, §1-4 & §19-22] on noncommutative rings that will be useful later since we will not assume the reader is familiar with noncommutative ring theory.

2.1 Noncommutative rings

In noncommutative rings, we distinguish between left ideals of R, which are closed under left multiplication by elements of R, and right ideals, which are closed under right multiplication. A *two-sided ideal* of R is a subset $I \subseteq R$ that is both a left ideal of R and a right ideal of R. Given a two-sided ideal I, we may form the quotient ring R/I and we have a natural surjective ring homomorphism $R \to R/I$ given by $a \mapsto a + I$ for $a \in R$. In a commutative ring R, the notions of left and right ideals coincide so we say I is an ideal of R if it is a left ideal of R, in which case I becomes a two-sided ideal.

Definition 2.1. Let R be a ring.

- A left-ideal or right-ideal I is *nil* if every element $x \in I$ is nilpotent, i.e., there exists $n \in \mathbb{Z}_{\geq 1}$ such that $x^n = 0$.
- A left-ideal or right-ideal I is *nilpotent* if there exists $n \in \mathbb{Z}_{\geq 1}$ such that

$$I^n = \underbrace{I \cdot I \cdot \ldots \cdot I}_{n \text{ times}} = 0.$$

- The *opposite ring* of A, denoted by A^{op}, is the ring with the same additive group as A, but with multiplication $*$ defined by $a * b = b \cdot a$ for $a, b \in A^{\mathrm{op}}$, where $\cdot$ is the multiplication in A.
- The *center* of R is the commutative subring of R defined by

$$\mathrm{Z}(R) = \{\, a \in R \mid \forall b \in R\colon \quad ab = ba \,\}.$$

- The *characteristic* of R, denoted by $\mathrm{char}(R)$, is the unique $n \in \mathbb{Z}_{\geq 0}$ such that (n) is the kernel of the unique ring homomorphism $\mathbb{Z} \to R$.

Given some ring R, we distinguish between left R-modules and right R-modules, similar to left and right ideals.

Definition 2.2. Let R and S be rings. An (R, S)-*bimodule* is an abelian group M with a left R-module structure and a right S-module structure such that

$$\forall m \in M, r \in R, s \in S\colon \qquad r \cdot (m \cdot s) = (r \cdot m) \cdot s.$$

Note 2.3. In particular, R is an (R, R)-bimodule. In situations where we want to emphasize that R should be considered as a left module, we will write ${}_R R$.

Definition 2.4. Let R be a ring.

- A left R-module M is *simple* if there are exactly two submodules of M.
- A *direct summand* of a left R-module M is a left R-submodule M' of M such that there exists a left submodule $M'' \subseteq M$ for which the canonical map $M' \oplus M'' \to M$ is an isomorphism of R-modules.
- A left R-module M is *semisimple* if every left submodule of M is a direct summand of M.
- A ring R is *semisimple* if ${}_R R$ is a semisimple left R-module (cf. [Lam01, Thm. (2.5)]).

- A left R-module M is *indecomposable* if there are exactly two direct summands of M.

Definition 2.5. Let R be a ring.

- An element $a \in R$ is *left-invertible* if there exists $b \in R$ such that $b \cdot a = 1$.
- An element $a \in R$ is *right-invertible* if there exists $b \in R$ such that $a \cdot b = 1$.
- An element of R is *invertible* or a *unit* if it is left-invertible and right-invertible. The units of R form a group, which is denoted by R^*.
- A ring R is a *division ring* if R contains exactly one element that is not a unit.

Note 2.6. If $a \in R$ is left-invertible and right-invertible, say $ba = ac = 1$ for $b, c \in R$, then $b = bac = c$. This justifies the notation a^{-1} for the inverse of an element $a \in R^*$ as there is exactly one inverse of a.

Note 2.7. Fields are the commutative division rings.

Definition 2.8. Let R be a ring. The *Jacobson radical*, $\mathrm{rad}(R)$, is the intersection of all maximal left ideals of R.

Remark 2.9. As can be found in [Lam01, §4], the Jacobson radical of a ring R is equal to the intersection of all maximal right ideals of R, which shows $\mathrm{rad}(R)$ is a two-sided ideal. In addition, $\mathrm{rad}(R)$ is the largest left ideal I for which $1 + I \subseteq R^*$ holds. In particular, any nil left ideal is contained in $\mathrm{rad}(R)$, since $1 - x$ is a unit when $x \in R$ is nilpotent.

A ring R is *left Artin* (*right Artin*) if every descending chain of left ideals (right ideals) stabilizes. For example, any finite ring is left Artin and right Artin.

In general, a nilpotent left ideal is nil, but the converse is not true in the ring

$$\mathbb{Z}[X_1, X_2, \dots]/(X_1, X_2^2, X_3^3, \dots),$$

because the ideal $(X_1, X_2, \dots)$ is nil but not nilpotent: $0 \neq X_2 X_3 \dots X_{n+1} \in I^n$ for any $n \geq 1$. The converse is, however, true in left Artin rings, by the following theorem.

Theorem 2.10 ([Lam01, Thm. (4.12)])**.** *Let R be a left Artin ring. Then* $\mathrm{rad}(R)$ *is nilpotent.*

Definition 2.11. Let R be a commutative ring. An *R-algebra* is a pair (A, θ) where A is a ring and $\theta \colon R \to A$ is a ring homomorphism, called the *structure morphism*, with image $\theta(R) \subseteq \mathrm{Z}(A)$.

An *algebra homomorphism* is a ring homomorphism $\varphi \colon A \to B$ from an R-algebra (A, θ) to an R-algebra (B, θ') such that $\theta' = \varphi \circ \theta$.

An *R-subalgebra* of an R-algebra (A, θ), is an R-algebra (B, θ') for which B is a subring of A and $\theta(x) = \theta'(x)$ for all $x \in R$.

2.2 Idempotents

The study of idempotents in a ring is useful for finding out if a ring is a product of two nonzero rings or if it is a matrix ring over some other ring.

Definition 2.12. Let R be a ring.

- An element $e \in R$ is an *idempotent* if $e^2 = e$.
- A *nontrivial idempotent* is an idempotent $e \neq 0, 1$.
- An idempotent $e \in R$ is *central* if $e \in \mathrm{Z}(R)$ (or equivalently $eR(1 - e) = (1 - e)Re = 0$).
- Two idempotents $e, f \in R$ are *orthogonal* if $ef = fe = 0$.
- An idempotent $e \in R$ is *primitive* if $e \neq 0$ and there are no orthogonal nonzero idempotents $a, b \in R$ such that $e = a + b$.

- An idempotent $e \in R$ is *local* if the ring eRe with unit element e has a unique maximal left ideal.

Note 2.13. Idempotents always come in pairs: if $e \in R$ is an idempotent, then $1 - e$ is also an idempotent. Moreover, e and $1 - e$ are orthogonal.

Note 2.14. In a ring R, given a central idempotent e, the natural reduction map gives a ring isomorphism $R \xrightarrow{\sim} R_1 \times R_2$, where $R_1 = R/R(1-e)$ and $R_2 = R/Re$.

Conversely, for nonzero rings R_1 and R_2, the product ring $R_1 \times R_2$ has (at least) two central idempotents: $(1, 0)$ and $(0, 1)$.

Given a ring homomorphism $\varphi\colon A \to B$ from a ring A to a ring B, it is clear that idempotents in A get mapped to idempotents in B, and orthogonal idempotents in A map to orthogonal idempotents in B. We will say an idempotent $e \in B$ *can be lifted to* A if there exists an idempotent $a \in A$ such that $\varphi(a) = e$.

Theorem 2.15 ([Lam01, Thm. (21.28)])**.** *Let R be a ring and $I \subset R$ a nil two-sided ideal. Then, any idempotent of R/I can be lifted to R under the natural map $R \to R/I$.*

Corollary 2.16. *Let R be a left Artin ring. Then any idempotent in $R/\mathrm{rad}(R)$ can be lifted to R.*

Proof. By Theorem 2.10, the two-sided ideal $\mathrm{rad}(R)$ is nilpotent. □

Definition 2.17. Let R be a ring. Then R is called *connected* if R has exactly two central idempotents.

Note 2.18. Now consider a commutative ring R, so every idempotent is central. We will show that the ring R is connected iff $\mathrm{Spec}(R)$ is a connected topological space.

If R has a nontrivial idempotent e, any prime ideal $\mathfrak{p}$ contains e or $1-e$, because $e(1-e) = 0 \in \mathfrak{p}$, but not both as it would otherwise contain $1 = e+(1-e)$. Therefore, $\mathrm{Spec}(R) = V((e)) \sqcup V((1-e))$ is the disjoint union of two nonempty closed sets.

Conversely suppose $\mathrm{Spec}(R) = V(I) \sqcup V(J)$ is a disjoint union of two nonempty closed sets for ideals I, J. Every prime ideal contains $I \cdot J$, so IJ is contained in $\mathfrak{N}$, the nilradical of R, by [AM69, Prop. 1.8]. No prime ideal contains both I and J, so $I + J = R$ holds and in particular, there exist $e \in I$ and $f \in J$ such that we have $e + f = 1$. Observe that

$$e - e^2 = e(e + f) - e^2 = e \cdot f \in \mathfrak{N},$$

holds, which implies that $e + \mathfrak{N}$ is a nontrivial idempotent in the ring $R/\mathfrak{N}$. Lifting $e + \mathfrak{N}$ in $R/\mathfrak{N}$ to an idempotent in R by Theorem 2.15 shows R is not connected.

As shown in Note 2.14, central idempotents correspond to decomposition of rings. In general, for a left R-module M, an idempotent in $\mathrm{End}_R(M)$, the endomorphism ring of M, corresponds to a decomposition of M into a direct sum of two submodules. For the regular left R-module ${}_RR$ the isomorphism $R \cong \mathrm{End}_R({}_RR)^{\mathrm{op}}$ that maps r to the endomorphism $\phi_r\colon x \mapsto xr$ yields the following lemma.

Lemma 2.19 (cf. [Lam01, Ex. 21.15])**.** *Let R be a ring. Suppose for some $n \geq 1$ there are mutually orthogonal idempotents $e_1, \ldots, e_n$ and mutually orthogonal idempotents $e'_1, \ldots, e'_n$ such that*

$$1 = e_1 + e_2 + \cdots + e_n = e'_1 + e'_2 + \cdots + e'_n,$$

and $Re_i \cong Re'_i$ as left R-modules for all $i = 1, \ldots, n$. Then there exists $u \in R^*$ such that for all $i \in \{1, \ldots, n\}$ we have $e'_i = ue_iu^{-1}$.

Proof. The orthogonal idempotents give rise to the decomposition

$$ {}_RR \xrightarrow{\sim} \bigoplus_{i=1}^{n} Re'_i \xrightarrow{\sim} \bigoplus_{i=1}^{n} Re_i \xrightarrow{\sim} {}_RR \tag{1} $$

of the left R-module ${}_RR$ where the isomorphism in the middle is induced by isomorphisms $Re'_i \xrightarrow{\sim} Re_i$.

Let $\varphi \in \mathrm{End}_R({}_RR)$ be the composition of the isomorphisms in (1). For any $i \in \{\, 1, \ldots, n \,\}$ the idempotent e_i corresponds under the isomorphism $R \cong \mathrm{End}_R({}_RR)^{\mathrm{op}}$ to a unique endomorphism $\pi_i \in \mathrm{End}_R({}_RR)$ that is the identity on Re_i and is the zero map on Re_j for all $j \neq i$. Similarly e'_i corresponds to a unique endomorphism π'_i that is the identity on Re'_i and vanishes on Re'_j for $j \neq i$. Then, we must have that $\pi_i = \varphi \circ \pi'_i \circ \varphi^{-1}$ for all $i \in \{\, 1, \ldots, n \,\}$.

Now φ corresponds to a unit $u \in R$. Because R is isomorphic to the opposite ring of $\mathrm{End}_R({}_RR)$, the identity $\pi_i = \varphi \circ \pi'_i \circ \varphi^{-1}$ shows that $e_i = u^{-1} e'_i u$ holds. Therefore, $e'_i = u e_i u^{-1}$ for $i = 1, \ldots, n$. □

3 Separability

In this section, we will introduce the notion of separable algebras, which generalizes the notion of separable field extensions. The main reference used here is Chapter II of [DI71].

3.1 Separable algebras

Let R be a commutative ring and A an R-algebra. The *enveloping algebra* A^{e}, defined as $A \otimes_R A^{\mathrm{op}}$, endows A with a left A^{e}-module structure given by the map

$$\begin{aligned} \cdot : \quad & A^{\mathrm{e}} \times A \to A \\ & ((a \otimes b), c) \mapsto acb \qquad (a, b, c \in A), \end{aligned}$$

which follows from the fact that A is an (A, A)-bimodule. Moreover, there is a left A^{e}-module homomorphism $\mu\colon A^{\mathrm{e}} \to A$ given by

$$\mu\colon a \otimes b \mapsto ab \qquad (a, b \in A),$$

extended R-linearly. As μ is surjective, this gives a short exact sequence of left A^{e}-modules

$$0 \longrightarrow \ker(\mu) \longrightarrow A^{\mathrm{e}} \xrightarrow{\mu} A \longrightarrow 0. \tag{2}$$

Remark 3.1. The morphism μ is a ring homomorphism if and only if A is commutative. If A is commutative, then

$$\mu(a \otimes b)\mu(c \otimes d) = abcd = (ac)(db) = \mu(ac \otimes db) \qquad (\text{for all } a, b, c, d \in A).$$

The converse can be shown by for example taking $a = d = 1$ in the equation above.

Note 3.2. We will show that the two-sided ideal $\ker(\mu) \subseteq A^{\mathrm{e}}$ is generated as a left A^{e}-module by elements of the form $(a \otimes 1) - (1 \otimes a)$ with $a \in A$. Clearly, $\mu((a \otimes 1) - (1 \otimes a)) = a - a = 0$ for $a \in A$. Conversely, suppose $\sum_{i=1}^{n} a_i \otimes b_i \in \ker(\mu)$ for some $n \in \mathbb{Z}_{\geq 0}$ and $a_i, b_i \in A$ $(i = 1, \ldots, n)$. Then,

$$\begin{aligned} \sum_{i=1}^{n} a_i \otimes b_i &= \left(\sum_{i=1}^{n} a_i b_i\right) \otimes 1 - \sum_{i=1}^{n} (a_i \otimes 1) \cdot \Big((b_i \otimes 1) - (1 \otimes b_i)\Big) \\ &= \sum_{i=1}^{n} (-a_i \otimes 1) \cdot \Big((b_i \otimes 1) - (1 \otimes b_i)\Big). \end{aligned}$$

Proposition 3.3 (Prop. II.1.1, [DI71])**.** *Let R be a commutative ring and A an R-algebra. Then, the following are equivalent:*

(1) *A is projective as a left A^{e}-module,*

(2) *the sequence in* (2) *splits as a sequence of left A^{e}-modules, and*

(3) *there is an element $e \in A^{\mathrm{e}}$ satisfying $\mu(e) = 1$ and $\ker(\mu) \cdot e = 0$.*

Definition 3.4. Let R be a commutative ring. An R-algebra A is *separable over R*, or *R-separable*, when A satisfies one of the conditions in Proposition 3.3.

An element in A^{e} for which (3) holds in Proposition 3.3 will be called a *separability idempotent for A*. Because $e - 1 \in \ker(\mu)$, the separability idempotent satisfies $(e - 1) \cdot e = 0$ so e is an idempotent, which justifies the name.

Example 3.5. It is easy to check that R is separable over R with 1 as separability idempotent.

Example 3.6. Let R be a nonzero commutative ring, and consider $A = \mathbf{M}_n(R)$ for some $n \in \mathbb{Z}_{\geq 1}$. Let $E_{ij} \in A$ be the matrix with a 1 in the (i,j)th entry and 0 elsewhere ($1 \leq i, j \leq n$). Define for every $j \in \{1, \ldots, n\}$,

$$e_j = \sum_{i=1}^{n} E_{ij} \otimes E_{ji} \quad \in A^{\mathrm{e}}.$$

First,

$$\mu(e_j) = \sum_{i=1}^{n} E_{ij}E_{ji} = \sum_{i=1}^{n} E_{ii} = \mathbb{I}_n,$$

and for $k, \ell \in \{1, \ldots, n\}$,

$$(E_{k\ell} \otimes 1)e_j = \sum_{i=1}^{n} (E_{k\ell}E_{ij}) \otimes E_{ji} = E_{kj} \otimes E_{j\ell} = \sum_{i=1}^{n} E_{ij} \otimes (E_{ji}E_{k\ell}) = (1 \otimes E_{k\ell})e_j.$$

Since any matrix is an R-linear combination of the E_{ij}, it follows that $\ker(\mu) \cdot e_j = 0$, so $e_1, \ldots, e_n$ are distinct separability idempotents for $\mathbf{M}_n(R)$, which shows $\mathbf{M}_n(R)$ is separable over R.

An important example of commutative separable R-algebras is given by the following proposition (cf. [For17, Prop. 4.6.1], [Sal99, Prop. 2.16]). Below, we give a more elementary proof than found in [For17, Prop. 4.6.1].

Proposition 3.7. *Let R be a commutative ring, and $f(t) \in R[t]$ a monic polynomial. Then $A = R[t]/(f(t))$ is separable over R if and only if $(f(t), f'(t)) = R[t]$.*

Proof. First, one can check that the proposition is true for $f = 1$ since A is the zero ring in this case, and $(1) = R[t]$, so let us assume $f \neq 1$.

Observe that $A^{\mathrm{e}} \cong R[X,Y]/(f(X), f(Y))$, and – using this isomorphism – an element $e(X,Y) \in A^{\mathrm{e}}$ satisfies $\mu(e) = 1$ and $\ker(\mu) \cdot e = 0$ iff $e(t,t) = 1$ in A and $(X - Y)e(X,Y) \in (f(X), f(Y))$ holds.

It can be shown by induction that for any polynomial $p(t) \in R[t]$ and *monic* polynomial $d(t)$, there exist unique $q(t), r(t)$ such that $\deg(r) < \deg(d)$ and $p(t) = q(t) \cdot d(t) + r(t)$ hold. Since $f(X) - f(Y)$ has $X = Y$ as a solution, $f(X) - f(Y)$ is divisible by $X - Y$ so let us take $g(X,Y) \in R[X,Y]$ such that

$$f(X) - f(Y) = g(X,Y) \cdot (X - Y)$$

holds. Now by considering the leading terms in X, one finds that the polynomial $g(X,Y)$ is monic in X and of degree $\deg(f) - 1$ in X. Moreover, taking the formal derivative with respect to X yields $f'(X) = g(X,Y) + (X - Y) \cdot \dfrac{\partial g(X,Y)}{\partial X}$, and by substituting X and Y with t, we see that $g(t,t) = f'(t)$ holds.

Now, when $(f(t), f'(t)) = R[t]$ holds, there is a polynomial $a(t) \in R[t]$ such that $a(t)f'(t) \equiv 1 \pmod{f(t)}$ in A. One may check that $a(X) \cdot g(X,Y)$ is a separability idempotent for A and this shows that A is separable over R.

Conversely, suppose A is R-separable. Then there is a polynomial $e(X,Y) \in R[X,Y]$ such that $e(t,t) \equiv 1 \pmod{f(t)}$ and $(X - Y)e(X,Y) \in (f(X), f(Y))$. Upon dividing $e(X,Y)$ by $g(X,Y)$, there are polynomials $a(X,Y), b(X,Y) \in R[X,Y]$ such that

$$e(X,Y) = a(X,Y) \cdot g(X,Y) + b(X,Y),$$

with $\deg_X(b) < \deg(f) - 1$. Multiplying both sides by $X - Y$, it follows that $(X - Y)b(X,Y) \in (f(X), f(Y))$. Since $(X - Y)b(X,Y)$ has degree at most $\deg(f) - 1$ as a polynomial in X, we even have $(X - Y)b(X,Y) \in (f(Y))$. When we take the formal derivative of $(X - Y)b(X,Y)$ with

respect to X, we see that $b(X,Y) + (X-Y)\dfrac{\partial b(X,Y)}{\partial X} \in (f(Y))$ holds so we have $b(t,t) = 0$ in A. Hence,

$$1 \equiv e(t,t) \equiv a(t,t)g(t,t) + b(t,t) \equiv a(t,t)f'(t) \qquad (\text{mod } f(t)),$$

which shows that $(f(t), f'(t)) = R[t]$. □

Given a separable R-algebra A, any quotient ring of A is separable by the following simple result.

Proposition 3.8. *Let A be a separable R-algebra over a commutative ring R and $I \subset A$ a two-sided ideal. Then A/I is separable over R.*

Proof. Let $e \in A^{\mathrm{e}}$ be a separability idempotent for A, let $\pi\colon A^{\mathrm{e}} \to (A/I)^{\mathrm{e}}$ be the ring homomorphism induced by $(a,b) \mapsto (a+I) \otimes (b+I)$ and let μ, μ' be the multiplication maps of A and A/I respectively.

Then it is clear that $\mu'(\pi(e)) = \mu(e) + I = 1$ and for any $a \in A$ we have

$$((a+I) \otimes 1)\pi(e) = \pi((a \otimes 1)e) = \pi((1 \otimes a)e) = (1 \otimes (a+I))\pi(e).$$

Hence, $\ker(\mu') \cdot \pi(e) = (0)$ which shows that $\pi(e)$ is a separability idempotent for A/I. □

The following proposition shows that a finite product of separable R-algebras is separable over R.

Proposition 3.9 (cf. [KO74, Prop. III.1.7(c)])**.** *Let R be a commutative ring and A, B be R-algebras. Then $A \times B$ is R-separable if and only if A is R-separable and B is R-separable.*

Proof. Suppose $A \times B$ is R-separable. By combining Proposition 3.8 and the canonical projection morphism $A \times B \to A$, it follows that A is R-separable. Similarly, B is also R-separable.

Conversely suppose A is R-separable with $s_A\colon A \to A^{\mathrm{e}}$ a splitting of the exact sequence in (2), with $\mu_A\colon A^{\mathrm{e}} \to A$ the multiplication map on A^{e}, and let $s_B\colon B \to B^{\mathrm{e}}$ be a section of the multiplication map $\mu_B\colon B^{\mathrm{e}} \to B$, i.e. s_B is a B^{e}-linear morphism and $\mu_B \circ s_B = \mathrm{id}_B$. Then, this naturally produces an $(A \times B)^{\mathrm{e}}$-linear map

$$\begin{aligned} s\colon (A \times B) &\to A^{\mathrm{e}} \times B^{\mathrm{e}}, \\ (a,b) &\mapsto (s_A(a), s_B(b)). \end{aligned}$$

Composing s with the canonical injection $\iota\colon A^{\mathrm{e}} \times B^{\mathrm{e}} \to (A \times B)^{\mathrm{e}}$, yields a section of the multiplication map $\mu\colon (A \times B)^{\mathrm{e}} \to A \times B$, as for any $r \in A^{\mathrm{e}}$ and $r' \in B^{\mathrm{e}}$ we have $(\mu \circ \iota)(r, r') = (\mu_A(r), \mu_B(r'))$. Therefore, (2) in 3.3 is satisfied. □

Definition 3.10. A ring A is a *separable ring*, or *separable*, if A is separable over $\mathbb{Z}$.

The following proposition will be used often, which states that separability is transitive in the sense as described below.

Proposition 3.11 (Transitivity of Separability, cf. [DI71, Prop. II.1.12])**.** *Let R be a commutative ring, S be a commutative, separable R-algebra and A a separable S-algebra. Then A is naturally an R-algebra and A is R-separable.*

On the other hand, if A is a separable R-algebra and S is an R-subalgebra of $\mathrm{Z}(A)$, then A is separable over S.

Moreover, given an R-separable R-algebra A and a commutative R-algebra S, the S-algebra $A \otimes_R S$ is S-separable. This is a simple corollary of the following proposition.

Proposition 3.12 ([DI71, Prop. II.1.6]). *Let R be a commutative ring and let S_1 and S_2 commutative R-algebras. Let A_1 be a separable S_1-algebra and A_2 a separable S_2-algebra. Then $A_1 \otimes_R A_2$ is a separable $S_1 \otimes_R S_2$-algebra under the operation induced by $(s_1 \otimes s_2)\cdot(a_1 \otimes a_2) = (s_1 \cdot a_1) \otimes (s_2 \cdot a_2)$.*

An important property of separable algebras is the "lifting property" of modules.

Proposition 3.13 ([DI71, Prop. II.2.3]). *Let R be a commutative ring, A an R-algebra and M a left A-module. If M is projective under its induced R-structure, then M is projective as A-module.*

For more on separability, we refer the reader to [DI71, Chapter II] and [For17, Chapter 4].

3.2 Finite separable rings

In this section, we determine which finite rings are separable over $\mathbb{Z}$. As we will see in Theorem 3.21, finite separable rings can be described very explicitly.

Before looking at separable rings, we look at the 'semisimple rings', which are classified precisely. In the case of finite rings, any semisimple ring turns out to be separable.

In ring theory, the Wedderburn-Artin theorem (see e.g. [Lam01, Thm. (3.5)]) is a celebrated result that classifies semisimple rings. Theorem (4.14) in [Lam01] states that a ring R is semisimple if and only if R is left Artin and $\mathrm{rad}(R) = 0$.

Theorem 3.14 (Wedderburn-Artin). *Let R be a semisimple ring. Then,*

$$R \cong \mathbf{M}_{n_1}(D_1) \times \mathbf{M}_{n_2}(D_2) \times \ldots \times \mathbf{M}_{n_r}(D_r)\,,$$

for suitable division rings $D_1, \ldots, D_r$ and $n_1, \ldots, n_r \in \mathbb{Z}_{\geq 1}$. The number r is uniquely determined as well as the pairs $(n_1, D_1), \ldots, (n_r, D_r)$ up to permutation and isomorphism of the division rings. Moreover, there are exactly r simple left R-modules up to isomorphism.

In addition, any ring of this form is semisimple.

Wedderburn's little theorem ([Lam01, Thm. (13.1)]) states that any finite division ring is a finite field. Therefore, a finite semisimple ring is a product of matrix rings over finite fields by the above theorem. The finite fields are separable rings and even any finite semisimple ring is separable.

Corollary 3.15. *Any finite semisimple ring R is separable.*

Proof. By the Wedderburn-Artin theorem, there is an isomorphism

$$R \cong \prod_{i=1}^{r} \mathbf{M}_{n_i}(k_i)\,,$$

for certain finite fields k_i and $n_i \in \mathbb{Z}_{\geq 1}$ $(i = 1, \ldots, r)$.

Consider a finite field k of characteristic p and of size p^n (so $n \in \mathbb{Z}_{\geq 1}$). Now the prime subfield $\mathbb{F}_p$ is separable by Proposition 3.8. Moreover, $k \cong \mathbb{F}_p[X]/(f(X))$ for some monic irreducible polynomial $f(X) \in \mathbb{F}_p[X]$ of degree n satisfying $(f, f') = \mathbb{F}_p[X]$, so k is separable over $\mathbb{F}_p$ by Proposition 3.7. As shown in example 3.6, $\mathbf{M}_{n_i}(k)$ is separable over k for $i = 1, \ldots, r$.

Hence by the transitivity of separability, $\mathbf{M}_{n_i}(k_i)$ is separable for all $i = 1, \ldots, r$. Moreover, products of separable rings are separable again by Proposition 3.9. Therefore, R is separable. □

Not all finite separable rings are, however, semisimple. For example $\mathbb{Z}/n\mathbb{Z}$ is a separable ring, but is not semisimple when $n \in \mathbb{Z}_{\geq 2}$ is not squarefree.

Now we will introduce truncated *Witt rings*, which will turn out to be separable but not necessarily semisimple.

Definition 3.16. Let k be a finite field of characteristic p and let $e \in \mathbb{Z}_{\geq 1}$. An *$e$-truncated Witt ring of k* is a pair (R, φ) with R a ring of the form

$$(\mathbb{Z}/p^e\mathbb{Z})[X]/(g(X)),$$

where $g(X)$ is irreducible modulo p with $\deg(g) = [k : \mathbb{F}_p]$, and φ is a surjective ring homomorphism from R to k.

Remark 3.17. There is a simple and precise description of the ideals of e-truncated Witt rings. Let R be an e-truncated Witt ring of k, with the notation as above. Because $p \in R$ is nilpotent any maximal ideal contains pR. Moreover, φ induces an isomorphism $R/pR \xrightarrow{\sim} k$ so pR is the unique maximal ideal of R. This shows that for any element $x \in R$ there exists a unique $i \in \{0, \ldots, e\}$ such that $x = p^i u$ for some $u \in R^*$. As a consequence, the ideals of the form (p^f) with $1 \leq f \leq e$ give all proper ideals of R.

Proposition 3.18. *Let k be a finite field, (R, φ) an e-truncated Witt ring of k, let $p = \mathrm{char}(k)$ and $e \in \mathbb{Z}_{\geq 1}$.*

Given any finite commutative local $\mathbb{Z}/p^e\mathbb{Z}$-algebra A with maximal ideal $\mathfrak{m}$ and a ring homomorphism $f\colon k \to A/\mathfrak{m}$, there exists a unique ring homomorphism $F\colon R \to A$ such that the diagram

$$\begin{array}{ccc} R & \overset{F}{\dashrightarrow} & A \\ \downarrow{\scriptstyle \varphi} & & \downarrow \\ k & \xrightarrow{f} & A/\mathfrak{m}, \end{array}$$

commutes.

Proof. Suppose R is given by $(\mathbb{Z}/p^e\mathbb{Z})[X]/(g(X))$ with g monic and irreducible modulo p. Then, $R/pR = \mathbb{F}_p[\overline{X}]/(\overline{g}(\overline{X}))$. Note that there is a one-to-one correspondence between ring homomorphisms $F\colon R \to A$ that make the diagram commute and roots $\alpha \in A$ of $g(X)$ for which $\alpha + \mathfrak{m} = f(\overline{X})$.

Take an arbitrary $r_0 \in A$ such that $r_0 + \mathfrak{m} = f(\overline{X})$ in $A/\mathfrak{m}$. Then, $g(r_0) \in \mathfrak{m}$ and $g'(r_0) \in A^*$ because $\overline{g}$ is a separable polynomial in $\mathbb{F}_p[\overline{X}]$. By applying Newton iteration, r_0 can be refined to a unique $\alpha \in A$ such that $g(\alpha) = 0$ and $\alpha + \mathfrak{m} = f(\overline{X})$. The unique ring homomorphism is now given by $R \to A,\ X \mapsto \alpha$. □

Remark 3.19. Witt rings are uniquely unique in the following sense. Suppose $(R_1, \varphi_1), (R_2, \varphi_2)$ are e-truncated Witt rings of a finite field k. Then there is a unique isomorphism $\psi\colon R_1 \to R_2$ such that $\varphi_1 = \varphi_2 \circ \psi$.

Using Proposition 3.18, we get unique morphisms $\psi\colon R_1 \to R_2$ and $\chi\colon R_2 \to R_1$ that reduce to the identity on k. Now, by making use of the uniqueness, Proposition 3.18 shows with R_1 in the role of R and A that $\chi \circ \psi = \mathrm{id}_{R_1}$, and similarly $\psi \circ \chi = \mathrm{id}_{R_2}$. Hence ψ is the *unique* isomorphism from R_1 to R_2 with $\varphi_1 = \varphi_2 \circ \psi$.

By the preceding remark, for any finite field k and $e \in \mathbb{Z}_{\geq 1}$ we can make a choice $(\mathrm{W}_e(k), \varphi)$ for an e-truncated Witt ring of k and say $\mathrm{W}_e(k)$ is *the* e-truncated Witt ring of k, where the choice for the map $\varphi\colon \mathrm{W}_e(k) \to k$ is implicit but nevertheless fixed.

Note 3.20. Proposition 3.18 may not hold when A is not commutative. Let $k = \mathbb{F}_2[\alpha]$ where $\alpha \in k$ satisfies $f(\alpha) = 0$ with $f(X) = X^2 + X + 1 \in \mathbb{F}_2[X]$, and let $\sigma\colon k \to k, x \mapsto x^2$ be the Frobenius endomorphism. Consider the ring $A = k[\varepsilon; \sigma]/(\varepsilon^2)$, with the rule $\varepsilon a = \sigma(a)\varepsilon$ for $a \in k$. Now f has α and $\alpha + \varepsilon$ as roots in A that reduce to α modulo $A\varepsilon$, the unique maximal left ideal of A. The 1-1 correspondence yields two distinct ring homomorphisms from k to A that are the identity on k after composing with the reduction morphism $A \to A/A\varepsilon$.

The Witt rings are the building blocks of finite separable rings, as the following theorem shows.

Theorem 3.21 (Structure theorem of finite separable rings)**.** *Finite separable rings are exactly the rings of the form*

$$\prod_{i=1}^{r} \mathbf{M}_{n_i}(\mathrm{W}_{e_i}(k_i)), \tag{3}$$

for some $r \in \mathbb{Z}_{\geq 0}$ where $n_i, e_i \in \mathbb{Z}_{\geq 1}$ and k_i are finite fields ($i = 1, \ldots, r$).

Proof. First, we will show that any Witt ring of the form

$$\mathrm{W}_e(k) = (\mathbb{Z}/p^e\mathbb{Z})[X]/(g(X))$$

is separable, where k is a finite field of characteristic p. Because $(\overline{g}, \overline{g}') = \mathbb{F}_p[X]$, there is an element $u \in (g, g')$ such that $u \in 1 + p(\mathbb{Z}/p^e\mathbb{Z})[X]$. Since p is nilpotent, u is a unit and $(g, g') = (\mathbb{Z}/p^e\mathbb{Z})[X]$. Using Proposition 3.7, the ring $\mathrm{W}_e(k)$ is separable over $\mathbb{Z}/p^e\mathbb{Z}$ and $\mathbb{Z}/p^e\mathbb{Z}$ is a separable ring by Proposition 3.8. Hence $\mathrm{W}_e(k)$ is a separable ring by transitivity.

From example 3.6 and transitivity, each term in (3) is separable. Hence any ring of the form in (3) is a separable ring by Proposition 3.9.

Conversely, let R be a finite separable ring.

Suppose first that in addition, R is connected. Theorem 6.2.62 in [CT16] shows that any finite connected separable ring is a matrix ring over a Witt ring, so $R \cong \mathbf{M}_n(\mathrm{W}_e(k))$ for $n, e \geq 1$ and k a finite field, shows that R is of the desired form.

Now, let us not assume that R is connected anymore. Then Proposition (22.2) in [Lam01] says that a left Artin ring R has a ring decomposition

$$R = c_1 R \times c_2 R \times \ldots \times c_r R,$$

where $r \in \mathbb{Z}_{\geq 1}$ and $c_i \in R$ are *centrally primitive* idempotents, i.e. every c_i is a nonzero central idempotent and c_i cannot be written as a sum of two nonzero central idempotents. In our case, R is a finite product of connected rings. By Proposition 3.9, the finite connected ring $c_i R$ is separable for $i \in \{1, \ldots, r\}$ so R is of the form as in (3). □

As $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ do not commute, $\mathbf{M}_n(R)$ is not commutative for any $n \geq 2$ and any R not the zero ring. This yields the following corollary.

Corollary 3.22. *Any finite commutative separable ring is a finite product of truncated Witt rings. Moreover, any such finite product of truncated Witt rings is a separable commutative ring.*

The Jacobson radical of a separable subring of a finite ring R is well understood, as the following lemma shows.

Lemma 3.23. *Let R be a finite ring and $S \subseteq R$ a separable subring. Then,* $\mathrm{rad}(S) = \mathrm{rad}(R) \cap S$.

Proof. By Theorem 2.10, the radical of R is nilpotent, so $\mathrm{rad}(R) \cap S$ is a nil left ideal in S. Hence by Remark 2.9, we have the inclusion $\mathrm{rad}(R) \cap S \subseteq \mathrm{rad}(S)$.

Conversely, by Theorem 3.21 we have

$$S \cong \prod_{i=1}^{r} \mathbf{M}_{n_i}(\mathrm{W}_{e_i}(k_i)), \tag{4}$$

for $n_i, e_i, \in \mathbb{Z}_{\geq 1}$ and finite fields k_i for $i = 1, \ldots, r$. Remark 3.17 shows that for a finite field k and $e \in \mathbb{Z}_{\geq 1}$, we have $\mathrm{rad}(\mathrm{W}_e(k)) = \mathrm{char}(k) \cdot \mathrm{W}_e(k)$, and $\mathrm{rad}(\mathbf{M}_n(\mathrm{W}_e(k))) = \mathrm{char}(k) \cdot \mathbf{M}_n(\mathrm{W}_e(k))$ follows by Example (7) in §4 of [Lam01].

Hence $\mathrm{rad}(S)$ corresponds under the isomorphism in (4) with

$$\prod_{i=1}^{r} \mathrm{char}(k_i) \cdot \mathbf{M}_{n_i}(\mathrm{W}_{e_i}(k_i))\,,$$

so we see that $\mathrm{rad}(S) = S \cdot n_0$ where $n_0 = \left(\prod_{p|\mathrm{char}(S)} p\right)$. Note that the natural number n_0 is nilpotent and central in R, so $R \cdot \mathrm{rad}(S) = R \cdot n_0 \subseteq \mathrm{rad}(R)$ holds, which shows the other inclusion, $\mathrm{rad}(S) \subseteq \mathrm{rad}(R) \cap S$. □

4 Maximal separable subrings

Consider a ring R. A separable subring $S \subseteq R$ is *maximal* if any separable subring $S' \subseteq R$ that contains S, is equal to S. If R is not separable, a natural question is to ask if there exists a unique maximal separable subring of R. In this section, we will prove the main result of our thesis, which is Theorem 1.2. But first we present a simple proof of this theorem in the case that the ring is commutative.

4.1 Commutative case

To answer this question, for a commutative ring R, this question can be answered positively if we allow ourselves to impose a finiteness condition on R.

Theorem 4.1. *Let R be a commutative ring and let A be a commutative R-algebra, such that A is Noetherian as an R-module, i.e., every ascending chain of submodules of A stabilizes. Then, A has a unique maximal R-separable R-subalgebra.*

Proof. Consider the partially ordered set $\mathcal{P}$ of R-subalgebras of A that are separable over R, ordered by inclusion. Note that the image of the structure morphism is a separable subring of A by Proposition 3.8, so $\mathcal{P}$ is not empty. As A is a Noetherian R-module, any ascending chain in $\mathcal{P}$ must stabilize so there exists a maximal element in $\mathcal{P}$.

Suppose S, S' are maximal elements in $\mathcal{P}$. The R-bilinear morphism $S \times S' \to A, (a, b) \mapsto ab$ induces a ring homomorphism $f\colon S \otimes_R S' \to A$. By Proposition 3.12, the tensor product $S \otimes_R S'$ is separable over R. Using Proposition 3.8, the image of the tensor product, $f(S \otimes_R S') \cong (S \otimes_R S')/\ker(f)$, is separable over R and contains $S \cup S'$. Thus, by maximality we conclude $S = f(S \otimes_R S') = S'$. □

Any finite commutative ring R is naturally a $\mathbb{Z}$-algebra, so we can deduce the following corollary directly from Theorem 4.1.

Corollary 4.2. *Let R be a finite commutative ring. Then there is a unique separable subring $S \subset R$ such that any separable subring of R is contained in S.*

4.2 Statement of theorem

If R is a finite ring, there may be two distinct maximal separable subrings of R, as the following example illustrates.

Example 4.3. Let $R = \mathbb{F}_2[\varepsilon]$ where ε satisfies $\varepsilon^2 = 0$. Then, the ring $\mathbf{M}_2(R)$ has $\mathbf{M}_2(\mathbb{F}_2)$ as a separable subring. The matrix

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

satisfies $M^2 = \mathbb{I}_2$ so the morphism $f\colon \mathbf{M}_2(R) \to \mathbf{M}_2(R), x \mapsto MxM$ is an automorphism with itself as inverse. Thus, $M \cdot \mathbf{M}_2(\mathbb{F}_2) \cdot M$ is a separable subring isomorphic to $\mathbf{M}_2(\mathbb{F}_2)$, but not equal to $\mathbf{M}_2(\mathbb{F}_2)$ because $M \left[\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right] M = \left[\begin{smallmatrix} 1 & \varepsilon \\ 0 & 0 \end{smallmatrix}\right] \notin \mathbf{M}_2(\mathbb{F}_2)$.

Suppose $\mathbf{M}_2(\mathbb{F}_2) \subset B \subset \mathbf{M}_2(R)$ for some ring B. Then one can show that $B \cong \mathbf{M}_2(B')$ for some $\mathbb{F}_2 \subseteq B' \subseteq R$. Looking at the sizes of the rings, either $B' = R$ or $B' = \mathbb{F}_2$ holds. This shows that $\mathbf{M}_2(\mathbb{F}_2)$ is a maximal separable subring, as well as $M \cdot \mathbf{M}_2(\mathbb{F}_2) \cdot M$.

For a ring R, the unit group of R acts on the set of separable subrings of R, by the group of inner automorphisms,

$$\mathrm{Inn}(R) = \{\, \varphi_u\colon x \mapsto uxu^{-1} \mid u \in R^* \,\} \quad \subseteq \mathrm{Aut}(R),$$

where a unit u sends a separable subring $S \subseteq R$ to $\varphi_u(S)$, which may be different from S when R is not commutative. Two separable subrings $S, T \subseteq R$ are *conjugate by* R^* if there exists $u \in R^*$ such that $S = \varphi_u(T)$. We are now ready to state an important theorem of this thesis.

Theorem 4.4 (Unique maximal subring)**.** *Let R be a finite ring. Then, there exists a maximal separable subring $S \subseteq R$ and any two maximal separable subrings of R are conjugate by R^*.*

The proof will be given at the end of this section. In order to prove this theorem, we will use a different notion of 'maximality'.

Definition 4.5. Let R be a finite ring. A separable subring S of R is *radical-maximal* if the natural map $S \to R/\mathrm{rad}(R)$ is surjective.

Note that a separable subring $S \subseteq R$ is radical-maximal if and only if $S + \mathrm{rad}(R) = R$.

Existence of a radical-maximal separable subring of a finite ring will be shown in Lemma 4.13 and Lemma 4.15 shows uniqueness. Then it follows from Lemma 4.16 that radical-maximality is equivalent to being maximal under inclusion, from which Theorem 4.4 follows.

4.3 Local rings

As defined in §19 of [Lam01], a ring R is local if $R/\mathrm{rad}(R)$ is a division ring, and it is shown in [Lam01] that R is local if and only if it contains exactly one maximal left ideal $\mathfrak{m}$.

In commutative ring theory, local rings play an important role, as any commutative Artin ring is a finite product of local Artin rings (cf. [AM69, (8.7)]) and one can localize at any prime ideal of a ring to get a local ring. For a field k of infinite cardinality, the left Artin ring $\mathbf{M}_2(k)$ has an infinite number of maximal left ideals of the form $I_\alpha = \{ \left[\begin{smallmatrix} a & \alpha a \\ b & \alpha b \end{smallmatrix}\right] \mid a, b \in k \}$ with $\alpha \in k^*$ so $\mathbf{M}_2(k)$ cannot be a finite product of local Artin rings. Moreover, the theory of localization does not easily generalize to noncommutative rings as mentioned just before [Lam01, (20.3)]. Nevertheless, local rings are encountered in the study of endomorphism rings of certain modules over rings that may or may not be commutative. Local rings will be important for us as they are 'easy' to work with and separable subrings of finite local rings are of a simple form.

Theorem 4.6. *Let R be a finite local ring. Then, R has a radical-maximal separable subring and any two of them are conjugate by an inner automorphism of R.*

Note that the special case where R is also assumed to be commutative is Theorem 6.3.1 in [BF12].

Before we prove this theorem, we will make use of the following result from group theory, which can be found in [Rob96, (9.1.2)].

Theorem 4.7 (Schur-Zassenhaus)**.** *Let N be a normal subgroup of a finite group G. Assume that $|N|$ and $m = [G : N]$ are relatively prime. Then G contains a subgroup of order m. Moreover, if N is solvable or G/N is solvable, then any two subgroups of order m are conjugate in G.*

Note that in fact N or G/N is solvable under the preceding assumptions since $|N|$ and m cannot both be even and the Feit-Thompson theorem ([FT63]) states that any finite group of odd order is solvable. For proving Theorem 4.6 it is sufficient to use a weaker version of Schur-Zassenhaus, which has an elementary proof.

Theorem 4.8. *Let N be a normal subgroup of a finite group G such that G/N is cyclic and assume $|N|$ and $m = |G/N|$ are relatively prime. Then G contains a subgroup of order $|G/N|$ and any two subgroups of order $|G/N|$ are conjugate in G.*

Proof. First, take an element $g \in G$ that maps to an element in G/N of order m. Then, $g^{|N|}$ generates a subgroup of G of order dividing m by Lagrange's theorem. Since m and $|N|$ are coprime, it follows that $\mathrm{ord}\left(g^{|N|}\right) = m$ so the natural map $\langle g^{|N|} \rangle \to G/N$ is an isomorphism.

To show any two subgroups of order $|G/N|$ are conjugate, we perform induction on the order of G/N. The theorem obviously holds if G/N is the trivial group.

Now let G, N be given with G/N cyclic of order $m \geq 2$ and assume the theorem is correct for all G', N' of order $< m$, and suppose H_1 and H_2 are two subgroups of G of order $|G/N|$. Then, as H_1 and N have coprime orders, their intersection is trivial, so $H_1 \to G/N$ is an isomorphism showing H_1 is cyclic and similarly H_2 is cyclic. Take a prime divisor p of m and write $m = p^a \cdot m'$ where $a \in \mathbb{Z}_{\geq 1}$ and $p \nmid m'$. Now any Sylow-p-group of H_1 or H_2 is a Sylow-p-group of G. Since any two Sylow-p-groups of G are conjugate, we may assume now that there is a Sylow-p-group S contained in H_1 and H_2 by performing the conjugation on H_2. Consider the group $G' = \mathrm{C}_G(S)$, the centralizer of S in G. The group G' contains S as a normal subgroup and contains H_1, H_2 because these groups are cyclic so abelian. We now may use the induction hypothesis on $N' = \mathrm{im}\,(N \cap G' \to G'/S)$ and G'/S. By the induction hypothesis, H_1/S and H_2/S are conjugate by some $gS \in G'/S$ for some $g \in G'$. Now $(H_1/S) = (gS)(H_2/S)(gS)^{-1}$ implies that $H_1 = gH_2g^{-1}$ as S is central in G'. $\square$

Proof of Theorem 4.6. Let $\mathfrak{m}$ be *the* maximal left ideal of R, which is a two-sided ideal because $\mathfrak{m} = \mathrm{rad}(R)$ holds. By [Lam01, Thm. (19.1)], the quotient $R/\mathfrak{m}$ is a finite division ring so it is a finite field because of Wedderburn's little theorem. Write $k = R/\mathfrak{m}$, let $p = \mathrm{char}(k)$ and $q = |k|$.

The reduction map $f\colon R^* \to (R/\mathfrak{m})^*$ is surjective because any $u \in R$ reducing to a nonzero element in $R/\mathfrak{m}$ is in $R \setminus \mathfrak{m} = R^*$. The kernel of f is $1 + \mathfrak{m}$ so the sequence

$$1 \longrightarrow 1 + \mathfrak{m} \longrightarrow R^* \xrightarrow{f} k^* \longrightarrow 1 \tag{5}$$

is a short exact sequence of finite groups.

For any $i \geq 1$, the R-module $\mathfrak{m}^i/\mathfrak{m}^{i+1}$ is a k-vector space. Because $\mathfrak{m}$ is nilpotent by Theorem 2.10, it is easy to see that $|\mathfrak{m}|$ is a power of q which shows that $1 + \mathfrak{m}$ is a p-group. Moreover, we have $\mathrm{char}(R) = p^e$ for some $e \in \mathbb{Z}_{\geq 1}$ since $p \in \mathfrak{m}$.

Clearly, $1 + \mathfrak{m}$ is a normal subgroup of R^* with order coprime to $|k^*| = q - 1$, so the Schur-Zassenhaus Theorem and Theorem 4.8 apply.

Existence: Let $G \subseteq R^*$ be a subgroup of order $q - 1$. Then, G is isomorphic to k^* so G is cyclic. Take a generator $x \in G$ and consider the commutative ring $R' = (\mathbb{Z}/p^e\mathbb{Z})[x] \subseteq R$.

The natural map $R' \to k$ is surjective by choice of x so the kernel of this map, $R' \cap \mathfrak{m}$, is a nilpotent maximal ideal. This shows that R' is local with maximal ideal $R' \cap \mathfrak{m}$. Moreover, there is a surjective morphism

$$(\mathbb{Z}/p^e\mathbb{Z})[X]/\big(X^{q-1} - 1\big) \to R',$$

by sending X to x. We may use Proposition 3.7 with the polynomial $g(X) = X^{q-1} - 1$ since

$$(g(X),\, g'(X)) = \big(X^{q-1} - 1,\, X^{q-2}\big) = (\mathbb{Z}/p^e\mathbb{Z})[X],$$

where we used that $q - 1$ is a unit in $\mathbb{Z}/p^e\mathbb{Z}$. This shows that $(\mathbb{Z}/p^e\mathbb{Z})[X]/(g(X))$ is separable over $\mathbb{Z}/p^e\mathbb{Z}$ and by transitivity, $(\mathbb{Z}/p^e\mathbb{Z})[X]/(g(X))$ is separable. As a consequence R' is separable by Proposition 3.8 and R' is radical-maximal because $R' \to k$ is surjective.

Uniqueness: Suppose now $S, T \subseteq R$ are two radical-maximal separable subrings of R. Similar to how we showed that R' is local, S and T are local with maximal ideals $S \cap \mathfrak{m}$ and $T \cap \mathfrak{m}$ respectively, because $S \to k$ and $T \to k$ are surjective maps.

By Theorem 3.21, the ring S is isomorphic to a matrix ring over a Witt ring. More specifically, because $S/\mathrm{rad}(S) \cong k$ must hold and S has characteristic p^e, we have $S \cong \mathrm{W}_e(k)$. Similarly, for T we have $T \cong \mathrm{W}_e(k)$.

By Definition 3.16, there exists $\alpha \in R$ such that $S = (\mathbb{Z}/p^e\mathbb{Z})[\alpha]$. Now, using the existence from above for the local ring S in the role of R, there exists $\beta \in S^*$ such that β has order $q - 1$ in S^* and the ring $(\mathbb{Z}/p^e\mathbb{Z})[\beta] \subseteq S$ is local and a radical-maximal separable subring of S. Because $(\mathbb{Z}/p^e\mathbb{Z})[\beta]$ surjects onto k, we again get that $(\mathbb{Z}/p^e\mathbb{Z})[\beta] \cong \mathrm{W}_e(k)$ so this yields $(\mathbb{Z}/p^e\mathbb{Z})[\beta] = S$ where β has order $q - 1$.

Similarly we can find a $\gamma \in R^*$ such that $T = (\mathbb{Z}/p^e\mathbb{Z})[\gamma]$ where γ has order $q-1$ in T^*. In both cases, $\langle\beta\rangle$ and $\langle\gamma\rangle$ are subgroups of R^* of order $q-1$. Therefore, by the Schur-Zassenhaus Theorem, there exists $u \in R^*$ such that $\langle\gamma\rangle = u\langle\beta\rangle u^{-1}$. This shows that

$$T = (\mathbb{Z}/p^e\mathbb{Z})[\gamma, \gamma^2, \ldots, \gamma^{q-1}] = u \cdot (\mathbb{Z}/p^e\mathbb{Z})[\beta, \beta^2, \ldots, \beta^{q-1}] \cdot u^{-1} = uSu^{-1}.$$

□

4.4 Radical-maximal subrings

Given the results found for finite local rings, we want to extend the theorem to arbitrary finite rings. The key point is that we can see the ring as a module over itself so that we can decompose this module into a direct sum of indecomposable modules.

Recall that a left R-module M is of *finite (composition) length* whenever any ascending chain of submodules in M stabilizes and any descending chain of submodules in M stabilizes. In particular, by the Hopkins-Levitzki theorem (cf. [Lam01, (4.19)]), any finitely generated left module over a left Artin ring is of finite length.

Theorem 4.9 (Krull-Schmidt theorem, [Lam01, Cor. (19.22)])**.** *Let R be a ring and M a left R-module of finite length. Then there exists a decomposition*

$$M \cong M_1 \oplus M_2 \oplus \ldots \oplus M_r,$$

where each M_i is an indecomposable submodule of M. Moreover, r is uniquely determined, and the sequence of isomorphism types of $M_1, \ldots, M_r$ is uniquely determined up to a permutation.

The idea is to use Theorem 4.6 on the endomorphism ring of an indecomposable module of finite order.

Theorem 4.10 ([Lam01, Thm. (19.17)])**.** *Let R be a ring and M an indecomposable left R-module of finite length. Then* $\mathrm{End}_R(M)$ *is a local ring and its unique maximal left ideal is nil.*

Proof. Let $f \in E := \mathrm{End}_R(M)$. By Fitting's lemma (cf. [Lam01, (19.16)]), we have for sufficiently large r that the natural map $\ker(f^r) \oplus f^r(M) \to M$ is an isomorphism. In particular, one can take r equal to the length of M. Because M is indecomposable, either $\ker(f^r) = 0$ or $f^r(M) = 0$ must hold. If $f^r(M) = 0$, then f is nilpotent. Otherwise $\ker(f^r) = 0$ and $f^r(M) = M$ hold, so f is injective and $f(M) = M$, which shows that f is a unit in E. Because every nonunit is nilpotent, Proposition (19.3) in [Lam01] shows E is a local ring and any element $f \in \mathrm{rad}(E)$ satisfies $f^r = 0$, so $\mathrm{rad}(E)$ is nil. □

Moreover, the following lemma is useful.

Lemma 4.11. *Let R be a ring and M_1, M_2 be finite indecomposable left R-modules such that $M_1 \ncong M_2$. Then,* $\mathrm{Hom}_R(M_2, M_1) \circ \mathrm{Hom}_R(M_1, M_2) \subseteq \mathrm{rad}(\mathrm{End}_R(M_1))$.

Proof. Let $f \in \mathrm{Hom}_R(M_2, M_1)$ and $g \in \mathrm{Hom}_R(M_1, M_2)$ and assume that $f \circ g$ does not belong to $\mathrm{rad}(\mathrm{End}_R(M_1))$. Since $f \circ g$ is not nilpotent by Theorem 4.10, neither is $g \circ f$ as $0 \neq (f \circ g)^{n+1} = f(g \circ f)^n g$ implies $(g \circ f)^n \neq 0$. Hence $g \circ f$ and $f \circ g$ are units so there exist $v \in \mathrm{End}_R(M_1)^*$ and $u \in \mathrm{End}_R(M_2)^*$ such that $u \circ g \circ f = g \circ f \circ u = \mathrm{id}_{M_2}$ and $v \circ f \circ g = f \circ g \circ v = \mathrm{id}_{M_1}$. However now $g \circ v$ is the inverse of f:

$$g \circ v \circ f = u \circ g \circ f \circ g \circ v \circ f = u \circ g \circ f = \mathrm{id}_{M_2}.$$

This contradicts $M_1 \ncong M_2$ so $f \circ g \in \mathrm{rad}(\mathrm{End}_R(M_1))$. □

Before we prove the existence of a radical-maximal separable subring of a finite ring R, we will need to write R as a generalized matrix ring of a special kind.

Lemma 4.12. *Let R be a nonzero finite ring. Then, there exist $n \in \mathbb{Z}_{\geq 1}$, numbers $m_i \in \mathbb{Z}_{\geq 1}$ and mutually nonisomorphic indecomposable right R-modules M_i for every $i = 1, \ldots, n$ such that*

$$R_R \cong \bigoplus_{i=1}^{n} M_i^{\oplus m_i},$$

as right R-modules and such that the following statements hold:

1. *The ring R is isomorphic to the generalized matrix ring*

$$M_R := \left[\mathrm{Hom}_R\Big(M_j^{\oplus m_j}, M_i^{\oplus m_i} \Big) \right]_{i,j=1}^{n},$$

   where the multiplication is similar to the ordinary matrix multiplication but with composition (and addition) of morphisms instead.

2. *For all $i \in \{1, \ldots, n\}$, the ring $\mathrm{End}_R(M_i)$ is a finite local ring and the (i,i)th entry of M_R, with the ring structure inherited from M_R, is a ring isomorphic to $\mathbf{M}_{m_i}(\mathrm{End}_R(M_i))$.*

3. *The radical of R corresponds under the isomorphism $R \xrightarrow{\sim} M_R$ to the matrices for which the (i,i)th entry belongs to $\mathbf{M}_{m_i}(\mathrm{rad}(\mathrm{End}_R(M_i)))$ for all $i = 1, \ldots, n$.*

Proof. Since R is finite, it is certainly right Artin. The decomposition is a direct consequence of the Krull-Schmidt theorem for right modules (see Theorem 4.9).

It is easy to check that the map $R \to \mathrm{End}_R(R_R)$ given by $r \mapsto (x \mapsto rx)$ is a ring isomorphism. As the endomorphism ring of a direct sum is isomorphic to a generalized matrix ring, we get an isomorphism

$$R \xrightarrow{\sim} \mathrm{End}_R\big(M_1^{\oplus m_1} \oplus \ldots \oplus M_n^{\oplus m_n}\big) \xrightarrow{\sim} M_R.$$

Now write E_i for the (i,i)th entry of M_R. For the second statement, note that E_i is isomorphic to

$$\mathrm{End}_R\big(M_i^{\oplus m_i}\big) \cong \mathbf{M}_{m_i}(\mathrm{End}_R(M_i)),$$

and $\mathrm{End}_R(M_i)$ is a finite local ring by Lemma 4.10.

For the last statement, let us denote by $\mathfrak{a}$, the additive subgroup of M_R consisting of $(\varphi_{ij})_{i,j=1}^{n} \in M_R$ such that $\varphi_{ii} \in \mathrm{rad}(E_i)$ for all $i = 1, \ldots, n$. By applying Lemma 4.11, one can check for all $i \neq j$ that

$$\mathrm{Hom}_R\Big(M_i^{\oplus m_i}, M_j^{\oplus m_j} \Big) \circ \mathrm{Hom}_R\Big(M_j^{\oplus m_j}, M_i^{\oplus m_i} \Big) \subseteq \mathrm{rad}(E_j),$$

since the map from the kth summand to the ℓth summand of the left hand side is a finite sum of maps in $\mathrm{Hom}_R(M_i, M_j) \circ \mathrm{Hom}_R(M_j, M_i)$ for any $k, \ell \in \{1, \ldots, m_j\}$. Therefore, $\mathfrak{a}$ is a two-sided ideal of M_R.

Consider an element $\varphi = (\varphi_{ij})_{i,j=1}^{n} \in \mathfrak{a}$ and take $N \in \mathbb{Z}_{\geq 1}$ such that $\mathrm{rad}(E_i)^N = 0$ for all $i \in \{1, \ldots, n\}$. Now let $M = n \cdot N + 1$. Then, for $i, j \in \{1, \ldots, n\}$, the (i,j)th entry of φ^{M+1} is equal to

$$\big(\varphi^{M+1}\big)_{i,j} = \sum_{k_1, k_2, \ldots, k_M = 1}^{n} \varphi_{ik_1} \circ \varphi_{k_1 k_2} \circ \ldots \circ \varphi_{k_{M-1} k_M} \circ \varphi_{k_M j}. \tag{6}$$

Let $(k_1, k_2, \ldots, k_M) \in \{1, \ldots, n\}^M$ be an arbitrary vector. By the pigeonhole principle, there is a value $v \in \{1, \ldots, n\}$ that occurs at least $N + 1$ times among the k_i. Say the first occurence is at index a and the last occurence is at index b. Then,

$$\varphi_{k_a k_{a+1}} \circ \ldots \circ \varphi_{k_{b-1} k_b} \in \mathrm{rad}(E_v)^N = 0,$$

so each summand in (6) is zero, which yields $\varphi^{M+1} = 0$.

It is now clear that $\mathfrak{a}$ is a nil ideal, so it follows that $\mathfrak{a} \subseteq \mathrm{rad}(M_R)$ by Remark 2.9. Moreover, the quotient ring is given by

$$M_R/\mathfrak{a} \cong \prod_{i=1}^{n} E_i/\mathrm{rad}(E_i)\,, \tag{7}$$

which is semisimple by [Lam01, (4.6)]. Hence by [Lam01, (4.14)] and [Lam01, Ex. 4.11], we can conlude $\mathrm{rad}(M_R) = \mathfrak{a}$ holds which proves the fourth statement. □

Lemma 4.13. *Let R be a finite ring. Then there exists a radical-maximal separable subring $S \subseteq R$.*

Proof. Let us now use Lemma 4.12 and copy the notation. Let $R' \subseteq R$ be the subring corresponding under $R \xrightarrow{\sim} M_R$ to the diagonal of M_R. By Lemma 4.12 statement 2, we can write

$$R' \cong \prod_{i=1}^{n} \mathbf{M}_{m_i}(A_i)\,, \tag{8}$$

where the A_i are finite local rings for $i = 1, \ldots, n$. By Theorem 4.6, for every i, there exist radical-maximal separable subrings $S_i \subseteq A_i$.

Let S be the subring of R that is isomorphic under (8) to

$$\mathbf{M}_{m_1}(S_1) \times \ldots \times \mathbf{M}_{m_n}(S_n)\,.$$

By Example 3.6 and Proposition 3.9, the ring $S \subseteq R$ is separable. Moreover, the natural map $R'/\mathrm{rad}(R') \xrightarrow{\sim} R/\mathrm{rad}(R)$ is an isomorphism by Lemma 4.12, statement 3. Because we have $R'/\mathrm{rad}(R') \cong \prod_{i=1}^{n} \mathbf{M}_{m_i}(A_i/\mathrm{rad}(A_i))$ and $S_i \to A_i/\mathrm{rad}(A_i)$ is surjective for all $i \in \{1, \ldots, n\}$, it is easily seen that S is a radical-maximal separable subring of R. □

4.5 Uniqueness of radical-maximal subrings

In this subsection, we will prove that any two radical-maximal separable subrings of a finite ring are conjugate by R^* and that radical-maximality and being maximal under inclusion are equivalent. This will prove Theorem 4.4.

First we consider the special case that R is a finite ring for which $R/\mathrm{rad}(R)$ is a matrix ring over a finite field. There are extra assumptions which become clear in the next lemma.

Lemma 4.14. *Let $R = \mathbf{M}_n(A)$ be a finite ring, where $n \in \mathbb{Z}_{\geq 1}$ and A is a local ring with residue field k, and let S_1, S_2 be two radical-maximal separable subrings of R. Let $e_1, \ldots, e_n \in S_1 \cap S_2$ be mutually orthogonal idempotents, primitive in R, such that their sum is 1. Suppose that for all $i, j \in \{1, \ldots, n\}$ and $\varepsilon = 1, 2$, we have $e_i S_\varepsilon \cong e_j S_\varepsilon$ as right S_ε-modules. Then, there exists $u \in R^*$ such that $S_2 = uS_1u^{-1}$.*

Proof. It follows from Lemma 3.23 that $\ker(S_1 \to R/\mathrm{rad}(R)) = \mathrm{rad}(S_1)$, so the natural map

$$S_1/\mathrm{rad}(S_1) \xrightarrow{\sim} R/\mathrm{rad}(R) \cong \mathbf{M}_n(k) \tag{9}$$

is an isomorphism by radical-maximality of S_1.

Theorem 3.21 shows that a finite separable ring T with $T/\mathrm{rad}(T) \cong \mathbf{M}_n(k)$ is of the form $T \cong \mathbf{M}_n(\mathrm{W}_e(k))$, for some $e \in \mathbb{Z}_{\geq 1}$ and T will have characteristic $\mathrm{char}(k)^e$. Because $\mathrm{char}(S_1) = \mathrm{char}(R) = \mathrm{char}(S_2)$ holds, we have

$$S_1 \cong S_2 \cong \mathbf{M}_n(\mathrm{W}_e(k))\,,$$

where $e \in \mathbb{Z}_{\geq 1}$ satisfies $\mathrm{char}(k)^e = \mathrm{char}(R)$.

By Lemma 2.19, there exists $v \in R^*$ such that $e_i = vE_{ii}v^{-1}$ for all $i \in \{1, \ldots, n\}$ where E_{ii} is the elementary matrix with a 1 in the (i,i)th entry. After conjugating both S_1 and S_2 by v, the assumptions of the lemma still hold so we may assume without loss of generality that $v = 1$ and $e_i = E_{ii}$ for $i \in \{1, \ldots, n\}$. It is then clear that e_1Re_1 is a local ring[1] isomorphic to A. The ring $e_1S_1e_1$ is isomorphic to $\mathrm{W}_e(k)$ so this is a separable subring of e_1Re_1. Moreover, $e_1S_1e_1$ is radical-maximal because [Lam01, Thm. (21.10)] states that $\mathrm{rad}(e_1Re_1) = e_1\mathrm{rad}(R)\,e_1$ so our assumption that the natural map $S_1 \to R/\mathrm{rad}(R)$ is a surjection implies surjectivity of the natural map

$$e_1S_1e_1 \to \overline{e_1}\,(R/\mathrm{rad}(R))\,\overline{e_1},$$

where $\overline{e_1}$ is the image of e_1 in $R/\mathrm{rad}(R)$. Similarly, $e_1S_2e_1$ is a radical-maximal separable subring of e_1Re_1. Therefore, by Theorem 4.6 there exist $\alpha, \beta \in e_1Re_1$ such that $\alpha\beta = \beta\alpha = e_1$ and

$$e_1S_2e_1 = \alpha\,(e_1S_1e_1)\,\beta.$$

For any $i, j \in \{1, \ldots, n\}$ and $\varepsilon = 1, 2$, we have a group isomorphism

$$\mathrm{Hom}_{S_\varepsilon}(e_jS_\varepsilon, e_iS_\varepsilon) \cong e_iS_\varepsilon e_j, \tag{10}$$

given by sending a morphism φ to $\varphi(e_j)$ since the map is completely determined by the image of e_j, and we have a ring isomorphism $\mathrm{End}_{S_\varepsilon}(e_iS_\varepsilon) \cong e_iS_\varepsilon e_i$ (cf. [Lam01, Prop. (21.6)]).

By our assumption that for $\varepsilon = 1, 2$, the modules $e_1S_\varepsilon, \ldots, e_nS_\varepsilon$ are mutually isomorphic, there exist $a_{i,\varepsilon} \in e_iS_\varepsilon e_1$ and $\widetilde{a_{i,\varepsilon}} \in e_1S_\varepsilon e_i$ for all $i \in \{1, \ldots, n\}$ such that for all $i, j \in \{1, \ldots, n\}$,

$$\mathrm{Hom}_{S_\varepsilon}(e_jS_\varepsilon, e_iS_\varepsilon) \cong \widetilde{a_{i,\varepsilon}} \circ \mathrm{Hom}_{S_\varepsilon}(e_1S_\varepsilon, e_1S_\varepsilon) \circ a_{j,\varepsilon},$$

where we see $a_{i,\varepsilon}$ and $\widetilde{a_{i,\varepsilon}}$ as homomorphisms using (10), and we have $a_{i,\varepsilon} \circ \widetilde{a_{i,\varepsilon}} = e_i$ and $\widetilde{a_{i,\varepsilon}} \circ a_{i,\varepsilon} = e_1$.

Similar to what we have seen in Lemma 4.12, for $\varepsilon = 1, 2$, the ring S_ε is isomorphic to the generalized matrix ring

$$\left[\mathrm{Hom}_{S_\varepsilon}(e_jS_\varepsilon, e_iS_\varepsilon)\right]_{i,j=1}^{n} \cong \left[e_iS_\varepsilon e_j\right]_{i,j=1}^{n}. \tag{11}$$

Multiplication between elements $s \in e_iS_\varepsilon e_j$ and $t \in e_kS_\varepsilon e_\ell$ can be done with matrix multiplication using the above or with the multiplication of S_ε but the result is the same, as $s \cdot t$ is zero when $j \neq k$ and lands in $e_iS_\varepsilon e_\ell$.

Now let us write $u := \sum_{i=1}^n \widetilde{a_{i,2}} \cdot \alpha \cdot a_{i,1}$ and $v := \sum_{j=1}^n \widetilde{a_{j,1}} \cdot \beta \cdot a_{j,2}$. Since $a_{i,\varepsilon}\widetilde{a_{j,\varepsilon}} = 0$ for $i \neq j$ it is an easy exercise to check that $u \cdot v = v \cdot u = 1$ holds and that for all $i, j \in \{1, \ldots, n\}$ we have

$$e_iS_2e_j = u\,(e_iS_1e_j)\,v.$$

Hence, $v = u^{-1}$ and from (11) we get $S_2 = uS_1u^{-1}$. □

Lemma 4.15. *Let R be a finite ring and let S_1, S_2 be two radical-maximal separable subrings of R. Then, there exists $u \in R^*$ such that $S_2 = uS_1u^{-1}$.*

Proof. Because S_1 is left Artin, [Lam01, Thm. (23.6)] and the two lines below [Lam01, Def. (23.1)] imply that there exist mutually orthogonal local (so also primitive) idempotents $e_i \in S_1$ such that $1 = e_1 + \ldots + e_n$. It follows from Lemma 3.23 that $\ker(S_1 \to R/\mathrm{rad}(R)) = \mathrm{rad}(S_1)$, so the natural map

$$S_1/\mathrm{rad}(S_1) \xrightarrow{\sim} R/\mathrm{rad}(R) \tag{12}$$

[1]Pay attention that e_1Re_1 is *not* a subring of R because it does not contain the same unit element of the multiplication. When we write 1 we will mean the unit element of R in this proof, and e_i is the unit element of e_iRe_i.

is an isomorphism by radical-maximality of S_1.

Proposition (21.22) in [Lam01] (cf. Theorem 2.15) implies that in a ring A with nilpotent Jacobson radical, an idempotent e is primitive in A if and only if $e + \mathrm{rad}(A)$ is primitive in $A/\mathrm{rad}(A)$. Applying this to S_1 and R, we have for any $i \in \{1, \ldots, n\}$ that $e_i + \mathrm{rad}(S_1)$ is primitive in $S_1/\mathrm{rad}(S_1)$ and thus $e_i + \mathrm{rad}(R)$ is primitive in $R/\mathrm{rad}(R)$, from which it follows that e_i is also primitive in R.

Similarly, for S_2 we may write $1 = e'_1 + \ldots + e'_m$ where the e'_i are mutually orthogonal idempotents that are local in S_2 and primitive in R. Now there are two ways to decompose R_R into indecomposable right R-modules,

$$R_R \cong \bigoplus_{i=1}^{n} e_i R \cong \bigoplus_{j=1}^{m} e'_j R,$$

because the modules e_iR and e'_jR are indecomposable by Proposition (21.8) in [Lam01]. Hence by Theorem 4.9, we have $n = m$ and after permuting the e'_j we may assume without loss of generality that $e_iR \cong e'_iR$ as right R-modules. By Lemma 2.19, there exists $u \in R^*$ such that $e'_i = ue_iu^{-1}$ for all $i \in \{1, \ldots, n\}$. We may now replace S_1 by uS_1u^{-1} (and e_i accordingly) so without loss of generality we can assume that for all $i \in \{1, \ldots, n\}$ we have $e'_i = e_i$.

Theorem 3.21 yields that S_1 is isomorphic to

$$S_1 \cong \prod_{\ell=1}^{N} \mathbf{M}_{m_\ell}(\mathrm{W}_{s_\ell}(k_\ell)), \tag{13}$$

for certain $N \in \mathbb{Z}_{\geq 1}$, $m_\ell, s_\ell \in \mathbb{Z}_{\geq 1}$ and finite fields k_ℓ (where $\ell \in \{1, \ldots, N\}$).

The set of idempotents $(0, \ldots, 0, E_{jj}, 0, \ldots, 0)$ where the elementary matrix E_{jj} is in the ℓth factor ($\ell \in \{1, \ldots, N\}$ and $j \in \{1, \ldots, m_\ell\}$) gives rise to a set of mutually orthogonal local idempotents $e''_1, \ldots, e''_k$ in S_1 (where $k = m_1 + \cdots + m_N$) under the isomorphism (13). Because the e_is and e''_is give two ways to decompose S_1 in indecomposable right S_1-submodules, $k = n$ holds by Theorem 4.9 and after reshuffling we have for all $i \in \{1, \ldots, n\}$ that $e_iS_1 \cong e''_iS_1$ as right S_1-modules. Moreover, by Lemma 2.19 there exists $v \in S_1^*$ such that for $i = 1, \ldots, n$ we have $e''_i = ve_iv^{-1}$. Therefore for $i, j \in \{1, \ldots, n\}$ we have $e_iS_1 \cong e_jS_1$ if and only if e_i and e_j are nonzero in the same factor in the right hand side of (13). Now for $\ell \in \{1, \ldots, N\}$, let c_ℓ be the sum of all the e_i with $i \in \{1, \ldots, n\}$ that are nonzero in the ℓth factor in (13). Note that given some $\ell \in \{1, \ldots, N\}$ and some $i \in \{1, \ldots, n\}$ with e_i nonzero in the ℓth factor in (13), then c_ℓ is the sum of e_j where $j \in \{1, \ldots, n\}$ satisfies $e_jS_1 \cong e_iS_1$ as right S_1-modules. It follows by the above that the c_ℓ are mutually orthogonal idempotents of S_1 summing to 1. Moreover, c_ℓ is central in S_1 because the sum of all the elementary matrices on the diagonal is 1 in a matrix ring.

Lemma (19.27) in [Lam01] states that two finitely generated projective right R-modules P and Q are isomorphic if and only if $P/(P \cdot \mathrm{rad}(R)) \cong Q/(Q \cdot \mathrm{rad}(R))$ as right $R/\mathrm{rad}(R)$-modules. If we apply this lemma for any $i, j \in \{1, \ldots, n\}$ on the right S_1-modules e_iS_1 and e_jS_1 as well as the right R-modules e_iR and e_jR, the ring isomorphism in (12) implies that there is an isomorphism $e_iS_1 \cong e_jS_1$ of right S_1-modules if and only if the right R-modules e_iR and e_jR are isomorphic. By defining c'_ℓ analogous to how c_ℓ were defined in S_1, we get that $c_\ell = c'_\ell$ since by symmetry we have $e_iS_1 \cong e_jS_1$ if and only if $e_iS_2 \cong e_jS_2$ (where $i, j \in \{1, \ldots, n\}$). Thus, c_ℓ is also a central idempotent in S_2 for any $\ell \in \{1, \ldots, N\}$.

Note that by [Lam01, (21.7)] we have $c_\ell Rc_\ell \cong \mathrm{End}_R(c_\ell R) \cong \mathbf{M}_{m_\ell}(\mathrm{End}_R(e_iR))$ where i is such that e_i has a nonzero factor in the ℓth factor in (13), and that $c_\ell S_1$ and $c_\ell S_2$ are radical-maximal separable subrings of $c_\ell Rc_\ell$ because

$$\mathrm{rad}(c_\ell Rc_\ell) = c_\ell \cdot \mathrm{rad}(R) \cdot c_\ell,$$

follows from [Lam01, Thm. (21.10)]. Thus for all $\ell \in \{1, \ldots, N\}$, we can use Lemma 4.14 on the ring $c_\ell Rc_\ell$, separable subrings $c_\ell S_1, c_\ell S_2$ and the set of idempotents e_i that sum to c_ℓ. So, there

exist $u_\ell, v_\ell \in c_\ell R c_\ell$ such that $u_\ell v_\ell = v_\ell u_\ell = c_\ell$ and $c_\ell S_2 = u_\ell (c_\ell S_1) v_\ell$. By taking $u = u_1 + \ldots + u_N$, we get $u^{-1} = v_1 + \ldots + v_N$ by orthogonality of the c_ℓ. Hence, we have $S_2 = u S_1 u^{-1}$. □

Not only are any two radical-maximal separable subrings of R conjugate, but any separable subring is, up to conjugation, a subring of a radical-maximal separable subring of R, as the following lemma shows.

Lemma 4.16. *Let R be a finite ring, $S \subseteq R$ a radical-maximal separable ring and $T \subseteq R$ a separable ring. Then, there exists $u \in R^*$ such that $T \subseteq uSu^{-1}$.*

Proof. First, $R' := T + \mathrm{rad}(R)$ is a subring of R with $\mathrm{rad}(R)$ a nilpotent two-sided ideal of R'. Moreover by Lemma 3.23,

$$R'/\mathrm{rad}(R) \cong T/(\mathrm{rad}(R) \cap T) = T/\mathrm{rad}(T)\,, \tag{14}$$

so $\mathrm{rad}(R') = \mathrm{rad}(R)$ and T is a radical-maximal subring of R'.

Consider the following diagram of inclusions:

$$\begin{array}{ccccc} T & \subset & R' & \subset & R \\ & & \cup & & \cup \\ & & R' \cap S & \subset & S. \end{array}$$

Because S is radical-maximal, we have $S + \mathrm{rad}(R) = R$. Intersecting both sides with R' yields $R' = R' \cap (S + \mathrm{rad}(R)) = (R' \cap S) + \mathrm{rad}(R)$ since $\mathrm{rad}(R) \subseteq R'$. Therefore, the natural map $\varphi\colon R' \cap S \to R'/\mathrm{rad}(R)$ is surjective. The nilpotent two-sided ideal $\mathrm{rad}(R' \cap S)$ maps under φ to (0) because $R'/\mathrm{rad}(R)$ is semisimple by (14). Conversely, we have $\ker(\varphi) = \mathrm{rad}(R) \cap (R' \cap S)$ so the kernel is nilpotent. This shows that $\ker(\varphi) = \mathrm{rad}(R' \cap S)$ so the map φ gives an isomorphism

$$(R' \cap S)\,/\mathrm{rad}(R' \cap S) \xrightarrow{\sim} R'/\mathrm{rad}(R)\,.$$

Now by Lemma 4.13, there is a separable ring $S' \subseteq R' \cap S$ such that the natural map

$$S' \longrightarrow (R' \cap S)/\mathrm{rad}(R' \cap S) \cong R'/\mathrm{rad}(R)$$

is surjective. Thus now S' and T are radical-maximal subrings of R'. Hence by Lemma 4.15, there exists $u \in (R')^* \subseteq R^*$ such that

$$T = uS'u^{-1} \subseteq uSu^{-1}.$$

□

This Lemma yields a proof of Theorem 1.1 almost immediately.

Proof of Theorem 1.1. First, suppose $S \subseteq R$ is radical-maximal separable subring of a finite ring R. Assume that $T \subseteq R$ is a separable ring containing S. By Lemma 4.16, there exists $u \in R^*$ such that $S \subseteq T \subseteq uSu^{-1}$. Considering cardinalities of these rings yields $S = T$. Hence S is a maximal separable subring of R under inclusion.

Conversely, suppose $S \subseteq R$ is a maximal separable subring of R under inclusion. Now let T be a radical-maximal separable subring of R, which exists by Lemma 4.13. Then Lemma 4.16 implies that $S \subseteq uTu^{-1}$ so by maximality of S we have $S = uTu^{-1}$. Now note that $\mathrm{rad}(R) = u \cdot \mathrm{rad}(R) \cdot u^{-1}$ since $\mathrm{rad}(R)$ is a two-sided ideal, so we have

$$S + \mathrm{rad}(R) = u(T + \mathrm{rad}(R))u^{-1} = R.$$

This shows that S is radical-maximal. □

Theorem 4.4 and Theorem 1.2 are now simple consequences of the above lemma's.

Proof of Theorem 4.4. Simple corollary of Theorem 1.1, Lemma 4.13 and Lemma 4.15. □

Proof of Theorem 1.2. This follows directly from Theorem 1.1 and Lemma 4.16. □

5 Deterministic polynomial-time algorithms

Theorem 4.4 shows that there exists a unique maximal separable subring of a finite ring up to conjugation. It is interesting to ask if there exists a deterministic polynomial-time algorithm to construct such a subring.

5.1 Basis representation of finite rings

In order to work with finite rings, an agreement must be made on how to represent such rings. Although the theorem on finite abelian groups tells that a finite abelian group can be written as a finite product of cyclic groups of prime power orders, one cannot expect that R^+ is given in such explicit form as this requires factorization of n when considering the ring $R = \mathbb{Z}/n\mathbb{Z}$.

Definition 5.1. A *basis representation of a finite ring* R, consists of $d_1, \ldots, d_t \in \mathbb{Z}_{\geq 2}$ for some $t \in \mathbb{Z}_{\geq 0}$ such that

$$R^+ \cong \bigoplus_{i=1}^{t} \mathbb{Z}/d_i\mathbb{Z},$$

and 'structure constants' $a_{ijk} \in \mathbb{Z}/d_k\mathbb{Z}$ $(1 \leq i, j, k \leq t)$ satisfying $e_i \cdot e_j = \sum_{k=1}^{t} a_{ijk} e_k$ where $e_i \in R$ corresponds to the generator 1 of the ith subgroup $\mathbb{Z}/d_i\mathbb{Z}$ of R^+.

When a finite ring R is given as the input to an algorithm, it is assumed from now on that R is given by a basis representation, and when R is an output of an algorithm, it is understood that the algorithm produces a basis representation of R. Moreover, if a finite ring occurs in an algorithm, this means there is a basis representation known for this ring. In addition, if a subring $S \subseteq R$ occurs in an algorithm, this not only means there is a basis representation for S but also that there is an injection map $S \to R$, which is determined by the images of the generators of S.

Note that a basis representation of a finite ring R has at least $\lg|R|$ bits and consists of at most $\mathcal{O}(\lg^3|R|)$ bits, because $2^t \leq |R|$ holds and specifying what the product of two generators is, requires roughly $\lg d_1 + \cdots + \lg d_t = \lg|R|$ bits at most. An algorithm with a ring R as input runs in polynomial time if the number of elementary ring operations is bounded by a polynomial in $\lg|R|$.

How to represent ideals and left R-modules is explained in [CT16, Chapter 3].

5.2 Test for separability

It seems unlikely that there is a deterministic polynomial-time algorithm that decides if a finite ring R is semisimple. In the special case $R = \mathbb{Z}/n\mathbb{Z}$, this is equivalent to deciding if n is squarefree and no polynomial-time algorithm is known for this problem, see [BHK+15]. However, separability can be tested in polynomial time.

Theorem 5.2 ([CT16, Thm. 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.*

As a special case, one can test if a finite ring is separable in polynomial time.

Corollary 5.3. *There exists a deterministic polynomial-time algorithm that, given a finite ring S, decides whether or not S is a separable ring.*

Proof. Suppose a finite ring S is given. By Theorem [CT16, Thm. 3.3.1], there is a polynomial-time algorithm that determines the prime subring of S, i.e. the image of the map $\mathbb{Z} \to S, 1 \mapsto 1$. Let $R = \mathbb{Z}/\mathrm{char}(S)\,\mathbb{Z}$ be the prime subring of S. Note that there is a $\mathbb{Z}$-module isomorphism

$$S \otimes_{\mathbb{Z}} S^{\mathrm{op}} \cong S \otimes_R S^{\mathrm{op}},$$

so certainly S is separable over $\mathbb{Z}$ if and only if S is separable over R. Hence, we can use Theorem 5.2 to determine if S is separable over R. □

5.3 Constructing a radical-maximal subring

The goal of this section is to prove the following theorem.

Theorem 5.4. *There exists a deterministic polynomial-time algorithm that, given a finite ring R, outputs a maximal separable subring $S \subseteq R$ as in Theorem 4.4.*

The idea to prove this theorem is to first find a nil two-sided ideal I such that R/I is separable and then find a separable subring $S \subseteq R$ that surjects onto R/I.

For example, given a finite ring R, the reduced ring $R/\mathrm{rad}(R)$ is separable by Corollary 3.15 but determining $\mathrm{rad}(R)$ is at least as hard as deciding if R is semisimple.

Definition 5.5. Let $A = \prod_{i=1}^{t} A_i$ be a left Artin ring with $\mathrm{char}(A) \neq 0$ where A_i is a connected ring for $i = 1, \ldots, t$. Moreover, write

$$A = \prod_{\substack{p \text{ prime} \\ e \in \mathbb{Z}_{\geq 1}}} A_{p,e}, \qquad \text{with } A_{p,e} = \prod_{\substack{1 \leq i \leq t \\ \mathrm{char}(A_i) = p^e}} A_i.$$

Then, the *generalized prime subring of A*, denoted by $\mathcal{P}_A$, is the product of the prime subrings of the nontrivial $A_{p,e}$.

For the algorithm of Theorem 5.4, we are interested in finding a two-sided ideal $I \subseteq \mathrm{rad}(R)$ such that R/I is separable. Such an ideal can be computed in polynomial time by the following theorem.

Theorem 5.6 ([CT16, Thm. 6.3.22])**.** *There exists a deterministic polynomial-time algorithm that, given a finite ring R, computes a nil two-sided ideal $\mathfrak{j}_R$ such that $R/\mathfrak{j}_R$ is separable and the prime subring and generalized prime subring of $R/\mathfrak{j}_R$ are equal.*

Definition 5.7. Let $d, n \in \mathbb{Z}_{\geq 1}$. Then we say d is a *unitary divisor* of n (or $d \parallel n$ for short) if $d \mid n$ and $\gcd(n/d, d) = 1$.

Another algorithm we will use is the coprime base algorithm [Ber05, Algorithm 18.1], which given a list of numbers $m_1, \ldots, m_n \in \mathbb{Z}_{\geq 1}$, outputs in polynomial time an integer $t \in \mathbb{Z}_{\geq 1}$, a list of numbers $q_1, \ldots, q_t \in \mathbb{Z}_{\geq 2}$ that are mutually coprime and $e_{ij} \in \mathbb{Z}_{\geq 0}$ for all $i \in \{1, \ldots, n\}, j \in \{1, \ldots, t\}$, such that

$$\forall i \in \{1, \ldots, n\}: \qquad m_i = q_1^{e_{i1}} \cdot q_2^{e_{i2}} \cdot \ldots \cdot q_t^{e_{it}},$$

and for any $j \in \{1, \ldots, t\}$ there exists $i \in \{1, \ldots, n\}$ such that $e_{ij} \geq 1$. A simple implementation of the coprime base algorithm can be found in [BDS93], which requires at most $\mathcal{O}(b^2)$ bit operations where b is the number of bits in the input. This upper bound will be sufficient for our purpose.

We are now ready to state the algorithm that determines a maximal separable subring of a finite ring R.

Algorithm 1: MaxSep(R)

Input: A finite ring R.

Output: A maximal separable subring $S \subseteq R$ in the sense of Theorem 4.4.

Calculate $\mathfrak{j}_R \subseteq R$ from Theorem 5.6;

$S \longleftarrow R/\mathfrak{j}_R, \quad \psi \longleftarrow \mathrm{id}_S, \quad n \longleftarrow 1;$

while $\mathfrak{j}_R^n \neq (0)$ **do**

Suppose $S^+ \cong \bigoplus_{i=1}^t (\mathbb{Z}/d_i\mathbb{Z})^{\oplus n_i}$ where the $d_i \in \mathbb{Z}_{\geq 2}$ are pairwise coprime and multiplication is given by $\cdot_S \colon S \otimes_{\mathbb{Z}} S \to S$.

Let $\mathcal{A} := \bigoplus_{i=1}^t \left(\mathbb{Z}/d_i^2\mathbb{Z}\right)^{\oplus n_i}$ and let $c \colon \mathcal{A} \to S$ be the canonical map, i.e. reduction modulo d_i on the ith component.

Lift $\cdot_S$ to a group homomorphism $m_0 \colon \mathcal{A} \otimes_{\mathbb{Z}} \mathcal{A} \to \mathcal{A}$ such that it commutes with c, i.e. $c \circ m_0 = \cdot_S \circ (c \otimes c)$.

Determine an element $g \in \mathrm{Hom}(\mathcal{A} \otimes_{\mathbb{Z}} \mathcal{A} \to \ker c)$ such that $\Psi(g) = \mu$, where

$$\Psi \colon \mathrm{Hom}(\mathcal{A} \otimes_{\mathbb{Z}} \mathcal{A},\ \ker c) \to \mathrm{Hom}(\mathcal{A} \otimes_{\mathbb{Z}} \mathcal{A} \otimes_{\mathbb{Z}} \mathcal{A},\ \ker c)$$

$$g \mapsto \Big(x \otimes y \otimes z \mapsto g(x \otimes m_0(y \otimes z)) + m_0(x \otimes g(y \otimes z)) - g(m_0(x \otimes y) \otimes z) - m_0(g(x \otimes y) \otimes z) \Big),$$

and $\mu := (x \otimes y \otimes z \mapsto m_0(m_0(x \otimes y) \otimes z) - m_0(x \otimes m_0(y \otimes z)))$.

Let S' be the ring with additive group $\mathcal{A}$ and multiplication $m_0 + g$.

Construct a group homomorphism $\psi' \colon {S'}^+ \to (R/\mathfrak{j}_R^{2n})^+$ such that composition with the canonical map $R/\mathfrak{j}_R^{2n} \to R/\mathfrak{j}_R^n$ gives $\psi \circ c$.

Let $M := \mathfrak{j}_R^n/\mathfrak{j}_R^{2n}$ and construct the group homomorphism

$$\Phi \colon \mathrm{Hom}\Big({S'}^+, M^+\Big) \to \mathrm{Hom}\left((S' \otimes_{\mathbb{Z}} S')^+, M^+\right),$$

$$f \mapsto \Big(x \otimes y \mapsto f(x)\psi'(y) + \psi'(x)f(y) - f(xy) \Big).$$

Construct a solution $f \in \mathrm{Hom}\Big({S'}^+, M^+\Big)$ of $\Phi(f) = \Big(x \otimes y \mapsto \psi'(xy) - \psi'(x)\psi'(y) \Big)$.

$S \longleftarrow S', \quad \psi \longleftarrow \psi' + f, \quad n \longleftarrow 2 \cdot n;$

return $\psi(S)$;

Lemma 5.8. *Algorithm 1 is a deterministic polynomial-time algorithm that on input a finite ring R, gives a radical-maximal separable subring of R.*

Proof. It is clear that $n = 2^{i-1}$ holds at the beginning of the ith iteration of the while-loop (with $i \geq 1$). By Theorem 2.10, the two-sided ideal $\mathfrak{j}_R$ is nilpotent. Moreover, for any $\ell \in \mathbb{Z}_{\geq 1}$ with $\mathfrak{j}_R^\ell \neq (0)$, we have

$$\left|\mathfrak{j}_R^{\ell+1}\right| \leq \frac{1}{2} \cdot \left|\mathfrak{j}_R^\ell\right|.$$

This shows that $\mathfrak{j}_R^{\lg|R|} = (0)$ holds. Thus, the while-loop gets executed at most $\lg\lg|R|$ times.

In addition, we will show that the while-loop has the following loop-invariants:

- The ring S is separable and the prime subring and generalized prime subring of S are equal.
- The map ψ is a ring homomorphism from S to $R/\mathfrak{j}_R^n$ and $\psi(S)$ is a radical-maximal subring of $R/\mathfrak{j}_R^n$.

Initially these two invariants hold by Theorem 5.6.

Now suppose the loop-invariants hold at the beginning of an iteration.

First in step 4, a suitable basis representation can be found with the use of the coprime base algorithm. If $S^+ \cong \bigoplus_{i=1}^{s} \mathbb{Z}/d_i'\mathbb{Z}$ is the basis representation known for S (where $d_i' \in \mathbb{Z}_{\geq 2}$), we can run the coprime base algorithm with input $d_1', \ldots, d_s'$. Let $(q_1, \ldots, q_t)$ and e_{ij} $(i \in \{1, \ldots, s\}, j \in \{1, \ldots, t\})$ be the output. Then by the Chinese remainder theorem, for every $i \in \{1, \ldots, s\}$, the factor $\mathbb{Z}/d_i'\mathbb{Z}$ can be written as a direct sum of cyclic groups, each of order a power of some q_j $(1 \leq j \leq t)$. In fact, we will show that the orders occurring are among $\{q_1^{r_1}, \ldots, q_t^{r_t}\}$ for suitably chosen $r_1, \ldots, r_t \in \mathbb{Z}_{\geq 1}$.

To see this, first note that S is a separable ring with prime subring equal to the generalized prime subring $\mathcal{P}_S$ of S as the loop invariants hold. Second by Theorem 3.21, the ring S is a product of matrix rings over Witt rings, and in general, the Witt ring $\mathrm{W}_e(k)$ is a free $\mathbb{Z}/\mathrm{char}(k)^e\,\mathbb{Z}$-module. Combining these two facts, for all prime numbers p, we have that all the summands of S^+ having an order divisible by p, have orders with the same p-adic valuation equal to the p-adic valuation of $\mathrm{char}(S)$. Hence any summand of S^+ that is a power of q_j for some $j \in \{1, \ldots, t\}$ is equal to $q_j^{r_j}$ for some r_j that only depends on j. Moreover we can construct the basis representation in step 4 by writing $d_j = q_j^{r_j}$ for $j \in \{1, \ldots, t\}$. Note that this basis representation is essentially describing a ring isomorphism,

$$S \cong \prod_{i=1}^{t} S/d_iS.$$

Hence the multiplication given on S is equivalent to multiplication maps on each of the $(\mathbb{Z}/d_i\mathbb{Z})^{\oplus n_i}$.

In step 6, we may find a group homomorphism m_0 that satisfies $c \circ m_0 = \cdot_S \circ (c \otimes c)$ by lifting the multiplication on each $(\mathbb{Z}/d_i\mathbb{Z})^{\oplus n_i}$ to a additive group homomorphism

$$(\mathbb{Z}/d_i^2\mathbb{Z})^{\oplus n_i} \otimes (\mathbb{Z}/d_i^2\mathbb{Z})^{\oplus n_i} \to (\mathbb{Z}/d_i^2\mathbb{Z})^{\oplus n_i},$$

simply by taking a lift of $c(a_j) \otimes_S c(a_k)$ where $j, k \in \{1, \ldots, n_i\}$ and $a_1, \ldots, a_{n_i}$ form the basis representation of $(\mathbb{Z}/d_i^2\mathbb{Z})^{\oplus n_i}$. For any $a, b \in \mathcal{A}$ of additive order d, d' respectively, we need to have that $m_0(a \otimes b)$ has order dividing $\gcd(d, d')$ for m_0 to be an additive group homomorphism. This is however resolved by the basis representation constructed in step 4.

It is easily verified that Ψ in step 7 is a well-defined group homomorphism. Moreover, because $\cdot_S$ is an associative map, the image of μ is contained in $\ker c$. Since $\mathcal{P}_S$ is the prime subring of S, we have $d_i \mid\mid \mathrm{char}(S)$ for all $i \in \{1, \ldots, t\}$, so $\mathrm{char}(S)/d_i$ is a unit in $\mathbb{Z}/d_i^2\mathbb{Z}$. Hence,

$$\ker c = \bigoplus_{i=1}^{t} \left(d_i\mathbb{Z}/d_i^2\mathbb{Z}\right)^{\oplus n_i} = \bigoplus_{i=1}^{t} \left(\mathrm{char}(S)\,\mathbb{Z}/d_i^2\mathbb{Z}\right)^{\oplus n_i} = \mathrm{char}(S) \cdot \mathcal{A}.$$

Suppose $g \in \mathrm{Hom}(\mathcal{A} \otimes \mathcal{A}, \ker c)$ and $x, y, z \in \mathcal{A}$. Then, $g(x \otimes y) \in \ker c$ so there is some $w \in \mathcal{A}$ such that $g(x \otimes y) = \mathrm{char}(S) \cdot w$ which in turn yields

$$g\left(g(x \otimes y) \otimes z\right) = g\left(\mathrm{char}(S) \cdot (w \otimes z)\right) = \mathrm{char}(S) \cdot g(w \otimes z) \in \mathrm{char}(S) \cdot (\mathrm{char}(S) \cdot \mathcal{A}) = 0.$$

Hence $g(g(x \otimes y) \otimes z) = 0$ and similarly one finds $g(x \otimes g(y \otimes z)) = 0$. Thus a bilinear map $g \in \mathrm{Hom}(\mathcal{A} \otimes \mathcal{A}, \ker c)$ satisfies $\Psi(g) = \mu$ if and only if $g + m_0$ is an associative map.

Now by Theorem 3.21, there is an isomorphism

$$S \cong \prod_{i=1}^{s} \mathbf{M}_{m_i}(\mathrm{W}_{e_i}(k_i)), \tag{15}$$

for certain $s \in \mathbb{Z}_{\geq 1}$, $m_i, e_i \in \mathbb{Z}_{\geq 1}$ and finite fields k_i. This gives two ways to write the additive group of S, namely

$$S^+ \cong \bigoplus_{i=1}^{s} (\mathbb{Z}/\mathrm{char}(k_i)^{e_i}\,\mathbb{Z})^{\oplus\, m_i^2} \cong \bigoplus_{i=1}^{t} (\mathbb{Z}/d_i\mathbb{Z})^{\oplus n_i},$$

where the first one is only of theoretic interest and the second one is computationally accessible. Since $\widehat{S} = \prod_{i=1}^{s} \mathbf{M}_{m_i}(\mathrm{W}_{2e_i}(k_i))$ is a separable ring, its additive group is

$$\bigoplus_{i=1}^{s} (\mathbb{Z}/\mathrm{char}(k_i)^{2e_i}\,\mathbb{Z})^{\oplus\, m_i^2} \cong \bigoplus_{i=1}^{t} \left(\mathbb{Z}/d_i^2\mathbb{Z}\right)^{\oplus n_i} = \mathcal{A}.$$

Moreover, there is a surjective ring homomorphism $\widehat{S} \to S$ which shows that the image of $\cdot_{\widehat{S}} - m_0$ is contained in $\ker c$ where $\cdot_{\widehat{S}}$ is the multiplication map of $\widehat{S}$. In addition, $\cdot_{\widehat{S}}$ is an associative bilinear map on $\mathcal{A}$ so $\Psi\left(\cdot_{\widehat{S}} - m_0\right) = \mu$.

Now note that the tensor products and Hom-groups occurring in step 7 can be determined in deterministic polynomial time, by [CT16, Prop. 2.4.1]. By [CT16, Prop. 2.3.15] and [CT16, Prop. 2.1.7], there exists a deterministic polynomial-time algorithm that determines whether μ is in the image of Ψ and, if this is the case, outputs a preimage of μ. By the above, it is guaranteed that μ is in the image of Ψ, so this algorithm produces some map g with $\Psi(g) = \mu$ in step 7.

Then S' is an additive abelian group with an associative bilinear multiplication map $g + m_0$. Because S is a ring, there exists an element $e_0 \in S'$ such that

$$\forall x \in S' \colon \quad e_0 \cdot x - x \in \ker c.$$

The reader may verify that $e_0 + e_0 - e_0 \cdot e_0$ is a unit element of S'. Thus S' is indeed a ring in step 8.

Theorem II.7.1 in [DI71] states that given a commutative ring R and a finitely generated R-algebra A, the ring A is separable over R if and only if for every maximal ideal $\mathfrak{m}$ of R the ring $A/\mathfrak{m}A$ is separable over $R/\mathfrak{m}$. In our case with $R = \mathbb{Z}$ and $A = S$, this theorem implies that S/pS is separable over $\mathbb{F}_p$ for any prime p dividing the characteristic of S. Moreover, since $S'/pS' \cong S/pS$, the theorem above shows that S' is a separable ring.

Because d_i is a unitary divisor of $\mathrm{char}(S)$, it is clear that d_i^2 is a unitary divisor of $\mathrm{char}(S') = \mathrm{char}(S)^2$ so $\mathcal{P}_{S'}$ is equal to the prime subring of S'.

Note that in step 9, it is easy to find a group homomorphism $\psi' \colon {S'}^{+} \to (R/\mathfrak{j}_R^{2n})^{+}$. Namely, if $a \in S'$ is one of the n_i generators in the basis representation of ${S'}^{+}$ where $i \in \{1, \ldots, t\}$, then we need to choose for $\psi'(a)$ a lift of $\psi(c(a))$ that has an order dividing d_i^2.

By Lemma 4.13, there is a separable subring $T \subseteq R/\mathfrak{j}_R^{2n}$ such that the natural map $T \to R/\mathrm{rad}(R)$ is surjective. Moreover, the image of T in $R/\mathfrak{j}_R^{n}$ and $\psi(S)$ are radical-maximal separable subrings of $R/\mathfrak{j}_R^{n}$. By Lemma 4.15, there exists $\overline{u} \in (R/\mathfrak{j}_R^{n})^*$ such that $(T + \mathfrak{j}_R^{n})/\mathfrak{j}_R^{n} = \overline{u} \cdot \psi(S) \cdot (\overline{u})^{-1}$. Since $(\mathfrak{j}_R^{n}/\mathfrak{j}_R^{2n})^2 = (0)$ holds, there exists a unit $u \in (R/\mathfrak{j}_R^{2n})^*$ that reduces to $\overline{u}$ and we may replace T by uTu^{-1}. So without loss of generality we may assume that

$$(T + \mathfrak{j}_R^{n})/\mathfrak{j}_R^{n} = \psi(S).$$

By Remark 3.17, equation (15) implies that

$$\psi(S) \cong \prod_{i=1}^{s} \mathbf{M}_{m_i}(\mathrm{W}_{f_i}(k_i))\,,$$

for certain $f_i \in \mathbb{Z}_{\geq 1}$ with $f_i \leq e_i$ and

$$T \cong \prod_{i=1}^{s} \mathbf{M}_{m_i}(\mathrm{W}_{g_i}(k_i))\,,$$

where $g_i \in \mathbb{Z}_{\geq f_i}$ for $i = 1, \ldots, s$. Because one has $\psi(S) = (T + \mathfrak{j}_R^{n})/\mathfrak{j}_R^{n} \cong T/(T \cap \mathfrak{j}_R^{n})$, it follows that for all $i = 1, \ldots, s$, there is an element $r \in T$ with $\mathrm{char}(k_i)^{f_i}$ in the ith component (on

the diagonal) and 0 elsewhere, which is now seen to lie in $\mathfrak{j}_R^n$ so $r^2 = 0$ holds. This shows that $\operatorname{char}(k_i)^{g_i} \mid \operatorname{char}(k_i)^{2f_i}$, or equivalently $g_i \leq 2f_i$ for all $i \in \{1, \ldots, s\}$. Because this in turn yields $g_i \leq 2e_i$ for $i \in \{1, \ldots, s\}$, we see that there exists a ring homomorphism $\chi\colon S' \to R/\mathfrak{j}_R^{2n}$ with image T such that the diagram

$$\begin{array}{ccc} S' & \xrightarrow{\chi} & R/\mathfrak{j}_R^{2n} \\ \big\downarrow{\scriptstyle c} & & \big\downarrow{\scriptstyle (\operatorname{mod} \mathfrak{j}_R^n)} \\ S & \xrightarrow{\psi} & R/\mathfrak{j}_R^n \end{array}$$

commutes. In particular, step 11 has $\chi - \psi'$ as a solution.

Now given such a solution f of the equation in step 11, it can be seen that

$$\forall x, y \in S'\colon \quad (\psi' + f)(x) \cdot (\psi' + f)(y) = \psi'(xy) + f(xy),$$

because $f(x)f(y) \in M^2 = (0)$ for all $x, y \in S'$. In particular, by filling in $x = y = 1$ in the above equation, $(\psi' + f)(1)$ is an idempotent and $(\psi' + f)(1) \in 1 + M$ implies that $(\psi' + f)(1)$ is a unit in $R/\mathfrak{j}_R^{2n}$ so we have $(\psi' + f)(1) = 1$. Thus, $\psi' + f$ is a ring homomorphism. In particular, the image of $\psi' + f$ is a separable subring of $R/\mathfrak{j}_R^{2n}$ by Proposition 3.8.

Because $\mathfrak{j}_R \subseteq \operatorname{rad}(R)$ holds, we have the following commuting diagram of rings,

$$\begin{array}{ccc} S' & \xrightarrow{\psi'+f} & R/\mathfrak{j}_R^{2n} \\ \big\downarrow{\scriptstyle c} & & \big\downarrow{\scriptstyle (\operatorname{mod} \mathfrak{j}_R^n)} \\ S & \xrightarrow{\psi} & R/\mathfrak{j}_R^n \\ & \searrow & \big\downarrow{\scriptstyle (\operatorname{mod} \mathfrak{j}_R)} \\ & & R/\mathfrak{j}_R \twoheadrightarrow R/\operatorname{rad}(R)\,. \end{array}$$

From the diagram it is clear that S' surjects to $R/\operatorname{rad}(R)$ so $(\psi' + f)(S')$ is a radical-maximal separable subring of $R/\mathfrak{j}_R^{2n}$.

Thus by the replacements in step 12, the loop invariants are preserved after one execution of the body of the while-loop. When the algorithm leaves the loop, we have $\mathfrak{j}_R^n = (0)$ so $\psi(S)$ is a radical-maximal separable subring of $R/(0) = R$. This proves the correctness of Algorithm 1.

By the tools developed in [CT16], one iteration of the while-loop, with the separable ring S at the beginning of the iteration, will run in time polynomial in the size of the basis representation for S. Thus, there exists $c \in \mathbb{R}_{\geq 1}$ such that the ith iteration takes time at most $\mathcal{O}(\lg^c |S_i|)$, where S_i is the separable ring S in the ith iteration. Let m be the number of times that the while-loop gets executed. Note that $|S_i| = |R/\mathfrak{j}_R|^{2^{i-1}}$ for $i = 1, \ldots, m$ so the total runtime of the while-loop can be found by solving a geometric series, i.e.

$$\sum_{i=1}^{m} \lg^c |S_i| \leq \lg^c |R/\mathfrak{j}_R| \cdot \left(1 + 2^c + \cdots + 2^{c(m-1)}\right) = \lg^c |R/\mathfrak{j}_R| \cdot \frac{2^{cm} - 1}{2^c - 1} \leq \lg^{2c} |R|\,,$$

because we have $m \leq \lg\lg |R|$ and $|R/\mathfrak{j}_R| \leq |R|$. Hence, Algorithm 1 is a polynomial-time algorithm. □

5.4 Finding a unit that conjugates radical-maximal subrings

Lemma 4.15 shows that two radical-maximal separable subrings S, T of a finite ring R are conjugated by a unit of R, i.e. there exists $u \in R^*$ such that $T = uSu^{-1}$. The goal of this subsection is to show that a unit with this property can be found in polynomial time.

Algorithm 2: CONJUGATION(R, S, T)

Input: A finite ring R, and radical-maximal separable subrings $S, T \subseteq R$.
Output: A unit $u \in R^*$ such that $T = uSu^{-1}$.

Determine with the algorithm of Theorem 5.6 a nilpotent two-sided ideal $J \subseteq R$ for which R/J is a separable ring;
$u \longleftarrow 1, \qquad S' \longleftarrow S, \qquad R' \longleftarrow R$;
while $J \neq (0)$ **do**
  Construct for every s_i in the basis representation of S' an element $t_i \in T$ such that t_i maps under the natural map $T \to R'/J$ to $s_i + J$;
  Let $\overline{S}, \overline{T}$ be the images of S' and T under $R' \to R'/J^2$ respectively and let $\overline{J} = J/J^2$.
  Consider the group homomorphism

$$\begin{aligned} \Phi\colon \quad & \overline{J} \to \mathrm{Hom}_{\mathbb{Z}}\big(\overline{S}, \overline{J}/(\overline{J} \cap \overline{T})\big), \\ & \overline{x} \mapsto \big(s \ \mapsto \ (s\overline{x} - \overline{x}s) + \overline{J} \cap \overline{T}\big), \end{aligned}$$

  and construct $\overline{x} \in \overline{J}$ such that $\Phi(\overline{x})$ is the (unique) morphism that sends s_i to $(s_i - t_i) + \overline{J} \cap \overline{T}$;
  Lift $\overline{x}$ to some $x \in J$;
  $u \longleftarrow (1 + x) \cdot u$;
  $S' \longleftarrow (1 + x)S'(1 + x)^{-1}$;
  $J \longleftarrow J^2$;
  $R' \longleftarrow T + J$;
return u;

Theorem 5.9. *Algorithm 2 is a deterministic polynomial-time algorithm that, given a finite ring R and two radical-maximal separable subrings S, T of R, determines a unit $u \in R^*$ such that $T = uSu^{-1}$.*

Proof. We start by showing that the while-loop in Algorithm 2 has as loop-invariants:

- The R-ideal J is contained in $\mathrm{rad}(R')$,
- The ring R' satisfies $S' + J = T + J = R' \subseteq R$,
- The ring S' satisfies $S' = uSu^{-1}$.

Note that these properties imply that S' and T are radical-maximal separable subrings of R', assuming the input specifications hold.

Initially, S' and T map to radical-maximal separable subrings of R'/J since $J \subseteq \mathrm{rad}(R')$. By Theorem 5.6, the ring R'/J is separable so it follows from Theorem 1.1 that the natural maps $S' \to R'/J$ and $T \to R'/J$ are surjective, i.e. we have $S' + J = T + J = R'$. Moreover, $u = 1$ and $S = S'$ hold in the beginning. Hence the loop-invariants hold initially.

Suppose we perform an iteration of the while-loop and assume that the loop-invariants hold. By Lemma 4.15, there exists some $v \in R'^*$ such that $T = vS'v^{-1}$. From $S' + J = R'$ it follows that the natural map $S' \to R'/J$ gives an isomorphism $S'/(J \cap S') \xrightarrow{\sim} R'/J$. Because $J \cap S'$ is contained in $\mathrm{rad}(S')$, it follows from the definition of the Jacobson radical that any $s \in S'$ is a unit in S' if and only $s + (J \cap S')$ is a unit in $S'/(J \cap S')$ or equivalently, s maps to a unit in R'/J. So there exists $s \in S'^*$ that maps to $v + J$ in $(R'/J)^*$ and we have $T = vS'v^{-1} = (vs^{-1})\big(sS's^{-1}\big)(vs^{-1})^{-1}$. Since $sS's^{-1} = S'$ this yields that $T = (vs^{-1})S'(vs^{-1})^{-1}$ where $vs^{-1} \in 1 + J$, so at the beginning of the execution of the loop, there is a unit $w \in 1 + J$ such that $T = wS'w^{-1}$. This shows there exists $y \in \overline{J}$ such that $\overline{T} = (1 + y)\overline{S}(1 - y)$, where we use $(1 + y)^{-1} = 1 - y$. In particular, it is easy to see that $\Phi(y)$ sends s_i to $(s_i - t_i) + \overline{J} \cap \overline{T}$ because $t_i \in (1 + y)s_i(1 - y) + \overline{J} \cap \overline{T}$. So the

unique morphism in step 6 is in the image of Φ, so a preimage can be found deterministically in polynomial time with the algorithms in [CT16]. Now we may safely assume that an $x \in J$ is found such that $\Phi(x + J^2) = \Phi(y)$. This implies

$$(1 + x)S'(1 + x)^{-1} + J^2 = (1 + y)S'(1 + y)^{-1} + J^2 = T + J^2.$$

Here, the inverse of $1+x$ is easily computable in polynomial time since $(1+x)^{-1} = 1-x+x^2-x^3+\ldots$ holds and x is nilpotent.

Using the new values of S', R' and J after step 8-11, it is clear that $S' + J = T + J = R'$ holds. Hence, the loop-invariants are preserved after one iteration.

Lastly, when the while-loop is finished, $J = 0$ holds and this yields

$$T = T + J = S' + J = uSu^{-1} + J = uSu^{-1},$$

so the output is correct.

It remains to show that the algorithm runs in deterministic polynomial time. Because $J^{\lg|R|} = (0)$ holds, the number of iterations is at most $\lg\lg|R|$, which is polynomial in the input size. Moreover, the number of preimages that need to be found in step 4 is equal to the number of elements in the basis representation of S', which is equal to the number of elements in the basis representation of S since S' is a conjugation of S by a unit in R. Thus, step 4 requires time polynomial in the input size. The number of $\mathbb{Z}$-linear generators for J is in each step at most $\lg|R|$ since $J \subseteq R$. Hence, we may conclude that Algorithm 2 is deterministic and runs in polynomial time. □

Corollary 5.10. *There exists a deterministic polynomial-time algorithm that given a radical-maximal separable subring S of a finite ring R and a separable ring $T \subseteq R$ determines a unit $u \in R^*$ such that $T \subseteq uSu^{-1}$.*

Proof. The following proof is similar to the proof of Lemma 4.16, but in this case we will work with the ideal $\mathfrak{j}_R$ from Theorem 5.6, which is contained in $\mathrm{rad}(R)$, instead of $\mathrm{rad}(R)$.

First, let us calculate the ideal $\mathfrak{j}_R$ from Theorem 5.6. Write $R' := T + \mathfrak{j}_R$ for the subring of R that contains T and $\mathfrak{j}_R$.

As is clear from Algorithm 1, the natural map $S \to R/\mathfrak{j}_R$ is surjective. In other words, $S + \mathfrak{j}_R = R$ holds. Intersecting this with R', we get $(S \cap R') + \mathfrak{j}_R = R'$ since R' is closed under addition. Thus the natural map $S \cap R' \to R'/\mathfrak{j}_R$ is surjective.

Now run Algorithm MaxSep on the ring $S \cap R'$ to find a radical-maximal subring of $S \cap R'$, say it finds S'. Then, the natural map $S' \to (S \cap R')/\mathrm{rad}(S \cap R')$ is surjective by definition. Now the maps $S \cap R' \to R'/\mathfrak{j}_R$ and $R'/\mathfrak{j}_R \to R'/\mathrm{rad}(R')$ are surjective so $S \cap R' \to R'/\mathrm{rad}(R')$ is a surjection to a semisimple ring. Hence $\mathrm{rad}(S \cap R') \subseteq \ker(S \cap R' \to R'/\mathrm{rad}(R'))$ and we have a surjection

$$S' \to R'/\mathrm{rad}(R'),$$

which shows that S' is a radical-maximal separable subring of R'. On the other hand, the map $T \to R'/\mathfrak{j}_R$ is surjective by definition of R' so T is a radical-maximal separable subring of R'.

Now by Theorem 5.9 there is a deterministic polynomial-time algorithm that finds $u \in (R')^*$ such that $T = uS'u^{-1} \subseteq uSu^{-1}$. □

References

[AG60] M. Auslander and O. Goldman. The Brauer group of a commutative ring. *Transactions of the American Mathematical Society*, 97(3):367–409, 1960.

[AM69] M.F. Atiyah and I.G. MacDonald. *Introduction to commutative algebra*. Addison-Wesley series in Mathematics. CRC Press, 1969.

[BDS93] E. Bach, J. Driscoll, and J. Shallit. Factor refinement. *Journal of Algorithms*, 15:199–222, 1993.

[Ber05] D.J. Bernstein. Factoring into coprimes in essentially linear time. *Journal of Algorithms*, 54(1):1–30, 2005.

[BF12] G. Bini and F. Flamini. *Finite commutative rings and their applications*, volume 680. Springer Science & Business Media, 2012.

[BHK+15] A.R. Booker, G.A. Hiary, J.P. Keating, et al. Detecting squarefree numbers. *Duke Mathematical Journal*, 164(2):235–275, 2015.

[CT16] I. Ciocănea-Teodorescu. *Algorithms for finite rings*. PhD thesis, Universiteit Leiden, 2016.

[DI71] F. DeMeyer and E. Ingraham. *Separable Algebras over Commutative Rings*, volume 181 of *Lecture Notes in Mathematics*. Springer-Verlag, 1971.

[For17] T.J. Ford. *Separable Algebras*, volume 183 of *Graduate studies in mathematics*. American Mathematical Society, 2017.

[FT63] W. Feit and J.G. Thompson. *Solvability of groups of odd order*, volume 13. Pacific Journal of Mathematics, 1963.

[KDS20] J. Kaur, S. Dutt, and R. Sehmi. On cyclic codes over Galois rings. *Discrete Applied Mathematics*, 280:156–161, 2020.

[KO74] M.-A. Knus and M. Ojanguren. *Théorie de la Descente et Algèbres d'Azumaya*, volume 389 of *Lecture Notes in Mathematics*. Springer-Verlag, 1974.

[Lam01] T.Y. Lam. *A First Course in Noncommutative Rings*, volume 131 of *Graduate Texts in Mathematics*. Springer-Verlag, second edition, 2001.

[Rob96] D. Robinson. *A Course in the Theory of Groups*, volume 80 of *Graduate Texts in Mathematics*. Springer-Verlag, second edition, 1996.

[Sal99] D.J. Saltman. *Lectures on Division Algebras*. Number 94 in Regional Conference Series in Mathematics. American Mathematical Society, 1999.