Bounding the unit index in terms of the additive quotient

Spieksma, A.V.J.

Alexander V.J. Spieksma
alexspieksma@gmail.com

Bounding the unit index in terms of the additive quotient

Bachelor thesis

August 28, 2019

Thesis supervisor: prof.dr. H.W. Lenstra

Leiden University
Mathematical Institute

Contents

1. Introduction

We bound the unit index of a subring in terms of its additive index and in terms of its additive quotient group; this is Theorem 1.1. It is a consequence of our second main result, Theorem 1.8, which describes the complete structure of a certain class of ring extensions.

To make matters more precise, we define the category **RingExt** of ring extensions. The objects are pairs of rings (E, F) with E a subring of F, and the morphisms are the ring homomorphisms between the larger rings that restrict to a map between the designated subrings. We say $E \subset F$ is a ring extension, or simply an extension, to indicate that (E, F) is in **RingExt**. For the sake of brevity, we often add adjectives to ring extensions that pertain to the larger ring, or to the subring if no confusion can arise. Let $E \subset F$ be an extension. The *additive index* of $E \subset F$ is the order of the additive quotient group F/E and is denoted by $(F : E)$. The *unit index* of $E \subset F$ is the order of the quotient set $F^\times/E^\times$ and is denoted by $(F^\times : E^\times)$.

We follow the convention that $\mathbb{N} = \mathbb{Z}_{\geq 1}$. For $n \in \mathbb{N}$ we define $u(n)$ to be the supremum of $(F^\times : E^\times)$ over all extensions $E \subset F$ with additive index n. For every finite abelian group A, we use $u(A)$ to denote the supremum of $(F^\times : E^\times)$ over all extensions $E \subset F$ with additive quotient group isomorphic to A. We let $l(n)$ and $l(A)$ denote the respective infima of the unit indices. Analogously, we define $u_{\text{fin}}(n)$, $u_{\text{fin}}(A)$, $l_{\text{fin}}(n)$ and $l_{\text{fin}}(A)$ by only considering extensions $E \subset F$ for which F has finite order.

Theorem 1.1. *Let $n \in \mathbb{N}$, let A be a finite abelian group and let A_p be the unique Sylow p-subgroup of A for each prime p. Then:*

(a) *both $u(n)$ and $u_{\text{fin}}(n)$ are given by the following expression, in which p ranges over all primes:*

$$\prod_p (p+1)^{\text{ord}_p(n)},$$

we have $l(n) = 1$, and $l_{\text{fin}}(n)$ is given by the above expression but with "$p+1$" replaced by "$p-1$";

(b) *both $u(A)$ and $u_{\text{fin}}(A)$ are given by the following expression, in which p ranges over all primes:*

$$\prod_p (p+1)^{\dim_{\mathbb{F}_p} A/pA} \cdot \#pA_p,$$

we have $l(A) = 1$, and $l_{\text{fin}}(A)$ is given by the above expression but with "$p+1$" replaced by "$p-1$".

We prove part (a) as Theorem 6.2 and part (b) as Theorem 6.5. It should be noted that upper bounds for the unit index in terms of the additive quotient have already been established in [Wol95] and [Wol97], although both papers only consider orders in number fields. To be specific, let E and F be orders in a common number field with $E \subset F$. In [Wol95, Theorem 3]

it is assumed that $F/E \cong \mathbb{Z}/p^k\mathbb{Z}$ for a prime p and $k \in \mathbb{N}$, and it is shown that $(F^\times : E^\times) \leq p^{k-1}(p+1)$. This upper bound is precisely the expression for $u(F/E)$ in part (b). The upper bounds for $(F^\times : E^\times)$ determined in [Wol97, Theorem 3], don't require F/E to be cyclic; however, these upper bounds are strictly larger than the expression for $u(F/E)$ in part (b).

It turns out that the results of Theorem 1.1 also hold if one only takes commutative rings into account. In fact, the theorem is significantly easier to prove in this case; we will not elaborate this however.

We move on to Theorem 1.8. An extension $E \subset F$ is *cosy* if E is a maximal subring of F with finite additive index, such that E does not contain any two-sided ideals of F except for the zero ideal. Below are six examples of cosy extensions. In corresponding order, it will be shown in Examples 4.1, 4.3, 4.4, 4.5, 8.2 and 8.3 that the extensions are indeed cosy.

Example 1.2. Let K be a finite field and let V be a non-zero, finite-dimensional K-vector space. Define $\mathrm{Diag}_K(V) = \{(x,x) : x \in \mathrm{End}_K(V)\}$. Then $\mathrm{Diag}_K(V) \subset \mathrm{End}_K(V) \times \mathrm{End}_K(V)$ is cosy.

If K is a field, V is a non-zero K-vector space and W is a subgroup of V, then $\mathrm{Fix}_K(W,V) = \{x \in \mathrm{End}_K(V) : xW \subset W\}$ is a subring of $\mathrm{End}_K(V)$.

Example 1.3. Let K be a finite field, let V be a finite-dimensional K-vector space and let W be a proper, non-zero subspace of V. Then the extension $\mathrm{Fix}_K(W,V) \subset \mathrm{End}_K(V)$ is cosy.

Let R be a commutative ring. An *R-algebra* is a ring A endowed with a ring homomorphism from R to the centre $Z(A)$ of A. An R-algebra is naturally a left and right R-module. Let A and B be R-algebras. The tensor product $A \otimes_R B$ has a natural ring structure determined by $(a \otimes b)(a' \otimes b') = (aa') \otimes (bb')$ and a natural R-algebra structure via the map $r \mapsto r \otimes 1$.

Let R and S be rings. An *R-S-bimodule* M is a left R-module and a right S-module such that $(rm)s = r(ms)$ for all $r \in R$, $s \in S$ and $m \in M$. Equivalently, M is an R-S-bimodule if it is a left $R \otimes_{\mathbb{Z}} S^{\mathrm{opp}}$-module, where S^{opp} is the opposite ring of S; the abelian group S with multiplication the other way around.

Example 1.4. Let K be a finite field, let $L \subset K$ be a field extension of prime degree and let V be a non-zero, finite-dimensional L-vector space. Then $\mathrm{End}_L(V) \subset K \otimes_L \mathrm{End}_L(V)$ is cosy.

Example 1.5. Let K be a finite field, let $K \subset L$ be a field extension of prime degree and let V be a non-zero, finite-dimensional L-vector space. Then the extension $\mathrm{End}_L(V) \subset \mathrm{End}_K(V)$ is cosy.

Let R be a ring and let I be an R-R-bimodule. Consider the abelian group $R \oplus I\epsilon$. We define a multiplication on $R \oplus I\epsilon$ by $(r + x\epsilon)(s + y\epsilon) = rs + (ry + xs)\epsilon$. This gives rise to the standard ring structure on $R \oplus I\epsilon$. The ring $R \oplus I\epsilon$ contains R as a subring and $I\epsilon$ as a two-sided ideal.

Example 1.6. Let K be a finite field, let L be the prime field of K, let $\sigma \in \mathrm{Aut}(K)$ and let V be a non-zero, finite-dimensional L-vector space. Set $E = K \otimes_L \mathrm{End}_L(V)$. Endow E with the E-E-bimodule structure defined by $((x \otimes a) \otimes (y \otimes b)) \cdot (z \otimes c) = (xz\sigma(y)) \otimes (acb)$ and write $E \oplus E\epsilon_\sigma = E \oplus E\epsilon$ to highlight the dependence on σ. Then $E \subset E \oplus E\epsilon_\sigma$ is cosy.

Example 1.7. Let K be a finite field and let L and M be subfields of K such that $K = LM$. Let U be an L-vector space and let V be an M-vector space such that both are non-zero and finite dimensional. Define $U_K = K \otimes_L U$ and $V_K = K \otimes_M V$. Set $E = \mathrm{End}_L(U) \times \mathrm{End}_M(V)$ and regard $\mathrm{Hom}_K(V_K, U_K)$ as E-E-bimodule via the action $((x_1, x_2) \otimes (y_1, y_2)) \cdot z = (\mathrm{id}_K \otimes x_1) \circ z \circ (\mathrm{id}_K \otimes y_2)$. Then $E \subset E \oplus \mathrm{Hom}_K(V_K, U_K)\epsilon$ is cosy.

We shall henceforth assume that an algebraically closed field Ω_p of characteristic p has been provided for every prime p. For each $k \in \mathbb{N}$ and each prime p, we denote the unique subfield of Ω_p with p^k elements by $\mathbb{F}_{p^k}$.

Theorem 1.8. *Define the following parametrised families of ring extensions with parameters as indicated:*

I. $\mathrm{Diag}_K(V) \subset \mathrm{End}_K(V) \times \mathrm{End}_K(V)$ *with* $K = \mathbb{F}_{p^k}$ *and* $V = K^n$ *for all primes* p *and* $k, n \in \mathbb{N}$*;*

II. $\mathrm{Fix}_K(W, V) \subset \mathrm{End}_K(V)$ *with* $K = \mathbb{F}_{p^k}$, $V = K^n$ *and* $W = K^m \times 0$ *for all primes* p *and* $k, n, m \in \mathbb{N}$ *such that* $m < n$*;*

III. $\mathrm{End}_L(V) \subset K \otimes_L \mathrm{End}_L(V)$ *with* $K = \mathbb{F}_{p^{kd}}$, $L = \mathbb{F}_{p^k}$ *and* $V = L^n$ *for all primes* p*, primes* d*, and* $k, n \in \mathbb{N}$*;*

IV. $\mathrm{End}_L(V) \subset \mathrm{End}_K(V)$ *with* $K = \mathbb{F}_{p^k}$, $L = \mathbb{F}_{p^{kd}}$ *and* $V = L^n$ *for all primes* p*, primes* d*, and* $k, n \in \mathbb{N}$*;*

V. $K \otimes_L \mathrm{End}_L(V) \subset (K \otimes_L \mathrm{End}_L(V)) \oplus (K \otimes_L \mathrm{End}_L(V))\epsilon_\sigma$ *as defined in Example 1.6 with* $K = \mathbb{F}_{p^k}$, $L = \mathbb{F}_p$ *and* $V = \mathbb{F}_p^n$ *for all primes* p*, automorphisms* $\sigma \in \mathrm{Aut}(K)$ *and* $k, n \in \mathbb{N}$*;*

VI. $\mathrm{End}_L(U) \times \mathrm{End}_M(V) \subset (\mathrm{End}_L(U) \times \mathrm{End}_M(V)) \oplus \mathrm{Hom}_K(V_K, U_K)\epsilon$ *as defined in Example 1.7 with* $K = \mathbb{F}_{p^{\mathrm{lcm}(d,e)}}$, $L = \mathbb{F}_{p^d}$, $M = \mathbb{F}_{p^e}$, $U = L^m$ *and* $V = M^n$ *for all primes* p *and* $d, e, m, n \in \mathbb{N}$*.*

Then each of these families consists of cosy extensions and every cosy extension is isomorphic to precisely one of these extensions.

A ring is *simple* if it contains precisely two two-sided ideals. A ring R is *semisimple* if every short exact sequence of left R-modules splits.

The proof of Theorem 1.8 is split into several parts. In Section 3 we determine the maximal subrings of simple rings of finite order. They will play an important role for our structure theorem for semisimple, cosy extensions; this is Theorem 4.8. The non-semisimple, cosy extensions are treated in Section 8. Here we also complete the proof of Theorem 1.8 as Theorem 8.10.

Our two main theorems are related due to Theorem 1.9. We define the *conductor* of an extension $E \subset F$ to be the set $\{x \in F : FxF \subset E\}$, which is a two-sided ideal of F that is contained in E by Lemma 2.2.

Theorem 1.9. *Let $E \subset F$ be an extension with finite additive index and let C be the conductor of $E \subset F$. Then:*

(a) *the ring F/C has finite order and $E/C \subset F/C$ has trivial conductor;*
(b) *we have $(F^\times : E^\times) \leq ((F/C)^\times : (E/C)^\times)$ with equality if $\#F$ is finite.*

This is essentially a corollary of [BL15, Lemma 3.7]. However, we prove Theorem 1.9 anew as Theorem 2.5. If $E \subset F$ is a maximal extension with finite additive index, then we shall see in Definition 2.8 that $E/C \subset F/C$ is cosy, where C is the conductor of $E \subset F$. Consequently, part (b) of Theorem 1.9 suggests that we can determine $u(n)$, $u_{\text{fin}}(n)$ and $l_{\text{fin}}(n)$ for all $n \in \mathbb{N}$ using only cosy extensions. This will indeed be the case and, in fact, only the semisimple version of our main structure theorem will be necessary to prove part (a) of Theorem 1.1. Most of the preparation for the proof of part (a) of Theorem 1.1 can be found in Section 5, where we compute the additive indices and unit indices of all cosy extensions. In Example 6.1 we will see that $l(n) = 1$ for all $n \in \mathbb{N}$. We derive part (b) of Theorem 1.1 from part (a) of Theorem 1.1.

2. Cosy extensions

This section introduces cosy extensions and establishes several elementary properties of cosy extensions. We will use the definitions and theory developed in this section throughout the other sections.

Definition 2.1. Let $E \subset F$ be an extension. The *conductor* of $E \subset F$ is the set $\{x \in F : FxF \subset E\}$. We denote it by $C(E \subset F)$.

Lemma 2.2. *Let $E \subset F$ be an extension. Then the conductor of $E \subset F$ is the greatest two-sided ideal of F that is contained in E.*

Proof. Write $C = C(E \subset F)$. It is obvious that C is a two-sided ideal of F. We have $C \subset \{x \in F : 1 \cdot x \cdot 1 \in E\} = E$, so C is contained in E. Let J be an arbitrary two-sided ideal of F that is contained in E. Then we have $FxF \subset J \subset E$ for all $x \in J$ and thus $J \subset C$. This proves Lemma 2.2. □

Lemma 2.3. *Let $E \subset F$ be an extension and let I be a two-sided ideal of F that is contained in E. Write $C = C(E \subset F)$. Then $C(E/I \subset F/I) = C/I$. In particular, if $I = C$, the conductor of $E/I \subset F/I$ is trivial.*

Proof. By Lemma 2.2, the set C is a two-sided ideal of F and we have $I \subset C \subset E$. Thus C/I is a two-sided ideal of F/I that is contained in E/I. Pick an arbitrary two-sided ideal of F/I that is contained in E/I and write it as J/I for some two-sided ideal J of F. Then J is contained in E and hence $J \subset C$. It follows that $J/I \subset C/I$. □

A ring is *left artinian* if it doesn't have an infinite strictly-descending chain of left ideals. This allows us to formulate the following lemma.

Lemma 2.4. *Let R and S be rings and let $\phi : R \to S$ be a surjective ring homomorphism. If R is left artinian, then the induced group homomorphism $R^\times \to S^\times$ is surjective as well.*

Proof. See [BL15, Lemma 3.4] □

We shall now state Theorem 1.9 again and prove it.

Theorem 2.5. *Let $E \subset F$ be an extension with finite additive index and let C be the conductor of $E \subset F$. Then:*

(a) *the ring F/C has finite order and $E/C \subset F/C$ has trivial conductor;*
(b) *we have $(F^\times : E^\times) \leq ((F/C)^\times : (E/C)^\times)$ with equality if $\#F$ is finite.*

Proof. (a) Clearly $I = \{x \in F : Fx \subset E\}$ is a left ideal of F with $I \subset E$. Regard F and I as left F-modules via left multiplication with quotient module F/I and associated ring homomorphism $\lambda : F \to \mathrm{End}(F/I)$. Then

$$\ker \lambda = \{x \in F : xF \subset I\} = \{x \in F : FxF \subset E\} = C.$$

Now regard F and E as right E-modules via right multiplication. The quotient module F/E yields a ring homomorphism $E \to \mathrm{End}(F/E)^{\mathrm{opp}}$. Its kernel is I and it reduces to an embedding $E/I \hookrightarrow \mathrm{End}(F/E)^{\mathrm{opp}}$. Consequently, the ring E/I has finite order and therefore F/I has finite order as well. The kernel of λ is C, so λ reduces to an embedding $F/C \hookrightarrow \mathrm{End}(F/I)$ and thus F/C has finite order. Lemma 2.3 yields $C(E/C \subset F/C) = 0$.

(b) The natural ring homomorphism $F \to F/C$ induces a group homomorphism $q : F^\times \to (F/C)^\times$. Since $q^{-1}((E/C)^\times) = E^\times$, the homomorphism q reduces to an embedding of sets $\overline{q} : F^\times/E^\times \hookrightarrow (F/C)^\times/(E/C)^\times$ and the inequality follows. If F has finite order, it is left artinian. According to Lemma 2.4 the map q is then surjective. The map $\overline{q}$ is then surjective as well, so we obtain an equality of unit indices. □

The inequality in part (b) of Theorem 2.5 can be strict. In fact, Example 2.6 shows that $(F^\times : E^\times)$ need not even divide $((F/C)^\times : (E/C)^\times)$.

Example 2.6. Let $\mathbb{H}$ be the $\mathbb{R}$-algebra of Hamilton quaternions. The map $\overline{\cdot} : \mathbb{H} \to \mathbb{H}, a + bi + cj + dk \mapsto a - bi - cj - dk$ is a ring antiautomorphism and $x\overline{x} = a^2 + b^2 + c^2 + d^2 \in \mathbb{R}_{\geq 0}$ for all $x = a + bi + cj + dk \in \mathbb{H}$.

Set $\zeta = (1 + \sqrt{-11})/2$, with $\sqrt{-11} = \sqrt{11} \cdot i$, and set $F = \mathbb{Z}[\zeta][j] \subset \mathbb{H}$. We have $\{\pm 1, \pm j\} \subset F^\times$. We now show the opposite inclusion holds. Note that $x\overline{x} \in F \cap \mathbb{R}_{\geq 0} = \mathbb{Z}_{\geq 0}$ for all $x \in F$. Let $x \in F^\times$ and set $y = x^{-1}$. Then $x\overline{x}y\overline{y} = x \cdot y\overline{y} \cdot \overline{x} = xy\overline{xy} = 1$ and it follows that $x\overline{x} = 1$. Write $x = (a + b\sqrt{-11})/2 + (c + d\sqrt{-11})j/2$ with $a, b, c, d \in \mathbb{Z}$ to obtain

$$4 = 4x\overline{x} = a^2 + 11b^2 + c^2 + 11d^2.$$

Then $b = d = 0$ and we have either $a = \pm 2$ and $c = 0$ or we have $a = 0$ and $c = \pm 2$. Hence x is an element of $\{\pm 1, \pm j\}$ and therefore $F^\times = \{\pm 1, \pm j\}$.

The polynomial $g = x^2 - x + 3 \in \mathbb{Z}[x]$ has ζ as zero, so there is a natural ring isomorphism $\mathbb{Z}[\zeta] \to \mathbb{Z}[x]/(g)$. By reducing coefficients modulo 2, one obtains a surjective ring homomorphism $\mathbb{Z}[x]/(g) \to \mathbb{F}_2[x]/(x^2+x+1)$. The polynomial $x^2 + x + 1 \in \mathbb{F}_2[x]$ is irreducible, so there is a ring isomorphism $\mathbb{F}_2[x]/(x^2 + x + 1) \to \mathbb{F}_4$. This describes a chain of ring homomorphisms

$$\mathbb{Z}[\zeta] \to \mathbb{Z}[x]/(g) \to \mathbb{F}_2[x]/(x^2 + x + 1) \to \mathbb{F}_4$$

with composition $\phi : \mathbb{Z}[\zeta] \to \mathbb{F}_4$. This is a surjective ring homomorphism.

Consider $\mathbb{F}_4[j] = \mathbb{F}_4 \oplus \mathbb{F}_4\, j$ and endow it with a ring structure via the relations $j^2 = 1$ and $jx = x^2 j$ for all $x \in \mathbb{F}_4$. Set $\overline{F} = \mathrm{End}_{\mathbb{F}_2}(\mathbb{F}_4)$. One readily checks that $\psi : \mathbb{F}_4[j] \to \overline{F}, a + bj \mapsto (x \mapsto ax + bx^2)$ is well-defined and an injective ring homomorphism. Since $\#\,\mathbb{F}_4[j] = 16 = \#\overline{F}$, the map ψ is an isomorphism. We can now define the surjective ring homomorphism $q : F \to \overline{F}, a + bj \mapsto \psi(\phi(a) + \phi(b)j)$.

Consider $W = \{0, \phi(\zeta)\}$ as an $\mathbb{F}_2$-subspace of $\mathbb{F}_4$ and define the subring $\overline{E} = \mathrm{Fix}_{\mathbb{F}_2}(W, \mathbb{F}_4)$ of $\overline{F}$. For $E = q^{-1}(\overline{E})$ the map q induces isomorphisms $F/(\ker q) \cong \overline{F}$ and $E/(\ker q) \cong \overline{E}$. The extension $\overline{E} \subset \overline{F}$ has trivial conductor, because the only proper two-sided ideal of $\overline{F}$ is the zero ideal. Set $C = C(E \subset F)$. Then Lemma 2.3 yields $C = \ker q$ and we therefore obtain $((F/C)^\times : (E/C)^\times) = (\overline{F}^\times : \overline{E}^\times) = 6/2 = 3$. Note that j is not contained in E, because $q(j)y = \psi(j)y = y^2 = 1 + y \notin W$ for $y = \phi(\zeta)$. Consequently, we find that $E^\times = \{\pm 1\}$ and $(F^\times : E^\times) = 4/2 = 2$. We observe that the unit index $(F^\times : E^\times) = 2$ doesn't divide $((F/C)^\times : (E/C)^\times) = 3$.

Remark 2.7. Let $n \in \mathbb{N}$ and let $E \subset F$ be an extension that has additive index n. By part (b) of Theorem 2.5, we have $(F^\times : E^\times) \leq (F : C)$ with $C = C(E \subset F)$. Our proof of Theorem 2.5 yields

$$(F^\times : E^\times) \leq (F : C) \leq n^{l(l+1)^2}$$

with $l = (\log n)/(\log 2)$. The more symmetric proof of the first statement of part (a) of Theorem 2.5 from [BL15, Lemma 3.7] yields a smaller bound, namely $(F : C) \leq n^{(l+1)^2}$. Both bounds show that $u(n)$, the supremum of the unit indices of all extensions with additive index n, is finite for all $n \in \mathbb{N}$.

We reformulate our definition of a cosy extension from Section 1 using the notion of the conductor of an extension. These two definitions of a cosy extension are equivalent due to Lemma 2.2.

Definition 2.8. An extension $E \subset F$ is *cosy* if E is a maximal subring of F and $E \subset F$ has finite index and trivial conductor.

Lemma 2.9. *Let $E \subset F$ be cosy and let I be a non-zero two-sided ideal of F. Then I is not contained in E and we have $E + I = F$.*

Proof. The conductor of $E \subset F$ is trivial, so I is not contained in E. The ring E is therefore a proper subring of $E + I$. Together with the maximality of E, this implies that $E + I = F$. □

Proposition 2.10. *Let $E \subset F$ be cosy. Then F has finite order and prime characteristic. Furthermore, $\#F$ and $(F : E)$ are prime powers.*

Proof. From part (a) of Theorem 2.5 it follows that F has finite order. Let p be a prime number that divides $\#F$ and consider the two-sided ideal $I = \{x \in F : px = 0\}$ of F. By Cauchy's Theorem there exists an element of additive order p in F, so $I \neq 0$ and thus $E + I = F$ by Lemma 2.9. We have $pF = pE + pI = pE \subset E$, so pF is a two-sided ideal of F that is contained in E. It follows that $pF = 0$ and therefore F has characteristic p. Consequently, every non-zero element of F has order p, so $\#F$ and $(F : E)$ are positive powers of p. □

Corollary 2.11. *Suppose that $E \subset F$ is a maximal extension. Then $(F : E)$ is infinite or a prime power.*

Proof. If the additive index $(F : E)$ is infinite there is nothing to prove, so suppose $(F : E)$ is finite. Set $C = C(E \subset F)$. Then the extension $E/C \subset F/C$ is maximal and thus cosy by Theorem 2.5. The result now follows directly from Proposition 2.10. □

3. Maximal subrings of simple rings

Recall that a ring is *simple* if it has precisely two two-sided ideals. This section is dedicated to the classification of maximal subrings of simple rings with finite order. It should be noted that simple rings and semisimple rings are strongly related. We recall some theory from [Lam01, §2–4].

A left module is *simple* if it has precisely two submodules. A left module is *semisimple* if it is a direct sum of simple left modules. A ring R is *semisimple* if every short exact sequence of left R-modules splits, or equivalently if every left R-module is semisimple. Every semisimple ring is a finite direct product of simple, semisimple rings. A ring is simple and semisimple if and only if it is isomorphic to a linear-endomorphism ring of a non-zero, finite-dimensional vector space over a division ring; if the ring has finite order, this division ring is a field. Every simple, semisimple ring has a unique simple left module up to isomorphism. The *Jacobson radical* of a ring R is the intersection of all maximal left ideals of R and is denoted by $J(R)$; it is a two-sided ideal of R. Clearly, $J(R) = 0$ if R is a simple ring. A one-sided or two-sided ideal I of a ring R is *nilpotent* if $I^k = 0$ for some $k \in \mathbb{N}$.

Lemma 3.1. *Let R be a ring of finite order. Then $J(R)$ is the greatest nilpotent two-sided ideal of R. Furthermore, R is a semisimple ring if and only if $J(R) = 0$.*

Proof. By [Lam01, Theorem 4.12], the Jacobson radical of a left artinian ring is its greatest nilpotent left ideal. By [Lam01, Theorem 4.14], a ring is semisimple if and only if it is left artinian and its Jacobson radical is trivial. Since R has finite order, R is left artinian and Lemma 3.1 follows. □

It follows from Lemma 3.1 that a simple ring of finite order is always semisimple, and thus isomorphic to $\mathrm{End}_K(V)$ for some finite field K and some non-zero, finite-dimensional K-vector space V. Hence we may assume that our simple rings of finite order are of this form.

Notation 3.2. Throughout this section we let K be a finite field and we let V be a non-zero, finite-dimensional K-vector space.

Lemma 3.3. *Let E be a subring of $\mathrm{End}_K(V)$ and let I be a non-zero left ideal of E. Then $I \cdot V$ is a non-zero subspace of V that is fixed by E.*

Proof. The set $I \cdot V$ is per definition closed under addition and the equalities $K \cdot I \cdot V = I \cdot K \cdot V = I \cdot V$ show that it is closed under scalar multiplication, so $I \cdot V$ is a subspace of V. We have $I \cdot V \neq 0$, because $\mathrm{End}_K(V)$ and therefore I act faithfully on V. Finally, E fixes $I \cdot V$ because $E \cdot I = I$. □

Lemma 3.4. *Let W be a proper, non-zero subspace of V. Define the ring $E = \mathrm{Fix}_K(W, V)$. Then $J(E) \neq 0$ and $J(E) \cdot V = W$.*

Proof. Regard V and W as left E-modules, let V/W be the quotient module and define the two-sided ideal $I = \mathrm{Ann}_E(W) \cap \mathrm{Ann}_E(V/W)$ of E. By [Lam01, Corollary 4.2], the Jacobson radical of a ring equals the intersection of the annihilators of its simple left modules. Both W and V/W are simple left E-modules, so $J(E) \subset I$. Note that I consists of all $x \in E$ such that $xW = 0$ and $xV \subset W$. We observe that $I^2 = 0$. Lemma 3.1 yields $I \subset J(E)$, so that $J(E) = I \neq 0$ and $J(E) \cdot V = I \cdot V = W$. □

Lemma 3.5. *Let E be a maximal subring of $\mathrm{End}_K(V)$. Then the following statements are equivalent:*

(a) *we have $E = \mathrm{Fix}_K(W, V)$ for a proper, non-zero subspace W of V;*
(b) *the ring E is not simple;*
(c) *the ring E fixes a proper, non-zero subspace of V.*

Proof. It follows immediately from Lemma 3.4 that (a) implies (b).

Next, we show that (b) implies (c). By Lemma 3.3 it suffices to find a non-zero left ideal I of E such that $I \cdot V \subsetneq V$. First suppose that $J(E) \neq 0$. Set $I = J(E)$. If $I \cdot V = V$, then we have $I^k \cdot V = V$ for all $k \in \mathbb{N}$, but this is absurd since I is nilpotent by Lemma 3.1. Thus $I \cdot V$ is a proper subspace of V. Now suppose that $J(E) = 0$. Then E is semisimple by Lemma 3.1 and therefore a direct product of two or more rings. It follows that E contains an idempotent $e \in Z(E)$ with $e \notin \{0, 1\}$. Let I be the left ideal of E generated by e. We have $(1 - e) \cdot I \cdot V = (1 - e)eV = 0$, so $I \cdot V \subsetneq V$.

Finally, we show that (c) implies (a). Let W be a proper, non-zero subspace that is fixed by E. Then $\mathrm{Fix}_K(W, V)$ is a proper subring of $\mathrm{End}_K(V)$. We have $E \subset \mathrm{Fix}_K(W, V)$ and the maximality of E implies that $E = \mathrm{Fix}_K(W, V)$. □

In Lemma 3.5 we have described the non-simple, maximal subrings of $\mathrm{End}_K(V)$. We describe the simple, maximal subrings E of $\mathrm{End}_K(V)$ by separating them into two cases: either $Z(F)$ is contained in E or it isn't.

Lemma 3.6. *Let E be a maximal, simple subring of $F = \mathrm{End}_K(V)$. Identify K with $Z(F)$ and set $L = Z(E)$. Suppose that $K \not\subset E$. Then:*

(a) *we have a field extension $L \subset K$ of prime degree and there exists a ring isomorphism $F \to K \otimes_L E$ that is the identity on E;*
(b) *there exists an L-subspace W of V with $\dim_L W = \dim_K V$ such that $K \cdot W = V$ and $E = \mathrm{Fix}_K(W, V)$.*

Proof. (a) We have $E \subsetneq K \cdot E$, because $K \not\subset E$. The maximality of E implies that $K \cdot E = F$ and since L centralises both E and K, we obtain $L \subsetneq Z(F) = K$. Set $D = K \otimes_L E$. Regard V as a left E-module and let W be a simple submodule. Then $E \cong \mathrm{End}_L(W)$ and $D \cong \mathrm{End}_K(K \otimes_L W)$, so D is simple. The ring homomorphism $D \to F, x \otimes y \mapsto xy$ is surjective because $F = K \cdot E$ and is injective because D is simple. This isomorphism is the identity on E and its inverse is the desired map. Finally, if $L \subset K$ is not of prime degree, there exists a subfield $L \subsetneq M \subsetneq K$ and we have $E \subsetneq M \otimes_L E \subsetneq D$, which contradicts the maximality of E.

(b) Let D and W be as in (a). Then W is an L-vector space with dimension $\dim_K V$, because $\mathrm{End}_K(K \otimes_L W) \cong D \cong F$. Secondly, we have

$$K \cdot W = K \cdot E \cdot W = F \cdot W = V.$$

Finally, we have $E \subset \mathrm{Fix}_K(W, V) \subsetneq F$ and thus the maximality of E yields $E = \mathrm{Fix}_K(W, V)$. □

Lemma 3.7. *Let E be a maximal, simple subring of $F = \mathrm{End}_K(V)$. Identify K with $Z(F)$ and set $L = Z(E)$. Suppose that $K \subset E$. Then $K \subset L$ is a field extension of prime degree, V is an L-vector space and $E = \mathrm{End}_L(V)$.*

Proof. It is clear that $K \subset L$ is a field extension. Since V is a left E-module, it is also an L-vector space. The E-submodules of V are K-subspaces. If such a submodule is non-zero and proper, part (c) of Lemma 3.5 shows that E is not simple, which is absurd. Hence V is a simple left E-module and thus $E = \mathrm{End}_L(V)$. It follows that $K \subsetneq L$. If the field extension $K \subset L$ is not of prime degree, there is a subfield $K \subsetneq M \subsetneq L$ and we have $E \subsetneq \mathrm{End}_M(V) \subsetneq \mathrm{End}_K(V)$, which contradicts the maximality of E. □

We now show the subrings of $\mathrm{End}_K(V)$ that appear in Lemmas 3.5 to 3.7 are maximal subrings. Note that any proper subring of $\mathrm{End}_K(V)$ is contained in a maximal subring, because $\mathrm{End}_K(V)$ has finite order.

Example 3.8. Let W be a proper, non-zero subspace of V and set $E = \mathrm{Fix}_K(W, V)$. Let D be a maximal subring of $\mathrm{End}_K(V)$ with $E \subset D$. Suppose that D is simple. We have $K \subset E \subset D$, so $D = \mathrm{End}_L(V)$ for a field

extension $K \subset L$ of prime degree by Lemma 3.7. The ring E contains an element x with a one-dimensional K-subspace of V as image. However, x is also contained in D, so the image of x is an L-subspace of V as well, which is absurd. It follows that D is not simple and therefore we have $D = \mathrm{Fix}_K(U, V)$ for a proper, non-zero K-subspace U of V by Lemma 3.5. Clearly E only fixes a single proper, non-zero K-subspace of V, so $U = W$ and $D = E$. Hence E is a maximal subring of $\mathrm{End}_K(V)$.

Example 3.9. Let $L \subset K$ be a field extension of prime degree and let W be an L-subspace of V such that $\dim_L W = \dim_K V$ and $K \cdot W = V$. Set $E = \mathrm{Fix}_K(W, V)$. If E is not a maximal subring of $\mathrm{End}_K(V)$, there exists a maximal subring $E \subset D \subsetneq F$. Suppose that $K \subset D$. Then it is not difficult to see that $F = K \cdot \mathrm{Fix}_K(W, V) = K \cdot E \subset D$, which is absurd. Consequently, $K \not\subset D$ and thus D is simple by Lemma 3.5. We find that $D = \mathrm{Fix}_K(U, V)$ for some field extension $M \subset K$ of prime degree and M-subspace U of V, using Lemma 3.6. We have $L \subset D \cap Z(F) \subset Z(D) = M$ and thus $L = M$, because $L \subset K$ has prime degree. Clearly $E = \mathrm{Fix}_K(W, V)$ is isomorphic to $\mathrm{End}_L(W)$, so E is simple. View U as a left E-module. Then U contains a simple left E-submodule that is an L-subspace with dimension $\dim_L W$, which equals $\dim_K V$. However, we have $\dim_L U = \dim_K V$, so U is a simple left E-module. Thus $D = E$ and hence E is a maximal subring of $\mathrm{End}_K(V)$.

Example 3.10. Let $K \subset L$ be a field extension of prime degree such that V is also an L-vector space. Set $E = \mathrm{End}_L(V)$. If E is not a maximal subring of $\mathrm{End}_K(V)$, there is a maximal subring $E \subset D \subsetneq F$. Since V is a simple left E-module, V is a simple left D-module as well. Using parts (b) and (c) of Lemma 3.5, the ring D is simple. Furthermore, we have $K \subset E \subset D$, so $D = \mathrm{End}_M(V)$ for some field extension $K \subset M$ of prime degree by Lemma 3.7. Clearly all elements of M commute with L, so $M \subset E$ and thus $M \subset L$. Since $K \subset L$ has prime degree, we find that $M = L$ and $D = E$, so E is a maximal subring of $\mathrm{End}_K(V)$.

Proposition 3.11. *The collection of maximal subrings of* $\mathrm{End}_K(V)$ *consists of the following three subcollections of subrings:*

A. *the subrings* $\mathrm{Fix}_K(W, V)$ *for all proper, non-zero subspaces* W *of* V*;*
B. *the subrings* $\mathrm{Fix}_K(W, V)$ *for all field extensions* $L \subset K$ *of prime degree and all* L*-subspaces* W *of* V *with* $\dim_L W = \dim_K V$ *and* $K \cdot W = V$*;*
C. *the subrings* $\mathrm{End}_L(V)$ *for all field extensions* $K \subset L$ *of prime degree and all* L*-vector-space structures on* V *that extend the* K*-vector-space structure on* V*.*

Proof. By Examples 3.8 to 3.10, the three collections consist of maximal subrings of $\mathrm{End}_K(V)$. Now let E be a maximal subring of $\mathrm{End}_K(V)$. If E is not simple, then E is contained in collection A by Lemma 3.5. Otherwise, E is simple. If $Z(F) \not\subset E$, then E is contained in collection B by Lemma 3.6. If $Z(F) \subset E$, then E is contained in collection C by Lemma 3.7. □

4. Semisimple, cosy extensions

In this section we prove the semisimple version of Theorem 1.8, namely Theorem 4.8. First, we restate Example 1.2 and show it describes semisimple, cosy extensions.

Example 4.1. Let K be a finite field and let V be a non-zero, finite-dimensional K-vector space. Consider the subring $E = \mathrm{Diag}_K(V)$ of the semisimple ring $F = \mathrm{End}_K(V) \times \mathrm{End}_K(V)$. Clearly, $E \subset F$ has finite additive index. We have $E \cong \mathrm{End}_K(V)$, so E is simple and the zero ideal is the only proper two-sided ideal of E; thus $C(E \subset F) = 0$. Now let D be a proper subring of F with $E \subset D$. Regard D/E, F/E and $\mathrm{End}_K(V)$ as left $E \otimes_{\mathbb{Z}} E^{\mathrm{opp}}$-modules in the natural manner. Then $\mathrm{End}_K(V)$ is a simple module, because its submodules are precisely its two-sided ideals when viewed as a ring. Moreover, F/E is isomorphic to $\mathrm{End}_K(V)$ as a module and is therefore simple as well. Then $D/E = 0$ and $D = E$, so E is a maximal subring of F. It follows that $E \subset F$ is cosy.

Lemma 4.2. *Let $E \subset F$ be an extension such that F is simple. Then $E \subset F$ is cosy if and only if it is maximal and F has finite order.*

Proof. The "only if" statement is clear by Proposition 2.10, so suppose that $E \subset F$ is maximal and $\#F$ is finite. The additive index of $E \subset F$ is finite, because F has finite order. Its conductor is trivial, because the only proper two-sided ideal of F is the zero ideal. Hence $E \subset F$ is cosy. □

This lemma allows us to leverage Proposition 3.11 to prove that Examples 1.3 to 1.5 describe cosy extensions, as we shall see now.

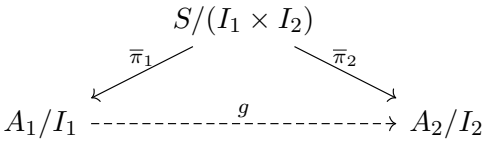
Example 4.3. Let K be a finite field, let V be a finite-dimensional K-vector space and let W be a proper, non-zero subspace of V. Then the extension $\mathrm{Fix}_K(W, V) \subset \mathrm{End}_K(V)$ is cosy by Proposition 3.11 and Lemma 4.2.

Example 4.4. Let K be a finite field, let $L \subset K$ be a field extension of prime degree and let V be a non-zero, finite-dimensional L-vector space. Consider the extension $\mathrm{End}_L(V) \subset K \otimes_L \mathrm{End}_L(V)$, which is isomorphic to the extension $\mathrm{End}_L(V) \subset \mathrm{End}_K(K \otimes_L V)$. We have $\mathrm{End}_L(V) = \mathrm{Fix}_K(V, K \otimes_L V)$, so this is maximal subring of $\mathrm{End}_K(K \otimes_L V)$ by Proposition 3.11. Using Lemma 4.2 it follows that $\mathrm{End}_L(V) \subset K \otimes_L \mathrm{End}_L(V)$ is cosy.

Example 4.5. Let K be a finite field, let $K \subset L$ be a field extension of prime degree and let V be a non-zero, finite-dimensional L-vector space. Then $\mathrm{End}_L(V) \subset \mathrm{End}_K(V)$ is cosy by Proposition 3.11 and Lemma 4.2.

Lemma 4.6 (Goursat). *Let R_1 and R_2 be rings and let $S \subset R_1 \times R_2$ be a subset. Then S is a subring of $R_1 \times R_2$ if and only if there exist subrings $A_1 \subset R_1$ and $A_2 \subset R_2$ with two-sided ideals $I_1 \subset A_1$ and $I_2 \subset A_2$ such that S is the graph of a ring isomorphism $g : A_1/I_1 \to A_2/I_2$, which is to say that $S = \bigcup_{x \in A_1} (x + I_1) \times g(x + I_1)$.*

Proof. Suppose first that S is a subring of $R_1 \times R_2$. Let $\pi_1 : S \to R_1$ and $\pi_2 : S \to R_2$ be the projection maps. Set $A_1 = \pi_1(S)$, $A_2 = \pi_2(S)$, $I_1 = \pi_1(\ker \pi_2)$ and $I_2 = \pi_2(\ker \pi_1)$. Then I_1 and I_2 are two-sided ideals of A_1 and A_2 respectively, because they are images of two-sided ideals under a surjective map. Note that $\ker \pi_2 = I_1 \times 0$ and $\ker \pi_1 = 0 \times I_2$. Now $I_1 \times I_2$ is a two-sided ideal of S with $\pi_1(I_1 \times I_2) = I_1$ and $\pi_2(I_1 \times I_2) = I_2$ so that both projections reduce to ring isomorphisms:



Then $g = \overline{\pi}_2 \circ \overline{\pi}_1^{-1} : A_1/I_1 \to A_2/I_2$ is a ring isomorphism with

$$S = \{(x_1, x_2) : g(x_1 + I_1) = x_2 + I_2\} = \bigcup_{x \in A_1} (x + I_1) \times g(x + I_1).$$

For the opposite implication, suppose S is the graph of such an isomorphism g. Consider the subring $S' = \{(x + I_1, g(x + I_1)) : x \in A_1\}$ of $A_1/I_1 \times A_2/I_2$. Then S is the inverse image of S' under the natural ring homomorphism $A_1 \times A_2 \to A_1/I_1 \times A_2/I_2$ and thus a subring of $R_1 \times R_2$. □

Lemma 4.7. *Let $E \subset F$ be semisimple and cosy. Suppose that F is not simple. Then E is simple and there exists an isomorphism $F \to E \times E$ that maps E bijectively to the diagonal.*

Proof. There exists an isomorphism $\phi : F \to R_1 \times R_2$ with R_1 simple and R_2 semisimple. By Lemma 4.6 there are subrings $A_1 \subset R_1$ and $A_2 \subset R_2$ with two-sided ideals $I_1 \subset A_1$ and $I_2 \subset A_2$ such that $\phi(E)$ is the graph of an isomorphism $g : A_1/I_1 \to A_2/I_2$. If $A_1 \neq R_1$ then $\phi(E) = A_1 \times R_2$ by the maximality of E and thus $0 \neq 0 \times R_2 \subset C(E \subset F) = 0$, which is absurd. Hence we have $A_1 = R_1$ and similarly $A_2 = R_2$. But then $I_1 \times I_2$ is a two-sided ideal of $\phi(F) = R_1 \times R_2$ that is contained in $\phi(E)$, so $I_1 \times I_2 = 0$. We can now regard g as an isomorphism from R_1 to R_2 with $\phi(E)$ as its graph. Then $\psi : R_1 \to E, x \mapsto \phi^{-1}(x, g(x))$ is an isomorphism, so E is simple and $(\psi, \psi \circ g^{-1}) \circ \phi : F \to E \times E$ is the desired isomorphism. □

We shall now formulate the semisimple version of Theorem 1.8 and prove it. The proof requires some basic theory of semisimple rings. At the start of Section 3 we provided a short overview.

Theorem 4.8. *Define the following parametrised families of ring extensions with parameters as indicated:*

I. $\mathrm{Diag}_K(V) \subset \mathrm{End}_K(V) \times \mathrm{End}_K(V)$ *with* $K = \mathbb{F}_{p^k}$ *and* $V = K^n$ *for all primes* p *and* $k, n \in \mathbb{N}$*;*

II. $\mathrm{Fix}_K(W, V) \subset \mathrm{End}_K(V)$ *with* $K = \mathbb{F}_{p^k}$, $V = K^n$ *and* $W = K^m \times 0$ *for all primes* p *and* $k, n, m \in \mathbb{N}$ *such that* $m < n$*;*

III. $\mathrm{End}_L(V) \subset K \otimes_L \mathrm{End}_L(V)$ *with* $K = \mathbb{F}_{p^{kd}}$, $L = \mathbb{F}_{p^k}$ *and* $V = L^n$ *for all primes* p, *primes* d, *and* $k, n \in \mathbb{N}$;

IV. $\mathrm{End}_L(V) \subset \mathrm{End}_K(V)$ *with* $K = \mathbb{F}_{p^k}$, $L = \mathbb{F}_{p^{kd}}$ *and* $V = L^n$ *for all primes* p, *primes* d, *and* $k, n \in \mathbb{N}$.

Then each of these families consists of semisimple, cosy extensions and every semisimple, cosy extension is isomorphic to precisely one of these extensions.

Proof. Examples 4.1 and 4.3 to 4.5 illustrate that the families I–IV consist of semisimple, cosy extensions. For the second part, it suffices to show that (a) every cosy extension is isomorphic to an extension in a family, that (b) extensions in different families are non-isomorphic, and that (c) different parameters yield non-isomorphic extensions within a family.

(a) Let $E \subset F$ be semisimple and cosy. If this extension isn't simple, it is isomorphic to an extension in Example 4.1 by Lemma 4.7. If it is simple, it is isomorphic to an extension in Examples 4.3 to 4.5 by Lemmas 4.2 and 3.5 to 3.7. It is not difficult to see that any extension in these examples is isomorphic to an extension described by one of the families I–IV.

(b) We make note of a unique property of each family: the larger ring in family I is not simple; the subring in family II is not simple; the subring and larger ring in family III are simple and the centre of the larger ring is not contained in the subring; the subring and the larger ring in family IV are simple and the centre of the larger ring is contained in the subring. Consequently, two extensions in different families are non-isomorphic.

(c) For families I, III and IV, an isomorphism of extensions clearly implies the equality of parameters. For family II, an isomorphism between two extensions $E_i = \mathrm{Fix}_{K_i}(W_i, V_i) \subset F_i = \mathrm{End}_{K_i}(V_i)$ for $i \in \{1, 2\}$ yields $K_1 = K_2$ and $V_1 = V_2$. Moreover, such an isomorphism induces a simple left-F_1-module structure on V_2 and therefore there exists a left-F_1-module isomorphism $\phi : V_1 \to V_2$. We have $\phi(W_1) = \phi(J(E_1) \cdot V_1) = J(E_2) \cdot V_2 = W_2$ by Lemma 3.4 and since ϕ is also K_1-linear, we obtain $W_1 = W_2$. It follows that the parameters of the two extensions are equal. □

5. Unit indices of cosy extensions

In this section we determine an upper bound and a lower bound for the unit indices of cosy extensions in terms of the additive index.

Lemma 5.1. *Let* R *be a ring and let* I *be a two-sided ideal of* R. *Suppose that* $1 + I \subset R^\times$. *Then the natural group homomorphism* $R^\times \to (R/I)^\times$ *reduces to a group isomorphism* $R^\times/(1 + I) \to (R/I)^\times$.

Proof. Let $q : R^\times \to (R/I)^\times$ be the natural group homomorphism. Its kernel is $(1 + I) \cap R^\times = 1 + I$. It remains to show that ϕ is surjective. Let $x+I \in (R/I)^\times$ and let $y+I \in (R/I)^\times$ be its inverse. Then $xy+I = yx+I = 1 + I \subset R^\times$, so xy and yx are units. Consequently, we have $xya = byx = 1$ for some $a, b \in R^\times$, so x is a unit that satisfies $\phi(x) = x + I$. □

Lemma 5.2. *Let $E \subset F$ be an extension and let I be a nilpotent two-sided ideal of F. If $E + I$ has finite order, then $((E + I) : E) = ((E + I)^\times : E^\times)$.*

Proof. Define the ring $D = E + I$. We have $1 + I \subset D^\times$ because I is nilpotent, and we have $E/(E \cap I) \cong D/I$. The two-sided ideal $E \cap I$ of E is nilpotent, so $1 + (E \cap I) \subset E^\times$. Now Lemma 5.1 yields

$$D^\times/(1 + I) \cong (D/I)^\times \cong (E/(E \cap I))^\times \cong E^\times/(1 + (E \cap I)).$$

Using the fact that D has finite order, these isomorphisms allow us to deduce that $(D : E) = (I : (E \cap I)) = ((1 + I) : (1 + (E \cap I))) = (D^\times : E^\times)$. □

With this lemma, we can prove Corollary 5.3. It describes the unit index in terms of the additive index for every non-semisimple, cosy extension. We refer to Section 8 for more properties of non-semisimple, cosy extensions.

Corollary 5.3. *Let $E \subset F$ be cosy. Suppose that F is not semisimple. Then we have $(F : E) = (F^\times : E^\times)$.*

Proof. The ring F has finite order by Proposition 2.10 and the Jacobson radical $J(F)$ of F is nilpotent and non-zero by Lemma 3.1. We then have $E + J(F) = F$ by Lemma 2.9 and $(F : E) = (F^\times : E^\times)$ by Lemma 5.2. □

Lemma 5.4. *Let $t \in \mathbb{N}$ with $t > 1$ and let $a, b \in \mathbb{N}$ be numbers satisfying $b \leq a$. Then $(t^a - 1)/(t^b - 1) \in [t^{a-b}, (t + 1)^{a-b}]$. Furthermore, the upper bound is assumed if and only if either $a = 2$ and $b = 1$ or $a = b$.*

Proof. Let r be the integer remainder after division of a by b. We have $0 \leq r < b$ and

$$\frac{t^a - 1}{t^b - 1} = t^{a-b} + \frac{t^{a-b} - 1}{t^b - 1} = \cdots = t^{a-b} + t^{a-2b} + \cdots + t^r + \frac{t^r - 1}{t^b - 1}.$$

The terms in the final sum are non-negative, so the sum is at least t^{a-b}. The coefficients of $t^{a-b}, t^{a-2b}, \ldots, t^r$ in the final sum are all 1. The final term is strictly less than 1 and is zero if $r = 0$. In the binomial expansion of $(t + 1)^{a-b}$ in $\mathbb{Z}[t]$, the coefficients of $t^0, t^1, \ldots, t^{a-b}$ are all at least 1, so $(t^a - 1)/(t^b - 1) \leq (t + 1)^{a-b}$.

For the second part, the "if" statement is clear, so suppose the upper bound is reached. The previous remarks imply that $r = 0$. Moreover, if $a - b > 1$, the coefficient of t in the binomial expansion of $(t + 1)^{a-b}$ is $a - b > 1$ and the upper bound is not reached. So $b \mid a$ and $a - b \in \{0, 1\}$. It follows that either $a = 2$ and $b = 1$ or $a = b$. □

We shall now determine the additive index and the unit index of every extension listed in Theorem 4.8, the classification of semisimple, cosy extensions. Each of the four families listed in Theorem 4.8 is treated, in order, by one of the following four examples.

Example 5.5. Let q be a prime power and let $n \in \mathbb{N}$. Consider the rings $E = \mathrm{Diag}_K(V)$ and $F = \mathrm{End}_K(V) \times \mathrm{End}_K(V)$ with $K = \mathbb{F}_q$ and $V = K^n$. We have $(F : E) = \#E = q^{n^2}$. The map from $E^\times$ to the set of ordered bases of K^n that sends a unit to the sequence of images of the standard basis vectors, is bijective. We find

$$(F^\times : E^\times) = \#E^\times = \prod_{i=0}^{n-1}(q^n - q^i) = \prod_{i=0}^{n-1} q^i(q^{n-i} - 1).$$

This number is clearly contained in $[(q-1)^{n^2}, q^{n^2}]$.

Example 5.6. Let q be a prime power and let $n, m \in \mathbb{N}$ with $m < n$. Consider the subring $E = \mathrm{Fix}_K(W, V)$ of $F = \mathrm{End}_K(V)$ with $K = \mathbb{F}_q$, $V = K^n$ and $W = K^m \times 0$. We have $(F : E) = q^{m(n-m)}$. Let $F^\times$ act transitively on the set X of m-dimensional subspaces of V. Under this action, $E^\times$ is the stabiliser of W and $(F^\times : E^\times) = \#X$ by the Orbit-Stabiliser Theorem. By counting as in Example 5.5, we obtain

$$(F^\times : E^\times) = \prod_{i=0}^{m-1} \frac{q^n - q^i}{q^m - q^i} = \prod_{i=0}^{m-1} \frac{q^{n-i} - 1}{q^{m-i} - 1}.$$

According to Lemma 5.4 this number is contained in $[q^{m(n-m)}, (q+1)^{m(n-m)}]$.

Example 5.7. Let q be a prime power, let d be a prime and let $n \in \mathbb{N}$. Consider the subring $E = \mathrm{End}_L(V)$ of $F = K \otimes_L \mathrm{End}_L(V)$ with $K = \mathbb{F}_{q^d}$, $L = \mathbb{F}_q$ and $V = L^n$. Due to Example 5.5, we know the orders of E and F and the orders of their unit groups. We obtain $(F : E) = q^{(d-1)n^2}$ and

$$(F^\times : E^\times) = \prod_{i=0}^{n-1} \frac{q^{di}(q^{d(n-i)} - 1)}{q^i(q^{n-i} - 1)}.$$

This product is contained in $[q^{(d-1)n^2}, (q+1)^{(d-1)n^2}]$ by Lemma 5.4.

Example 5.8. Let q be a prime power, let d be a prime and let $n \in \mathbb{N}$. Consider the subring $E = \mathrm{End}_L(V)$ of $F = \mathrm{End}_K(V)$ with $K = \mathbb{F}_q$, $L = \mathbb{F}_{q^d}$ and $V = L^n$. We determined the orders of E and F and the orders of their unit groups in Example 5.5. We obtain $(F : E) = q^{d(d-1)n^2}$ and

$$(F^\times : E^\times) = \frac{\prod_{i=0}^{dn-1} q^i(q^{dn-i} - 1)}{\prod_{i=0}^{n-1} q^{di}(q^{dn-di} - 1)} = \prod_{\substack{i=0 \\ d \nmid i}}^{dn-1} q^i(q^{dn-i} - 1).$$

This product is contained in $[(q-1)^{d(d-1)n^2}, q^{d(d-1)n^2}]$.

We can now determine an upper bound and a lower bound for the unit indices of cosy extensions in terms of the additive index. Before we formulate Proposition 5.9, we recall that $\#F$ and $(F : E)$ are prime powers for any cosy extension $E \subset F$ according to Proposition 2.10.

Proposition 5.9. *Let $E \subset F$ be cosy. Write $(F : E) = p^k$ for a prime p and $k \in \mathbb{N}$. Then $(F^\times : E^\times) \in [(p-1)^k, (p+1)^k]$.*

Proof. If F is not semisimple, then $(F^\times : E^\times) = p^k$ by Corollary 5.3. Now suppose that F is semisimple. Then the extension $E \subset F$ is isomorphic to an extension listed in Theorem 4.8. In Examples 5.5 to 5.8 we have determined the additive index and the unit index of every extension described in Theorem 4.8. Therefore, $(F^\times : E^\times)$ is contained in the interval at the end of one of these examples for some power q of p. Such an interval is clearly contained in $[(p-1)^k, (p+1)^k]$. □

Remark 5.10. Let p be a prime number. Corollary 5.3 and the expressions for the additive index and unit index together with the bounds of the unit index in Examples 5.5 to 5.8, allow us to deduce the following. There are only two cosy extensions, up to isomorphism, that reach the upper bound in Proposition 5.9, namely $\mathrm{Fix}_{\mathbb{F}_p}(\mathbb{F}_p \times 0, \mathbb{F}_p^2) \subset \mathrm{End}_{\mathbb{F}_p}(\mathbb{F}_p^2)$ and $\mathbb{F}_p \subset \mathbb{F}_{p^2}$. Both of these have unit index $p+1$. The extension $\mathbb{F}_p \subset \mathbb{F}_p \times \mathbb{F}_p$ along the diagonal is the only cosy extension, up to isomorphism, that assumes the lower bound in Proposition 5.9. It has unit index $p-1$.

6. Bounding the unit index

This section is dedicated to our unit-index theorem, Theorem 1.1. We recall that $u(n)$ is the supremum and $l(n)$ is the infimum of the unit indices of all extensions with additive index n, for all $n \in \mathbb{N}$. If A is a finite abelian group, then $u(A)$ is the supremum and $l(A)$ is the infimum of the unit indices of all extensions $E \subset F$ with $F/E \cong A$. We defined $u_{\mathrm{fin}}(n)$, $l_{\mathrm{fin}}(n)$, $u_{\mathrm{fin}}(A)$ and $l_{\mathrm{fin}}(A)$ analogously by only taking extensions $E \subset F$ into account for which F has finite order.

We illustrate in Example 6.1 that $l(n) = 1$ for all $n \in \mathbb{N}$. We will later see that it also shows that $l(A) = 1$ for each finite abelian group A.

Example 6.1. Let $n \in \mathbb{Z}$ and define $\zeta = \sqrt{-2}$. Consider the ring $F = \mathbb{Z}[\zeta] = \mathbb{Z} + \mathbb{Z}\,\zeta$ and its subring $E = \mathbb{Z} + nF = \mathbb{Z} + n\,\mathbb{Z}\,\zeta$. Then the additive quotient group F/E is isomorphic to $\mathbb{Z}/n\,\mathbb{Z}$ and thus $(F : E) = n$. Note that the map $\sigma : F \to F, a + b\zeta \mapsto a - b\zeta$ is a ring automorphism. Let $a + b\zeta \in F^\times$ and let $c + d\zeta$ be its inverse. Then

$$1 = (a + b\zeta)(c + d\zeta) \cdot \sigma((a + b\zeta)(c + d\zeta)) = (a^2 + 2b^2)(c^2 + 2d^2)$$

and we deduce that $a^2 + 2b^2 = 1$. This implies that $a = \pm 1$ and $b = 0$, so $F^\times = \{\pm 1\}$ and $(F^\times : E^\times) = 1$. Thus for all $n \in \mathbb{N}$, there exists an extension $E \subset F$ with additive index n and unit index 1.

Theorem 6.2. *Let $n \in \mathbb{N}$. Then both $u(n)$ and $u_{\mathrm{fin}}(n)$ are given by the following expression, in which p ranges over all primes:*

$$\prod_p (p+1)^{\mathrm{ord}_p(n)},$$

we have $l(n) = 1$, and $l_{\mathrm{fin}}(n)$ is given by the above expression but with "$p+1$" replaced by "$p-1$".

Proof. Let $E \subset F$ be an extension with additive index n. Let $E = E_0 \subset E_1 \subset \cdots \subset E_t = F$ be a chain of maximal subrings. By Theorem 2.5, there is a cosy extension $\overline{E}_i \subset \overline{F}_i$ such that $(E_{i+1}^\times : E_i^\times) \leq (\overline{F}_i^\times : \overline{E}_i^\times)$, with equality if F has finite order, and such that its additive index equals $(E_{i+1} : E_i)$ for each $i \in \{0, \ldots, t-1\}$. We have $(F : E) = \prod_{i=0}^{t-1}(E_{i+1} : E_i)$ and $(F^\times : E^\times) = \prod_{i=0}^{t-1}(E_{i+1}^\times : E_i^\times)$. It then follows from Proposition 5.9 that both $u(n)$ and $u_{\text{fin}}(n)$ are bounded from above by the expression in the theorem, while $l_{\text{fin}}(n)$ is bounded from below by the described expression.

Recall from Remark 5.10 that $\mathbb{F}_p \subset \mathbb{F}_{p^2}$ and $\mathbb{F}_p \subset \mathbb{F}_p \times \mathbb{F}_p$ have additive index p and unit indices $p+1$ and $p-1$ respectively for all primes p. Consider the two extensions $\prod_p \mathbb{F}_p^{n_p} \subset \prod_p \mathbb{F}_{p^2}^{n_p}$ and $\prod_p \mathbb{F}_p^{n_p} \subset \prod_p (\mathbb{F}_p \times \mathbb{F}_p)^{n_p}$, where p ranges over all primes, and $n_p = \text{ord}_p(n)$. Both have additive index n. The unit index of the former is the expression in the theorem, while the unit index of the latter is the described expression for $l_{\text{fin}}(n)$. Hence the values of $u(n)$, $u_{\text{fin}}(n)$ and $l_{\text{fin}}(n)$ are as stated. We have $l(n) = 1$ by Example 6.1. $\square$

Lemma 6.3. *Let p be a prime number, let A be a finite abelian p-group and let $E \subset F$ be an extension with trivial conductor and $F/E \cong A$. Then:*

(a) *we have an extension $E \subset E + pF$ with unit index $\#pA$;*
(b) *the interval $[(p-1)^{\dim_{\mathbb{F}_p} A/pA} \cdot \#pA, (p+1)^{\dim_{\mathbb{F}_p} A/pA} \cdot \#pA]$ contains the unit index $(F^\times : E^\times)$.*

Proof. (a) Define the two-sided ideal $I = pF$ of F. Then $E + I$ is a ring. Let $\phi : F/E \to A$ be a group isomorphism. Then ϕ restricts to a group isomorphism from $(E+I)/E = p(F/E)$ to pA and therefore $((E+I) : E) = \#pA$. The two-sided ideal I is nilpotent, because the conductor of $E \subset F$ is trivial and $I^k \subset p^k F \subset E$ for the exponent p^k of A. Note that F has finite order due to Theorem 2.5. Then $E + I$ has finite order as well and Lemma 5.2 gives $((E+I)^\times : E^\times) = ((E+I) : E) = \#pA$.

(b) The map ϕ from (a) induces a group isomorphism $F/(E+I) \to A/pA$. Using Theorem 6.2 we obtain $(F^\times : (E+I)^\times) \in [(p-1)^k, (p+1)^k]$, where $k \in \mathbb{N}$ satisfies $\#(A/pA) = p^k$. Every non-zero element of A/pA has order p, so we can also write $k = \dim_{\mathbb{F}_p} A/pA$. One obtains the statement in the lemma by observing that $(F^\times : E^\times) = (F^\times : (E+I)^\times) \cdot ((E+I)^\times : E^\times)$. $\square$

The following example shows that for any prime p and any $k \in \mathbb{N}$, there exists an extension $E \subset F$ with $F/E \cong A = \mathbb{Z}/p^k\mathbb{Z}$ such that the unit index equals $(p+1)^{\dim_{\mathbb{F}_p} A/pA} \cdot \#pA$ or $(p-1)^{\dim_{\mathbb{F}_p} A/pA} \cdot \#pA$. That is, the upper bound and lower bound in part (b) of Lemma 6.3 are achieved.

Example 6.4. Let p be a prime and let $k \in \mathbb{N}$. Consider the group $A = \mathbb{Z}/p^k\mathbb{Z}$ with upper bound $(p+1)^{\dim_{\mathbb{F}_p} A/pA} \cdot \#pA = (p+1)p^{k-1}$ and lower bound $(p-1)^{\dim_{\mathbb{F}_p} A/pA} \cdot \#pA = (p-1)p^{k-1}$. Set $E = \mathbb{Z}/p^k\mathbb{Z}$, let $f \in E[x]$ be a monic polynomial of degree 2 and set $F = E[x]/(f) = E + Ex$. Then $E \subset F$ has trivial conductor and F/E is isomorphic to A. By part (a) of

Lemma 6.3 we have $((E+pF)^\times : E^\times) = p^{k-1}$. We have $(F : E+pF) = p$, so $E+pF$ is a maximal subring of F. The conductor $C = C(E+pF \subset F)$ is pF, so $(E+pF)/C \subset F/C$ is isomorphic to the cosy extension $\mathbb{F}_p \subset \mathbb{F}_p[x]/(g)$, where g is f with coefficients reduced modulo p. This cosy extension has the same unit index as $E+pF \subset F$ by Theorem 2.5. If the polynomial g is irreducible, we have $\mathbb{F}_p[x]/(g) \cong \mathbb{F}_{p^2}$ so that $(F^\times : (E+pF)^\times) = p+1$ and $(F^\times : E^\times) = (p+1)p^{k-1}$. In case g is the product of two different irreducible factors, we have $\mathbb{F}_p[x]/(g) \cong \mathbb{F}_p \times \mathbb{F}_p$ so that $(F^\times : (E+pF)^\times) = p-1$ and $(F^\times : E^\times) = (p-1)p^{k-1}$. Both such g exist for any p and k, so the upper and lower bounds in part (b) of Lemma 6.3 are attained for $A = \mathbb{Z}/p^k\mathbb{Z}$.

Theorem 6.5. *Let A be a finite abelian group and let A_p be the unique Sylow p-subgroup of A for each prime p. Then both $u(A)$ and $u_{\mathrm{fin}}(A)$ are given by the following expression, in which p ranges over all primes:*

$$\prod_p (p+1)^{\dim_{\mathbb{F}_p} A/pA} \cdot \#pA_p,$$

we have $l(A) = 1$, and $l_{\mathrm{fin}}(A)$ is given by the above expression but with "$p+1$" replaced by "$p-1$".

Proof. First we prove that for every finite abelian group A, the expression in the theorem is an upper bound for $u(A)$ and $u_{\mathrm{fin}}(A)$ and that the described expression for $l_{\mathrm{fin}}(A)$ is a lower bound for $l_{\mathrm{fin}}(A)$. This is done by induction on the number of distinct primes N that divide $\#A$.

If $N = 0$ the statement is obviously true. Let $N \geq 0$ and suppose the statement holds for all finite abelian groups A such that at most N distinct primes divide $\#A$. Let A be a finite abelian group such that precisely $N+1$ distinct primes divide $\#A$, let $E \subset F$ be an extension with $F/E \cong A$ and let p be a prime that divides $\#A$. Set $D = E + p^k F$, where p^k is the exponent of the Sylow p-subgroup A_p of A. We have $F/D \cong A_p$ and $A/pA \cong A_p/pA_p$, because A is the direct sum of its Sylow subgroups. It follows from Theorem 2.5 and Lemma 6.3 that

$$(F^\times : D^\times) \leq (p+1)^{\dim_{\mathbb{F}_p} A/pA} \cdot \#pA_p.$$

If F has finite order, we also have $(F^\times : D^\times) \geq (p-1)^{\dim_{\mathbb{F}_p} A/pA} \cdot \#pA_p$. Note that F/E is isomorphic to $(F/D) \oplus (D/E)$ and $p \nmid \#(D/E)$. Hence the statement follows by applying the induction hypothesis to D/E.

Let A be a finite abelian group. Write A as a direct sum of the cyclic groups $E_i = \mathbb{Z}/p_i^{k_i}\mathbb{Z}$ with p_i prime and $k_i \in \mathbb{N}$ for $i \in \{1, \ldots, t\}$. As Example 6.4 shows, there is an extension $E_i \subset F_i$ such that $F_i/E_i \cong E_i$ and $(F_i^\times : E_i^\times) = (p+1)^{\dim_{\mathbb{F}_p} E_i/pE_i} \cdot \#pE_i$ for all $i \in \{1, \ldots, t\}$. The extension $\prod_{i=1}^t E_i \subset \prod_{i=1}^t F_i$ has A as additive quotient group and has the expression in the theorem as unit index. In a similar manner one constructs an extension with additive quotient group A with the expression for $l_{\mathrm{fin}}(A)$ as unit index using Example 6.4, or with unit index 1 using Example 6.1. This completes the proof of Theorem 6.5. □

7. Bimodules of semisimple rings

In this section we determine the simple left $R \otimes_{\mathbb{Z}} R^{\mathrm{opp}}$-modules for all semisimple rings R with prime-power order. We require this solely for technical reasons in the proofs of Lemmas 8.8 and 8.9. We refer to the start of Section 3 for a short overview of basic theory of semisimple rings. Recall from Section 1 that Ω_p is an algebraically closed field of characteristic p for every prime p. For each $k \in \mathbb{N}$ and each prime p, we denote the unique subfield of Ω_p with p^k elements by $\mathbb{F}_{p^k}$.

We now provide an example of such a simple left $R \otimes_{\mathbb{Z}} R^{\mathrm{opp}}$-module.

Example 7.1. Let R be a semisimple ring with order p^k for a prime p and $k \in \mathbb{N}$. There exist finite fields $K_1, \ldots, K_t \subset \Omega_p$ and non-zero, finite-dimensional $\mathbb{F}_p$-vector spaces $V_1, \ldots, V_t$ such that R is isomorphic to the ring $\prod_{i=1}^t R_i$ with $R_i = K_i \otimes_{\mathbb{F}_p} \mathrm{End}_{\mathbb{F}_p}(V_i)$ for all $i \in \{1, \ldots, t\}$.

Let $i, j \in \{1, \ldots, t\}$ and let $\sigma \in \mathrm{Aut}(K_j)$. Consider the additive abelian group $H_{ij} = (K_iK_j) \otimes_{\mathbb{F}_p} \mathrm{Hom}_{\mathbb{F}_p}(V_j, V_i)$. It is not difficult to see that this is a simple left $(K_iK_j) \otimes_{\mathbb{F}_p} \mathrm{End}_{\mathbb{F}_p}(V_i) \otimes_{\mathbb{F}_p} \mathrm{End}_{\mathbb{F}_p}(V_j)^{\mathrm{opp}}$-module via the action $(x \otimes a \otimes b) \cdot (y \otimes c) = (xy) \otimes (acb)$. Now consider the map

$$\begin{aligned} R_i \otimes_{\mathbb{Z}} R_j^{\mathrm{opp}} \quad &\to (K_iK_j) \otimes_{\mathbb{F}_p} \mathrm{End}_{\mathbb{F}_p}(V_i) \otimes_{\mathbb{F}_p} \mathrm{End}_{\mathbb{F}_p}(V_j)^{\mathrm{opp}} \\ (x \otimes a) \otimes (y \otimes b) &\mapsto (x\sigma(y)) \otimes a \otimes b. \end{aligned}$$

This is a surjective ring homomorphism and if one composes it with the projection map $R \otimes_{\mathbb{Z}} R^{\mathrm{opp}} \to R_i \otimes_{\mathbb{Z}} R_j^{\mathrm{opp}}$, one obtains a surjective ring homomorphism $R \otimes_{\mathbb{Z}} R^{\mathrm{opp}} \to (K_iK_j) \otimes_{\mathbb{F}_p} \mathrm{End}_{\mathbb{F}_p}(V_i) \otimes_{\mathbb{F}_p} \mathrm{End}_{\mathbb{F}_p}^{\mathrm{opp}}$. This induces a simple left-$R \otimes_{\mathbb{Z}} R^{\mathrm{opp}}$-module structure on H_{ij}, which we denote by H_{ij}^{σ} to highlight the dependence on σ. Note that H_{ij} and H_{ij}^{σ} implicitly depend on the chosen fields and vector spaces that shall depend on the context.

Lemma 7.2. *Let R be a ring and let M be a left R-module. Let $R_1, \ldots, R_t$ be rings such that $R \cong \prod_{i=1}^t R_i$. Then M is simple if and only if there exists $i \in \{1, \ldots, t\}$ such that M has a simple left-R_i-module structure that induces the original left-R-module structure on M via the projection map $R \to R_i$.*

Proof. The "if" statement is clear, so, conversely, suppose that M is a simple left R-module. Regard R and $R_1, \ldots, R_t$ in the obvious way as R-R-bimodules. Then we have $M \cong R \otimes_R M \cong \bigoplus_{i=1}^t (R_i \otimes_R M)$. Since M is simple, this induces a left-R-module isomorphism $\phi : R_i \otimes_R M \to M$ for some $i \in \{1, \ldots, t\}$. Then $x \cdot m = \phi(x \otimes m)$ for $x \in R_i$ and $m \in M$ defines the desired left-R_i-module structure on M. □

Lemma 7.3. *Let $K \subset L$ and $K \subset M$ be field extensions inside an algebraically closed field Ω such that $K \subset M$ is finite Galois. Let X be a complete set of representatives of* $\mathrm{Gal}(M/K)/\mathrm{Gal}(M/(L \cap M))$. *Then we have a ring isomorphism $L \otimes_K M \to \prod_{\sigma \in X} LM$ given by $x \otimes y \mapsto (x\sigma(y))_{\sigma \in X}$.*

Proof. There exists $\alpha \in M$ with $M = K[\alpha]$ by the Primitive Element Theorem. Let f be the minimum polynomial of α over K and write $f = f_1 \cdots f_t$ with $f_1, \ldots, f_t \in L[x]$ monic and irreducible. Since f is separable, no two polynomials of $f_1, \ldots, f_t$ share a root in Ω and therefore $f_1, \ldots, f_t$ are pairwise coprime. The maximal two-sided ideals $(f_1), \ldots, (f_t)$ of $L[x]$ are then also pairwise coprime. Using the Chinese Remainder Theorem, we find

$$L \otimes_K M \cong L \otimes_K (K[x]/(f)) \cong L[x]/(f) \cong \prod_{i=1}^{t} L[x]/(f_i).$$

There is a bijection from $\mathrm{Gal}(M/K)$ to the set of zeroes of f in M given by $\sigma \mapsto \sigma(\alpha)$. Two elements of $\mathrm{Gal}(M/K)$ share an equivalence class in $\mathrm{Gal}(M/K)/\mathrm{Gal}(M/(L \cap M))$ if and only if they map α to a zero of the same f_i, for $i \in \{1, \ldots, t\}$. Hence we have

$$L \otimes_K M \cong \prod_{i=1}^{t} L[x]/(f_i) \cong \prod_{\sigma \in X} L[\sigma(\alpha)] = \prod_{\sigma \in X} LM.$$

Composing the natural isomorphisms gives the desired isomorphism. □

Lemma 7.4. *Let R be a semisimple ring of order p^k for some prime p and $k \in \mathbb{N}$. Let $K_1, \ldots, K_t \subset \Omega_p$ be finite fields and let $V_1, \ldots, V_t$ be non-zero, finite-dimensional $\mathbb{F}_p$-vector spaces such that $R \cong \prod_{i=1}^{t} K_i \otimes_{\mathbb{F}_p} \mathrm{End}_{\mathbb{F}_p}(V_i)$. Then the modules H_{ij}^{σ} for $i, j \in \{1, \ldots, t\}$ and $\sigma \in \mathrm{Aut}(K_j)$ from Example 7.1 are, up to isomorphism, the only simple left $R \otimes_{\mathbb{Z}} R^{\mathrm{opp}}$-modules.*

Proof. Due to Example 7.1, we only need to show that every simple left $R \otimes_{\mathbb{Z}} R^{\mathrm{opp}}$-module is isomorphic to one of the described modules. Clearly, the rings $R \otimes_{\mathbb{Z}} R^{\mathrm{opp}}$ and $R \otimes_{\mathbb{F}_p} R^{\mathrm{opp}}$ are isomorphic. For all $i, j \in \{1, \ldots, t\}$, let X_{ij} be a complete set of representatives of $\mathrm{Aut}(K_j)/\mathrm{Gal}(K_j/(K_i \cap K_j))$. Set $R_i = K_i \otimes_{\mathbb{F}_p} \mathrm{End}_{\mathbb{F}_p}(V_i)$ for all $i \in \{1, \ldots, t\}$. Using Lemma 7.3 we find

$$R \otimes_{\mathbb{Z}} R^{\mathrm{opp}} \cong \prod_{i=1}^{t} \prod_{j=1}^{t} R_i \otimes_{\mathbb{F}_p} R_j^{\mathrm{opp}} \cong \prod_{i=1}^{t} \prod_{j=1}^{t} \prod_{\sigma \in X_{ij}} E_{ij}^{\sigma},$$

with $E_{ij}^{\sigma} = (K_i K_j) \otimes_{\mathbb{F}_p} \mathrm{End}_{\mathbb{F}_p}(V_i) \otimes_{\mathbb{F}_p} \mathrm{End}_{\mathbb{F}_p}(V_j)^{\mathrm{opp}}$ for all $i, j \in \{1, \ldots, t\}$ and all $\sigma \in X_{ij}$. We have $\mathrm{End}_{\mathbb{F}_p}(V_j)^{\mathrm{opp}} \cong \mathrm{End}_{\mathbb{F}_p}(V_j^*)$ for the dual vector space V_j^* of V_j. It follows that E_{ij}^{σ} is isomorphic to the simple ring $\mathrm{End}_{K_i K_j}((K_i K_j) \otimes_{\mathbb{F}_p} V_i \otimes_{\mathbb{F}_p} V_j^*)$ and therefore E_{ij}^{σ} is simple itself.

Let M be a simple left $R \otimes_{\mathbb{Z}} R^{\mathrm{opp}}$-module. According to Lemma 7.2 there exist $i, j \in \{1, \ldots, t\}$ and $\sigma \in X_{ij}$ such that M is a simple left E_{ij}^{σ}-module and the original left-$R \otimes_{\mathbb{Z}} R^{\mathrm{opp}}$-module structure on M is induced by the projection map $R \otimes_{\mathbb{Z}} R^{\mathrm{opp}} \to E_{ij}^{\sigma}$. In Example 7.1 we saw that H_{ij} is a simple left E_{ij}^{σ}-module and thus M is isomorphic to H_{ij} as a left E_{ij}^{σ}-module. If one compares the left-$R \otimes_{\mathbb{Z}} R^{\mathrm{opp}}$-module structure on H_{ij}^{σ} from Example 7.1 and the isomorphism in Lemma 7.3, it is clear that the left-$R \otimes_{\mathbb{Z}} R^{\mathrm{opp}}$-module structure on H_{ij} induced by the projection map $R \otimes_{\mathbb{Z}} R^{\mathrm{opp}} \to E_{ij}^{\sigma}$, is precisely H_{ij}^{σ}. Hence M and H_{ij}^{σ} are isomorphic as left $R \otimes R^{\mathrm{opp}}$-modules. □

8. The structure of cosy extensions

This section is dedicated to completing the proof of our main structure theorem, Theorem 1.8. Here we treat the non-semisimple, cosy extensions. We refer to the start of Section 3 for a short overview of theory concerning semisimple rings and the Jacobson radical.

Let R be a ring and let I be an R-R-bimodule. Recall that we endowed $R \oplus I\epsilon$ with the multiplication $(r + x\epsilon)(s + y\epsilon) = rs + (ry + xs)\epsilon$ to turn it into a ring. The ring $R \oplus I\epsilon$ contains R as a subring and $I\epsilon$ as a two-sided ideal. Note that $(I\epsilon)^2 = 0$.

Lemma 8.1. *Let E be a ring with finite order and let I be a simple left $E \otimes_{\mathbb{Z}} E^{\mathrm{opp}}$-module that satisfies ${}_E\mathrm{Ann}(I) \cap \mathrm{Ann}_E(I) = 0$. Set $F = E \oplus I\epsilon$. Then $E \subset F$ is non-semisimple and cosy.*

Proof. Since E has finite order, both I and F also have finite order. We have $(I\epsilon)^2 = 0$, so $I\epsilon \subset J(F)$ by Lemma 3.1. The two-sided ideal $I\epsilon$ is non-zero, so $J(F)$ is non-zero as well. Consequently, F is non-semisimple by Lemma 3.1.

We now prove that $E \subset F$ is cosy. The additive index of $E \subset F$ is $\#I$, which is finite. Set $C = C(E \subset F)$. Since C is contained in E, we have $C \cdot I\epsilon = I\epsilon \cdot C = 0$ and therefore C is contained in ${}_E\mathrm{Ann}(I) \cap \mathrm{Ann}_E(I)$. It follows that $C = 0$. For maximality, let D be a subring of F with $E \subsetneq D$. Regard E, D and F as left $E \otimes_{\mathbb{Z}} E^{\mathrm{opp}}$-modules. Then the inclusion map $D \hookrightarrow F$ reduces to an injective homomorphism $D/E \hookrightarrow I\epsilon$. This last map is an isomorphism because $I\epsilon$ is simple; hence $D = F$ and $E \subset F$ is cosy. □

We restate the extensions described in Examples 1.6 and 1.7 and prove they are non-semisimple, cosy extensions in Examples 8.2 and 8.3.

Example 8.2. Let K be a finite field, let L be the prime field of K, let $\sigma \in \mathrm{Aut}(K)$ and let V be a non-zero, finite-dimensional L-vector space. Consider the ring $E = K \otimes_L \mathrm{End}_L(V)$ and the E-E-bimodule E with action $((x \otimes a) \otimes (y \otimes b)) \cdot (z \otimes c) = (xz\sigma(y)) \otimes (acb)$. Write $E \oplus E\epsilon_\sigma = E \oplus E\epsilon$. Since E is a simple ring, it is also a simple left $E \otimes_{\mathbb{Z}} E^{\mathrm{opp}}$-module. We clearly have ${}_E\mathrm{Ann}(E) = 0$ and thus ${}_E\mathrm{Ann}(E) \cap \mathrm{Ann}_E(E) = 0$. According to Lemma 8.1, the extension $E \subset E \oplus E\epsilon_\sigma$ is non-semisimple and cosy.

Example 8.3. Let K be a finite field and let L and M be subfields of K such that $K = LM$. Let U be an L-vector space and let V be an M-vector space such that both are non-zero and have finite dimension. Define $U_K = K \otimes_L U$ and $V_K = K \otimes_M V$. Set $E = \mathrm{End}_L(U) \times \mathrm{End}_M(V)$ and $I = \mathrm{Hom}_K(V_K, U_K)$. The action $((x_1, x_2) \otimes (y_1, y_2)) \cdot z = (\mathrm{id}_K \otimes x_1) \circ z \circ (\mathrm{id}_K \otimes y_2)$ defines an E-E-bimodule structure on I. It is not difficult to see that I is a simple left $E \otimes_{\mathbb{Z}} E^{\mathrm{opp}}$-module. Furthermore, we have ${}_E\mathrm{Ann}(I) = 0 \times \mathrm{End}_M(V)$ and $\mathrm{Ann}_E(I) = \mathrm{End}_L(U) \times 0$, so ${}_E\mathrm{Ann}(I) \cap \mathrm{Ann}_E(I) = 0$. It now follows from Lemma 8.1 that $E \subset E \oplus I\epsilon$ is non-semisimple and cosy.

Proposition 8.4. *Let $E \subset F$ be cosy. Then $(J(F))^2 = 0$.*

Proof. Set $J = J(F)$. Let $n \in \mathbb{N}$ with $n \geq 2$ and suppose that $J^n \neq 0$. It follows from Lemma 2.9 that $E + J^n = F$. Therefore, we have the equality $J = J \cap F = J \cap (E + J^n) = J \cap E + J^n$ and thus

$$F = E + (J \cap E + J^n)^n \subset E + (J \cap E)^n + J^{2n-1} = E + J^{2n-1},$$

so $F = E + J^{2n-1}$. If we perform this process with $2n - 1$ instead of n, we obtain $F = E + J^{4(n-1)+1}$. By induction, we find $F = E + J^{2^k(n-1)+1}$ for all $k \in \mathbb{N}$. However, J is nilpotent by Lemma 3.1, so $F = E + J^{2^k(n-1)+1} = E$ for some $k \in \mathbb{N}$, which is absurd. We conclude that $J^2 = 0$. □

The following lemma is the converse of Lemma 8.1.

Lemma 8.5. *Let $E \subset F$ be non-semisimple and cosy. Write $J = J(F)$. Then the map $\phi : E \oplus J\epsilon \to F, x + y\epsilon \mapsto x + y$ is a ring isomorphism. Moreover, J is a simple left $E \otimes_{\mathbb{Z}} E^{\mathrm{opp}}$-module and ${}_E\mathrm{Ann}(J) \cap \mathrm{Ann}_E(J) = 0$.*

Proof. By Lemma 3.1 we have $J \neq 0$ and by Lemma 2.9 we have $E + J = F$. Let J carry its natural left-$E \otimes_{\mathbb{Z}} E^{\mathrm{opp}}$-module structure and let I be a submodule. Using Proposition 8.4 we obtain

$$F \cdot I \cdot F = (E + J) \cdot I \cdot (E + J) \subset I + J^2 + J^3 = I,$$

so I is a two-sided ideal of F. In particular, $E \cap J$ is a two-sided ideal of F and therefore trivial, because $C(E \subset F) = 0$. We have now shown that $E + J = F$ and $E \cap J = 0$, so ϕ is bijective. Due to Proposition 8.4 it is a ring homomorphism.

Now let I be an $E \otimes_{\mathbb{Z}} E^{\mathrm{opp}}$-submodule of J and suppose that $I \neq 0, J$. Then we have $(E + I) \cap J = (E \cap J) + I = I \subsetneq J$, so $E + I$ is a proper subring of F, but this is absurd by Lemma 2.9. It follows that J is simple. For $A = {}_E\mathrm{Ann}(J) \cap \mathrm{Ann}_E(J)$ we have $F \cdot A \cdot F = (E + J)A(E + J) = A$, so A is a two-sided ideal of F and therefore trivial, because $C(E \subset F) = 0$. □

Corollary 8.6. *Let $E \subset F$ be non-semisimple and cosy. Then the ring E is semisimple.*

Proof. Write $J = J(F)$. The isomorphism ϕ in Lemma 8.5 indicates that $E + J = F$ and $E \cap J = 0$. We obtain the sequence $E \cong E/(E \cap J) \cong (E+J)/J = F/J$ of natural ring isomorphisms. It is clear that $J(F/J) = 0$, so $J(E) = 0$ and hence E is semisimple by Lemma 3.1. □

If $E \subset F$ is a non-semisimple, cosy extension, then $\#E$ is a prime power by Proposition 2.10 and E is semisimple by Corollary 8.6. Thus we can apply Lemma 7.4 to classify $J(F)$ up to left-$E \otimes_{\mathbb{Z}} E^{\mathrm{opp}}$-module isomorphism. With the following lemma we can determine whether modules within such an isomorphism class result in isomorphic extensions, and whether modules in different classes result in isomorphic extensions.

Lemma 8.7. *For $i \in \{1,2\}$, let R_i be a ring and let I_i be an R_i-R_i-bimodule. Then the extensions $R_1 \subset R_1 \oplus I_1\epsilon$ and $R_2 \subset R_2 \oplus I_2\epsilon$ are isomorphic if and only if there is a ring isomorphism $\phi : R_1 \to R_2$ and a group isomorphism $\psi : I_1 \to I_2$ such that $\psi(xzy) = \phi(x)\psi(z)\phi(y)$ for all $x, y \in R_1$ and $z \in I_1$.*

Proof. For the first implication, suppose that $\phi : R_1 \oplus I_1\epsilon \to R_2 \oplus I_2\epsilon$ is a ring isomorphism with $\phi(R_1) = R_2$. Then $\phi|_{R_1} : R_1 \to R_2$ is a ring isomorphism and it induces a group isomorphism $(R_1 \oplus I_1\epsilon)/R_1 \to (R_2 \oplus I_2\epsilon)/R_2$. Since $(R_i \oplus I_i\epsilon)/R_i$ is isomorphic to I_i for $i \in \{1,2\}$, we find the group isomorphism $\psi = \pi \circ \phi|_{I_1} : I_1 \to I_2$, where $\pi : R_2 \oplus I_2\epsilon \to I_2$ is the projection map. For all $x, y \in R_1$ and $z \in I_1$ we have

$$\psi(xzy) = \pi(\phi(x)\phi(z)\phi(y)) = \phi(x)\pi(\phi(z))\phi(y) = \phi(x)\psi(z)\phi(y).$$

For the opposite implication, consider the map $R_1 \oplus I_1\epsilon \to R_2 \oplus I_2\epsilon$ given by $x + y\epsilon \mapsto \phi(x) + \psi(y)\epsilon$. It is not difficult to see that this map is a ring isomorphism that maps R_1 bijectively to R_2. □

Lemma 8.8. *Let $E \subset F$ be non-semisimple and cosy. Suppose E is simple. Then there exist a finite field K, a field automorphism $\sigma \in \mathrm{Aut}(K)$ and a non-zero, finite-dimensional L-vector space V, where L is the prime field of K, such that the extension $E \subset F$ is isomorphic to $K \otimes_L \mathrm{End}_L(V) \subset (K \otimes_L \mathrm{End}_L(V)) \oplus (K \otimes_L \mathrm{End}_L(V))\epsilon_\sigma$, as defined in Example 8.2.*

Proof. The ring E has finite order by Proposition 2.10 and is therefore isomorphic to $D = K \otimes_{\mathbb{F}_p} \mathrm{End}_{\mathbb{F}_p}(V)$ for some prime p, some finite field $K \subset \Omega_p$ and a non-zero, finite-dimensional $\mathbb{F}_p$-vector space V. By Lemma 8.5, the Jacobson radical $J(F)$ is a simple left $E \otimes_{\mathbb{Z}} E^{\mathrm{opp}}$-module and $E \subset F$ is isomorphic to $E \subset E \oplus J(F)\epsilon$. It follows from Lemma 7.4 that $J(F)$ is isomorphic to $H^\sigma_{11} = K \otimes_{\mathbb{F}_p} \mathrm{End}_{\mathbb{F}_p}(V)$ for some $\sigma \in \mathrm{Aut}(K)$, as in Example 7.1. Note that H^σ_{11} is the same D-D-bimodule we used to construct $D \oplus D\epsilon_\sigma$ in Example 8.2. Using Lemma 8.7, we see that the extensions $E \subset E \oplus J(F)\epsilon$ and $D \subset D \oplus D\epsilon$ are isomorphic, which proves Lemma 8.8. □

Lemma 8.9. *Let $E \subset F$ be non-semisimple and cosy. Suppose E is not simple. Then there exist a prime p, finite fields K, L and M with $L, M \subset K$ and $LM = K$, an L-vector space U and an M-vector space V, both of which are non-zero and finite dimensional, such that $E \subset F$ is isomorphic to $\mathrm{End}_L(U) \times \mathrm{End}_M(V) \subset (\mathrm{End}_L(U) \times \mathrm{End}_M(V)) \oplus \mathrm{Hom}_K(V_K, U_K)$, as defined in Example 8.3.*

Proof. The ring E is semisimple by Corollary 8.6 and its order is a prime power by Proposition 2.10. Thus E is isomorphic to $\prod_{i=1}^t K_i \otimes_{\mathbb{F}_p} \mathrm{End}_{\mathbb{F}_p}(V_i)$ for some $t \in \mathbb{Z}_{\geq 2}$, a prime p, finite fields $K_1, \ldots, K_t \subset \Omega_p$ and non-zero, finite-dimensional $\mathbb{F}_p$-vector spaces $V_1, \ldots, V_t$. Moreover, $J(F)$ is a simple left $E \otimes_{\mathbb{Z}} E^{\mathrm{opp}}$-module and $E \subset F$ is isomorphic to $E \subset E \oplus J(F)\epsilon$ due to Lemma 8.5. By Lemma 7.4, the module $J(F)$ is isomorphic to $H^\sigma_{ij} =$

$(K_iK_j) \otimes_{\mathbb{F}_p} \mathrm{Hom}_{\mathbb{F}_p}(V_j, V_i)$ for some $i, j \in \{1, \dots, t\}$ and $\sigma \in \mathrm{Aut}(K_j)$, as in Example 7.1. If $i = j$ or $t > 2$, we have ${}_E\mathrm{Ann}(H^\sigma_{ij}) \cap \mathrm{Ann}_E(H^\sigma_{ij}) \neq 0$, which is absurd by Lemma 8.5. Thus $i \neq j$ and $t = 2$. By reordering we may assume that $i = 1$ and $j = 2$. Consider the ring automorphism ϕ of $\prod_{m=1}^t K_m \otimes_{\mathbb{F}_p} \mathrm{End}_{\mathbb{F}_p}(V_m)$ given by $(x \otimes a, y \otimes b) \mapsto (x \otimes a, \sigma(y) \otimes b)$ and let ψ be the identity map $H^\sigma_{ij} \to H^{\mathrm{id}}_{ij}$. Then $\psi(xzy) = \phi(x)\psi(z)\phi(y)$ for all $x, y \in E$ and $z \in J(F)$. The desired result follows from Lemma 8.7. □

We are now able to prove Theorem 1.8.

Theorem 8.10. *Define the following parametrised families of ring extensions with parameters as indicated:*

I. $\mathrm{Diag}_K(V) \subset \mathrm{End}_K(V) \times \mathrm{End}_K(V)$ *with* $K = \mathbb{F}_{p^k}$ *and* $V = K^n$ *for all primes* p *and* $k, n \in \mathbb{N}$*;*

II. $\mathrm{Fix}_K(W, V) \subset \mathrm{End}_K(V)$ *with* $K = \mathbb{F}_{p^k}$, $V = K^n$ *and* $W = K^m \times 0$ *for all primes* p *and* $k, n, m \in \mathbb{N}$ *such that* $m < n$*;*

III. $\mathrm{End}_L(V) \subset K \otimes_L \mathrm{End}_L(V)$ *with* $K = \mathbb{F}_{p^{kd}}$, $L = \mathbb{F}_{p^k}$ *and* $V = K^n$ *for all primes* p*, primes* d*, and* $k, n \in \mathbb{N}$*;*

IV. $\mathrm{End}_L(V) \subset \mathrm{End}_K(V)$ *with* $K = \mathbb{F}_{p^k}$, $L = \mathbb{F}_{p^{kd}}$ *and* $V = L^n$ *for all primes* p*, primes* d*, and* $k, n \in \mathbb{N}$*;*

V. $K \otimes_L \mathrm{End}_L(V) \subset (K \otimes_L \mathrm{End}_L(V)) \oplus (K \otimes_L \mathrm{End}_L(V))\epsilon_\sigma$ *as defined in Example 8.2 with* $K = \mathbb{F}_{p^k}$, $L = \mathbb{F}_p$ *and* $V = L^n$ *for all primes* p*, automorphisms* $\sigma \in \mathrm{Aut}(K)$ *and* $k, n \in \mathbb{N}$*;*

VI. $\mathrm{End}_L(U) \times \mathrm{End}_M(V) \subset (\mathrm{End}_L(U) \times \mathrm{End}_M(V)) \oplus \mathrm{Hom}_K(V_K, U_K)\epsilon$ *as defined in Example 8.3 with* $K = \mathbb{F}_{p^{\mathrm{lcm}(d,e)}}$, $L = \mathbb{F}_{p^d}$, $M = \mathbb{F}_{p^e}$, $U = L^m$ *and* $V = M^n$ *for all primes* p *and* $d, e, m, n \in \mathbb{N}$*.*

Then each of these families consists of cosy extensions and every cosy extension is isomorphic to precisely one of these extensions.

Proof. In Theorem 4.8 we classified the semisimple, cosy extensions as families I–IV. According to Examples 8.2 and 8.3, families V and VI consist of non-semisimple, cosy extensions. Semisimple, cosy extensions and non-semisimple, cosy extensions are non-isomorphic, so it suffices to show that (a) every non-semisimple, cosy extension is isomorphic to an extension in family V or family VI, that (b) extensions in family V and extensions in family VI are non-isomorphic, and that (c) different parameters yield non-isomorphic extensions within family V and within family VI.

(a) Let $E \subset F$ be a non-semisimple, cosy extension. If E is simple, then $E \subset F$ is isomorphic to an extension in Example 8.2 by Lemma 8.8. Otherwise, E is not simple and $E \subset F$ is isomorphic to an extension in Example 8.3 by Lemma 8.9. It is not difficult to see that any extension in these two examples is isomorphic to an extension in family V or VI.

(b) In family V the subrings are simple, while they are not in family VI.

(c) For family V, suppose $E_i = K_i \otimes_{L_i} \mathrm{End}_{L_i}(V_i) \subset F_i = E_i \oplus I_i\epsilon_{\sigma_i}$ with $I_i = E_i$ for $i \in \{1, 2\}$ are two isomorphic extensions. By Lemma 8.7, there

is a ring isomorphism $\phi : E_1 \to E_2$ and a group isomorphism $\psi : I_1 \to I_2$ such that $\psi(xzy) = \phi(x)\psi(z)\phi(y)$ for all $x, y \in E_1$ and $z \in I_1$. This implies that $K_1 = K_2$, $L_1 = L_2$ and $V_1 = V_2$. For $a \in I_1$ and $x \in K_1$ we have

$$\phi(\sigma_1(x))\psi(a) = \psi(\sigma_1(x)a) = \psi(ax) = \psi(a)\phi(x) = \sigma_2(\phi(x))\psi(a),$$

so $\phi|_{K_1} \circ \sigma_1 = \sigma_2 \circ \phi|_{K_1}$ and thus $\sigma_1 = \sigma_2$, as $\mathrm{Aut}(K_1)$ is an abelian group.

For family VI, suppose $E_i = \mathrm{End}_{L_i}(U_i) \times \mathrm{End}_{M_i}(V_i) \subset F_i = E_i \oplus I_i\epsilon$ with $I_i = \mathrm{Hom}_{K_i}(V_{K_i}, U_{K_i})$ for $i \in \{1, 2\}$ are two isomorphic extensions. There is a ring isomorphism $\phi : E_1 \to E_2$ and a group isomorphism $\psi : I_1 \to I_2$ such that $\psi(xzy) = \phi(x)\psi(z)\phi(y)$ for all $x, y \in E_1$ and $z \in I_1$ by Lemma 8.7. We have $\phi({}_{E_1}\mathrm{Ann}(I_1)) = {}_{E_2}\mathrm{Ann}(I_2)$ and $\phi(\mathrm{Ann}_{E_1}(I_1)) = \mathrm{Ann}_{E_2}(I_2)$. This implies the equality of parameters. □

References

[BL15] Alex Bartel and Hendrik W. Lenstra Jr. "Commensurability of automorphism groups". In: *arXiv e-prints* (2015). DOI: 10.1112/S0010437X1600823X.

[Lam01] Tsit Yuen Lam. *A first course in noncommutative rings*. 2nd ed. Graduate texts in mathematics, 131. Springer-Verlag, 2001. ISBN: 9781441986160.

[Wol95] John Wolfskill. "Bounding a unit index in terms of a ring index". In: *Mathematika* 42.1 (1995), pp. 199–205. DOI: 10.1112/S0025579300011499.

[Wol97] John Wolfskill. "Comparing the unit groups of two orders in a number field". In: *Rocky Mountain J. Math.* 27.4 (1997), pp. 1279–1289. DOI: 10.1216/rmjm/1181071875.