ON K-THEORETIC INVARIANTS OF SEMIGROUP C*-ALGEBRAS FROM ACTIONS OF CONGRUENCE MONOIDS

CHRIS BRUCE AND XIN LI

Abstract. We study semigroup C*-algebras of semigroups associated with number fields and initial data arising naturally from class field theory. These semigroup C*-algebras turn out to have an interesting C*-algebraic structure, giving access to many new examples of classifiable C*-algebras and exhibiting phenomena which have not appeared before. Moreover, using K-theoretic invariants, we investigate how much information about the initial number-theoretic data is encoded in our semigroup C*-algebras.

1. Introduction

Semigroup C*-algebras are C*-algebras generated by left regular representations of left-cancellative semigroups. They form a natural example class of C*-algebras and have been studied in various contexts for several families of semigroups, for instance positive cones in totally ordered groups [3, 14, 36], semigroups naturally arising in combinatorial or geometric group theory [5, 6, 42], semigroups given by presentations [33], or semigroups of number-theoretic origin [23, 7, 15, 28, 29]. It was this last class of examples which has triggered many of the recent developments in semigroup C*-algebras (see [11] and the references therein for an overview).

While semigroup C*-algebras for the full $ax + b$-semigroups over rings of algebraic integers have been studied in [7, 15, 28, 29], the first-named author considered a much more general class of semigroups in [1, 2] and showed that, while providing a rich source of new examples, they allow for a similar analysis as in the full $ax + b$ case. This generalization, which is very natural from the number-theoretic point of view, proceeds as follows: Given a number field K with ring of algebraic integers R, a modulus $\mathfrak{m}$ for K, and a group Γ of residues modulo $\mathfrak{m}$, define the associated congruence monoid $R_{\mathfrak{m},\Gamma}$ as the multiplicative submonoid of elements in R that are relatively prime to $\mathfrak{m}$ and reduce to an element of Γ modulo $\mathfrak{m}$, and form the semi-direct product $R \rtimes R_{\mathfrak{m},\Gamma}$ where $R_{\mathfrak{m},\Gamma}$ acts on R by multiplication. In this way, we obtain a generalization of the construction of $ax + b$-semigroups (the latter corresponding to the case of trivial $\mathfrak{m}$ and Γ). The data $(\mathfrak{m}, \Gamma)$ canonically gives rise to a class field $K(\mathfrak{m})^{\bar{\Gamma}}$ of K, which, in the case of trivial $\mathfrak{m}$ and Γ, is simply the Hilbert class field of K. The semigroup C*-algebras attached to these generalized $ax + b$-semigroups turn out to be very interesting from the C*-algebraic perspective. In particular, their K-theoretic invariants are very rich and exhibit interesting new phenomena which have not appeared before.

Our goal in this paper is twofold. The first goal is a careful analysis of the semigroup C*-algebras $C^*_\lambda(R \rtimes R_{\mathfrak{m},\Gamma})$ and their K-theoretic invariants. Building on this, the second goal is to address the following natural question:

How much of the initial number field K and the class field $K(\mathfrak{m})^{\bar{\Gamma}}$
does our semigroup C*-algebra $C^*_\lambda(R \rtimes R_{\mathfrak{m},\Gamma})$ remember?

More precisely, our goal is to extract information about K and $K(\mathfrak{m})^{\bar{\Gamma}}$ from K-theoretic invariants of $C^*_\lambda(R \rtimes R_{\mathfrak{m},\Gamma})$. The idea of using K-theory to extract information goes back to the classification programme

2010 *Mathematics Subject Classification.* Primary 46L05, 46L80; Secondary 11Rxx, 11R37.

The first-named author was supported by the Natural Sciences and Engineering Research Council of Canada through an Alexander Graham Bell CGS-D award.

of C*-algebras and has already proven to be fruitful in the case of $ax+b$-semigroups [28, 29]. Our main result reads as follows:

Theorem (see Theorem 5.5)**.** *Suppose that K and L are number fields with rings of algebraic integers R and S. Let $\mathfrak{m}$ and $\mathfrak{n}$ be moduli for K and L, and let Γ and Λ be subgroups of $(R/\mathfrak{m})^*$ and $(S/\mathfrak{n})^*$, respectively. Suppose that there is an isomorphism $C^*_\lambda(R \rtimes R_{\mathfrak{m},\Gamma}) \cong C^*_\lambda(S \rtimes S_{\mathfrak{n},\Lambda})$. Then*

(i) *K and L are arithmetically equivalent, and $K(\mathfrak{m})^{\bar{\Gamma}}$ and $L(\mathfrak{n})^{\bar{\Lambda}}$ are Kronecker equivalent;*
(ii) *if the class fields $K(\mathfrak{m})^{\bar{\Gamma}}$ and $L(\mathfrak{n})^{\bar{\Lambda}}$ of K and L are both Galois over $\mathbb{Q}$, then $\#\mathrm{Cl}^{\bar{\Gamma}}_{\mathfrak{m}} = \#\mathrm{Cl}^{\bar{\Lambda}}_{\mathfrak{n}}$;*
(iii) *if K or L is Galois, then $K = L$; in particular, K is Galois if and only if L is Galois;*
(iv) *if K or L is Galois and both the class fields $K(\mathfrak{m})^{\bar{\Gamma}}$ and $L(\mathfrak{n})^{\bar{\Lambda}}$ are Galois over $\mathbb{Q}$, then*
  (a) *$K = L$;*
  (b) *$K(\mathfrak{m})^{\bar{\Gamma}} = L(\mathfrak{n})^{\bar{\Lambda}}$ (in any algebraically closed field containing both $K(\mathfrak{m})^{\bar{\Gamma}}$ and $L(\mathfrak{n})^{\bar{\Lambda}}$);*
  (c) *$R^* \cdot (R_{\mathfrak{n}} \cap R_{\mathfrak{m},\Gamma}) = S^* \cdot (S_{\mathfrak{m}} \cap S_{\mathfrak{n},\Lambda})$;*
  (d) *$\mathrm{Cl}^{\bar{\Gamma}}_{\mathfrak{m}} \cong \mathrm{Cl}^{\bar{\Lambda}}_{\mathfrak{n}}$ (as abelian groups).*

We refer the reader to § 2 for more precise definitions and more detailed explanations of our constructions. Here and in the sequel, we consider arithmetic equivalence and Kronecker equivalence over $\mathbb{Q}$.

We would like to point out that even in the case of trivial initial data, i.e., for ordinary $ax+b$-semigroups, our main theorem improves existing results. Indeed, in the present paper (more precisely in Theorem 5.3 and Corollary 5.4 below), we answer the natural question left open from [28] whether it is possible to read off the number of roots of unity from our semigroup C*-algebras. This requires new techniques, including a detailed analysis of K-theoretic invariants, which is interesting on its own right. In addition, we are able to extract new information about the class fields naturally associated with our initial data (which in the case of trivial data is given by the Hilbert class fields). Indeed, by computing the torsion order of the K_0-class of the identity projection in quotients of $C^*_\lambda(R \rtimes R_{\mathfrak{m},\Gamma})$ by its minimal primitive ideals, we show that a certain set of prime numbers is an invariant of the C*-algebra $C^*_\lambda(R \rtimes R_{\mathfrak{m},\Gamma})$. This set differs from the Kronecker set of the class field $K(\mathfrak{m})^{\bar{\Gamma}}$ by only finitely many primes, so that we recover $K(\mathfrak{m})^{\bar{\Gamma}}$ up to Kronecker equivalence. This information was not available in [28].

This paper is organized as follows. We begin with a brief discussion of general semigroup C*-algebras in § 2.1 and then specialize to the case of semigroups of $ax+b$ type arising from actions of congruence monoids on rings of algebraic integers in § 2.2. In § 2.3 we explain how the number-theoretic data used to define a congruence monoid naturally gives rise to a class field (i.e., finite abelian extension), and in § 2.4 we show that how one can recover information about the congruence monoids from these class fields. In § 3, we show that all the semigroup C*-algebras $C^*_\lambda(R \rtimes R_{\mathfrak{m},\Gamma})$ are purely infinite in a very strong sense, i.e., they absorb $\mathcal{O}_\infty$ tensorially, $C^*_\lambda(R \rtimes R_{\mathfrak{m},\Gamma}) \cong \mathcal{O}_\infty \otimes C^*_\lambda(R \rtimes R_{\mathfrak{m},\Gamma})$. This means that our semigroup C*-algebras fall into the scope of the classification programme for C*-algebras. More precisely, they belong to the class of C*-algebras classified by Kirchberg in [21]. This motivates a detailed analysis of the K-groups of our semigroup C*-algebras, which we initiate in § 4.1. Furthermore, to illustrate our results, we discuss several concrete example classes along the way (see for instance § 4.1.1, § 4.1.3, or Theorem 5.9). We also present a first example of a semigroup whose left and right boundary quotients do not have isomorphic K-theory (see Remark 4.25), which is a completely new phenomenon that has not appeared before. This is an outgrowth of the general discussion of K-theory for boundary quotients of our semigroup C*-algebras in § 4.2. Finally, in § 5.2, we prove stronger reconstruction results if in addition to the semigroup C*-algebras, we also keep track of canonical Cartan subalgebras. All these additional results show that our semigroup C*-algebras form an interesting class of examples from a C*-algebra perspective, giving access to many new examples of classifiable C*-algebras.

This project was initiated during a visit of the first-named author to Queen Mary University of London, and he would like to acknowledge this and thank the mathematics department there for its hospitality.

2. Preliminaries

2.1. **Semigroup C*-algebras.** Let P be a left cancellative semigroup (with identity, say, for convenience), and consider the Hilbert space $\ell^2(P)$ with its canonical orthonormal basis $\{\delta_x : x \in P\}$. Since P is left cancellative, each $p \in P$ gives rise to an isometry $\lambda(p) : \ell^2(P) \to \ell^2(P)$ that is determined by $\lambda(p)(\delta_x) = \delta_{px}$ for $x \in P$. The *left regular C*-algebra of* P is $C^*_\lambda(P) := C^*(\{\lambda(p) : p \in P\})$. Let $I_l(P)$ be the inverse semigroup generated by the isometries $\lambda(P)$, and put $D_\lambda(P) := C^*(\{ss^* : s \in I_l(P)\})$. Each projection ss^* for $s \in I_l(P)$ corresponds to a subset of P; such subsets are called constructible right ideals, and the set of constructible right ideals in P is denoted by $\mathcal{J}_P$.

Assume that P embeds into a group G. Then $D_\lambda(P)$ coincides with the canonical diagonal sub-C*-algebra of $C^*_\lambda(P)$, namely $D_\lambda(P) = \ell^\infty(P) \cap C^*_\lambda(P)$ where we view $\ell^\infty(P)$ as a sub-C*-algebra of $\mathcal{L}(\ell^2(P))$ in the canonical way. Moreover, there is a canonical partial action of G on $D_\lambda(P)$, and $C^*_\lambda(P)$ can be written as the partial crossed product $C^*_\lambda(P) \cong D_\lambda(P) \rtimes_r G$. The C*-algebra $D_\lambda(P) \rtimes_r G$ can be identified with the reduced C*-algebra of the partial transformation groupoid $G \ltimes \Omega_P$ where $\Omega_P := \operatorname{Spec}(D_\lambda(P))$, so one obtains a description of $C^*_\lambda(P)$ as a groupoid C*-algebra (see [30] for details). This is useful for many purposes, for instance, in the case that $G \ltimes \Omega_P$ is topologically principal, so that $C(\Omega_P)$ is a Cartan subalgebra of $C^*_r(G \ltimes \Omega_P)$, we obtain that $D_\lambda(P)$ is a Cartan subalgebra of $C^*_\lambda(P)$.

We refer the reader to [26, 27, 30] and [11, Chapter 5] for the general theory of semigroup C*-algebras.

2.2. **Congruence monoids and semigroup C*-algebras associated with their actions.** We briefly review the construction from [1, § 3]. Let K be a number field with ring of algebraic integers R, and let $\mathcal{P}_K$ denote the set of non-zero prime ideals of R. Each fractional ideal $\mathfrak{a}$ of K has a unique factorization $\mathfrak{a} = \prod_{\mathfrak{p} \in \mathcal{P}_K} \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{a})}$ where $v_\mathfrak{p}(\mathfrak{a}) \in \mathbb{Z}$ is zero for all but finitely many $\mathfrak{p}$. For $x \in K^\times$, we let $v_\mathfrak{p}(x) := v_\mathfrak{p}((x))$ where (x) is the principal fractional ideal of K generated by x. Given a modulus $\mathfrak{m} = \mathfrak{m}_\infty \mathfrak{m}_0$ for K, let

$$(R/\mathfrak{m})^* := \Big(\prod_{w \mid \mathfrak{m}_\infty} \langle \pm 1 \rangle \Big) \times (R/\mathfrak{m}_0)^*$$

be the multiplicative group of residues modulo $\mathfrak{m}$. Let

$$R_\mathfrak{m} := \{a \in R^\times : v_\mathfrak{p}(a) = 0 \text{ for all } \mathfrak{p} \mid \mathfrak{m}_0\}$$

denote the multiplicative semigroup of non-zero algebraic integers that are relatively prime to $\mathfrak{m}_0$; note that $R_\mathfrak{m}$ only depends on the support of $\mathfrak{m}_0$, that is, on $\operatorname{supp}(\mathfrak{m}_0) := \{\mathfrak{p} \in \mathcal{P}_K : \mathfrak{p} \mid \mathfrak{m}_0\}$. For $a \in R_\mathfrak{m}$, let

$$[a]_\mathfrak{m} := ((\operatorname{sign}(w(a)))_{w \mid \mathfrak{m}_\infty}, a + \mathfrak{m}_0) \in (R/\mathfrak{m})^*.$$

Then $R_\mathfrak{m} \to (R/\mathfrak{m})^*$, $a \mapsto [a]_\mathfrak{m}$, is a semigroup homomorphism. If Γ is a subgroup of $(R/\mathfrak{m})^*$, then

$$R_{\mathfrak{m},\Gamma} := \{a \in R_\mathfrak{m} : [a]_\mathfrak{m} \in \Gamma\}$$

is a unital subsemigroup of $R^\times$, which is called a *congruence monoid*. Note there is some freedom in choosing $\mathfrak{m}_\infty$ and the infinite part of Γ without changing the congruence monoid.

The monoid $R_{\mathfrak{m},\Gamma}$ acts on R by multiplication, so one may form the semi-direct product $R \rtimes R_{\mathfrak{m},\Gamma}$. Let $K_{\mathfrak{m},\Gamma} := \{x \in K_\mathfrak{m} : [x]_\mathfrak{m} \in \Gamma\}$; by [1, Proposition 3.2], $K_{\mathfrak{m},\Gamma} = R^{-1}_{\mathfrak{m},\Gamma} R_{\mathfrak{m},\Gamma}$. By [1, Proposition 3.3], the semigroup $R \rtimes R_{\mathfrak{m},\Gamma}$ is left Ore with group of left quotients equal to $G(R \rtimes R_{\mathfrak{m},\Gamma}) = (R^{-1}_\mathfrak{m} R) \rtimes K_{\mathfrak{m},\Gamma}$, where $R^{-1}_\mathfrak{m} R = \{a/b : a \in R, b \in R_\mathfrak{m}\} \subseteq K^\times$ is the localization of R at $R_\mathfrak{m}$.

By [1, Proposition 3.4], $R \rtimes R_{\mathfrak{m},\Gamma}$ satisfies the independence condition from [26], and the semilattice $\mathcal{J}_{R \rtimes R_{\mathfrak{m},\Gamma}}$ of constructible right ideals in $R \rtimes R_{\mathfrak{m},\Gamma}$ is given by

$$\mathcal{J}_{R \rtimes R_{\mathfrak{m},\Gamma}} = \{(x + \mathfrak{a}) \times (\mathfrak{a} \cap R_{\mathfrak{m},\Gamma}) : x \in R, \mathfrak{a} \in \mathcal{I}^+_\mathfrak{m}\} \cup \{\emptyset\}$$

where $\mathcal{I}^+_\mathfrak{m}$ is the semigroup of integral ideals relatively prime to $\mathfrak{m}_0$.

By [1, equation (3) and Proposition 5.4], we can identify $C^*_\lambda(R \rtimes M)$ with the reduced groupoid C*-algebra of the partial transformation groupoid $(Q \rtimes G) \ltimes \Omega$ in such a way that $D_\lambda(R \rtimes M)$ is carried onto $C(\Omega)$, where the space Ω and the partial action of $Q \rtimes G$ are described in [1, § 5.2]. The groupoid $(Q \rtimes G) \ltimes \Omega$ is topologically principal by [1, Proposition 6.3], so $D_\lambda(R \rtimes M)$ is a Cartan subalgebra of $C^*_\lambda(R \rtimes M)$ (cf. § 2.1).

Moreover, using the above description as a groupoid C*-algebra, the primitive ideal space of $C^*_\lambda(R \rtimes R_{\mathfrak{m},\Gamma})$ has been computed in [1, § 7] as $\mathrm{Prim}(C^*_\lambda(R \rtimes R_{\mathfrak{m},\Gamma})) \cong 2^{\mathcal{P}^{\mathfrak{m}}_K}$, where $\mathcal{P}^{\mathfrak{m}}_K := \mathcal{P}_K \setminus \mathrm{supp}(\mathfrak{m}_0)$, and $2^{\mathcal{P}^{\mathfrak{m}}_K}$ is given the power-cofinite topology. This homeomorphism is order-preserving, so it follows that the non-zero minimal primitive ideals of $C^*_\lambda(R \rtimes R_{\mathfrak{m},\Gamma})$ are in one-to-one correspondence with the primes in $\mathcal{P}^{\mathfrak{m}}_K$.

2.3. **Class fields associated with congruence monoids.** We will need some standard results on ray class fields from the ideal-theoretic point of view. The reader may consult for instance [35] for more details about class field theory.

Let K be a number field with ring of algebraic integers R, and let $\mathcal{P}_K$ denote the set of non-zero prime ideals of R. Let $\mathfrak{m}$ be a modulus for K, let $\mathcal{I}_\mathfrak{m}$ denote the group of fractional ideals of K which are relatively prime to $\mathfrak{m}_0$, and let $K_\mathfrak{m}$ be the subgroup of $K^\times$ consisting elements that are relatively prime to $\mathfrak{m}_0$. Then the map $a \mapsto [a]_\mathfrak{m}$ extends to a surjective group homomorphism $K_\mathfrak{m} \to (R/\mathfrak{m})^*$ (see, for example, [1, § 2.2]). Let $i : K_\mathfrak{m} \to \mathcal{I}_\mathfrak{m}$ be the canonical homomorphism given by $a \mapsto aR$. Let $K_{\mathfrak{m},1} := \{x \in K_\mathfrak{m} : [x]_\mathfrak{m} = 1\}$, so that $K_\mathfrak{m}/K_{\mathfrak{m},1} \cong (R/\mathfrak{m})^*$. The group $\mathrm{Cl}_\mathfrak{m}(K) := \mathcal{I}_\mathfrak{m}/i(K_{\mathfrak{m},1})$ is the *ray class group modulo* $\mathfrak{m}$. When it will not cause confusion, we will simply write $\mathrm{Cl}_\mathfrak{m}$ rather than $\mathrm{Cl}_\mathfrak{m}(K)$. The ray class group associated with the trivial modulus is the usual ideal class group of K, that is, $\mathrm{Cl}_{(1)} = \mathrm{Cl}$.

There is the following exact sequence relating $\mathrm{Cl}_\mathfrak{m}$ to the ideal class group of K:

$$0 \to R^*/R^*_{\mathfrak{m},1} \to K_\mathfrak{m}/K_{\mathfrak{m},1} \to \mathrm{Cl}_\mathfrak{m} \to \mathrm{Cl} \to 0 \tag{1}$$

where $R^*_{\mathfrak{m},1} := R^* \cap K_{\mathfrak{m},1}$ (see [35, Chapter V, Theorem 1.7]).

Suppose L/K is a finite extension of number fields. For a prime $\mathfrak{P} \in \mathcal{P}_L$ lying over a prime $\mathfrak{p} \in \mathcal{P}_K$, we write $f_{L/K}(\mathfrak{P}|\mathfrak{p})$ for the inertia degree of $\mathfrak{P}$ over $\mathfrak{p}$, and $e_{L/K}(\mathfrak{P}|\mathfrak{p})$ for the ramification index of $\mathfrak{P}$ over $\mathfrak{p}$ (see [38, Chapter I, §8] for the definitions). If L is Galois, then $f_{L/K}(\mathfrak{P}|\mathfrak{p})$ does not depend on $\mathfrak{P}$, and we simply write $f_{L/K}(\mathfrak{p})$ instead of $f_{L/K}(\mathfrak{P}|\mathfrak{p})$. When $K = \mathbb{Q}$ and $\mathfrak{p} = p\mathbb{Z}$ for a rational prime p, we will often abuse notation and write p instead of $p\mathbb{Z}$.

Now suppose that L/K is a finite Galois extension, and let S denote the ring of algebraic integers in L. If a prime $\mathfrak{p} \in \mathcal{P}_K$ is unramified in L and $\mathfrak{P} \in \mathcal{P}_L$ with $\mathfrak{P} \mid \mathfrak{p}$, then each element of the decomposition group

$$D_\mathfrak{P}(L/K) = \{\sigma \in \mathrm{Gal}(L/K) : \sigma(\mathfrak{P}) = \mathfrak{P}\}$$

defines an automorphism of the finite field $S/\mathfrak{P}$, and this gives a canonical identification of $D_\mathfrak{P}(L/K)$ with the Galois group $\mathrm{Gal}((S/\mathfrak{P})/(R/\mathfrak{p}))$ of the field extension $(S/\mathfrak{P})/(R/\mathfrak{p})$. Since this latter group is cyclic, so is $D_\mathfrak{P}(L/K)$. The *Frobenius automorphism corresponding to* $\mathfrak{P}$ is the automorphism $(\mathfrak{P}, L/K) \in \mathrm{Gal}(L/K)$ such that under the identification $D_\mathfrak{P}(L/K) \cong \mathrm{Gal}((S/\mathfrak{P})/(R/\mathfrak{p}))$, $(\mathfrak{P}, L/K)$ is sent to the automorphism of $S/\mathfrak{P}$ that is determined by $x + \mathfrak{P} \mapsto x^{N(\mathfrak{p})} + \mathfrak{P}$. Here $N(\mathfrak{p}) = \#(R/\mathfrak{p})$ is the norm of $\mathfrak{p}$. It is known that the set

$$\mathrm{Fr}_\mathfrak{p}(L/K) := \{(\mathfrak{P}, L/K) : \mathfrak{P} \in \mathcal{P}_L \text{ with } \mathfrak{P} \mid \mathfrak{p}\}$$

is a conjugacy class in $\mathrm{Gal}(L/K)$. Indeed, $\mathrm{Gal}(L/K)$ acts transitively on the set of primes in $\mathcal{P}_L$ that lie over $\mathfrak{p}$, and if $\tau \in \mathrm{Gal}(L/K)$, then $(\tau(\mathfrak{P}), L/K) = \tau(\mathfrak{P}, L/K)\tau^{-1}$.

If L/K is abelian, that is, if L is a Galois extension of K with abelian Galois group, then $\mathrm{Fr}_\mathfrak{p}(L/K)$ consists of a single element, which we shall denote by $(\mathfrak{p}, L/K)$; this automorphism is called the *Frobenius automorphism corresponding to* $\mathfrak{p}$.

For each modulus $\mathfrak{m}$ of K, let $K(\mathfrak{m})$ denote the associated ray class field of K (see [35, Chapter V, § 3]). Then $K(\mathfrak{m})$ satisfies:

(a) $K(\mathfrak{m})$ is a finite abelian extension of K,

(b) if a prime $\mathfrak{p} \in \mathcal{P}_K$ ramifies in $K(\mathfrak{m})$, then $\mathfrak{p} \mid \mathfrak{m}_0$, and if a real embedding w of K ramifies in $K(\mathfrak{m})$ — meaning that there is a complex embedding of $K(\mathfrak{m})$ that extends w — then $w \mid \mathfrak{m}_\infty$ (see [35, Chapter V, Remark 3.8]);

(c) the Artin reciprocity map

$$\mathcal{I}_\mathfrak{m} \to \mathrm{Gal}(K(\mathfrak{m})/K),\ \mathfrak{a} \mapsto \prod_{\mathfrak{p}|\mathfrak{a}} (\mathfrak{p}, K(\mathfrak{m})/K)^{v_\mathfrak{p}(\mathfrak{a})}$$

descends to a group isomorphism $\psi_{K(\mathfrak{m})/K} : \mathrm{Cl}_\mathfrak{m} \xrightarrow{\cong} \mathrm{Gal}(K(\mathfrak{m})/K)$.

Moreover, given moduli $\mathfrak{m}$ and $\mathfrak{n}$, we have $K(\mathfrak{m}) \subseteq K(\mathfrak{n})$ if $\mathfrak{m} \mid \mathfrak{n}$.

The ray class field $K(1)$ corresponding to the trivial modulus is called the *Hilbert class field of* K. The Hilbert class field is the maximal everywhere unramified abelian extension of K. The Artin map gives an isomorphism $\mathrm{Cl}(K) \cong \mathrm{Gal}(K(1)/K)$, and we have the following commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & i(K_\mathfrak{m})/i(K_{\mathfrak{m},1}) & \longrightarrow & \mathrm{Cl}_\mathfrak{m} & \longrightarrow & \mathrm{Cl} & \longrightarrow & 0 \\ & & \cong\downarrow & & \cong\downarrow{\scriptstyle \psi_{K(\mathfrak{m})/K}} & & \cong\downarrow{\scriptstyle \psi_{K(1)/K}} & & \\ 0 & \longrightarrow & \mathrm{Gal}(K(\mathfrak{m})/K(1)) & \longrightarrow & \mathrm{Gal}(K(\mathfrak{m})/K) & \longrightarrow & \mathrm{Gal}(K(1)/K) & \longrightarrow & 0 \end{array} \tag{2}$$

Using the isomorphism $K_\mathfrak{m}/K_{\mathfrak{m},1} \cong (R/\mathfrak{m})^*$, we get a homomorphism $(R/\mathfrak{m})^* \cong K_\mathfrak{m}/K_{\mathfrak{m},1} \to \mathrm{Cl}_\mathfrak{m}$; by exactness of (1), its kernel is $[R^*]_\mathfrak{m}$, the image of the unit group R^* in $(R/\mathfrak{m})^*$, and its range is $i(K_\mathfrak{m})/i(K_{\mathfrak{m},1})$. Therefore, using (2), we may identify $(R/\mathfrak{m})^*/[R^*]_\mathfrak{m}$ with $\mathrm{Gal}(K(\mathfrak{m})/K(1))$. Thus, Galois theory gives an inclusion-reversing bijection between the set of subgroups of $(R/\mathfrak{m})^*/[R^*]_\mathfrak{m}$ and the set of subfields of $K(\mathfrak{m})$ that contain $K(1)$.

Now we see that the arithmetic data $(\mathfrak{m}, \Gamma)$ used to define the congruence monoid $R_{\mathfrak{m},\Gamma}$ also canonically determines a class field of K. Namely, let $\bar{\Gamma}$ be the image of Γ under the composite $(R/\mathfrak{m})^* \twoheadrightarrow (R/\mathfrak{m})^*/[R^*]_\mathfrak{m} \cong \mathrm{Gal}(K(\mathfrak{m})/K(1))$, and consider the fixed field associated with $\bar{\Gamma}$, that is, the field $K(\mathfrak{m})^{\bar{\Gamma}}$ consisting of elements in $K(\mathfrak{m})$ that are fixed by every element of $\bar{\Gamma}$. Observe that $K(\mathfrak{m})^{\bar{\Gamma}}$ only depends on the image of Γ in $(R/\mathfrak{m})^*/[R^*]_\mathfrak{m}$ and that $K(\mathfrak{m})^{\bar{\Gamma}}$ always contains $K(1)$.

Using the inclusion $\mathrm{Gal}(K(\mathfrak{m})/K(1)) \hookrightarrow \mathrm{Gal}(K(\mathfrak{m})/K)$, we may also view $\bar{\Gamma}$ as subgroup of $\mathrm{Gal}(K(\mathfrak{m})/K)$. The isomorphism $\psi_{K(\mathfrak{m})/K} : \mathrm{Cl}_\mathfrak{m} \cong \mathrm{Gal}(K(\mathfrak{m})/K)$ takes the subgroup $i(K_{\mathfrak{m},\Gamma})/i(K_{\mathfrak{m},1})$ onto $\bar{\Gamma}$, so we have isomorphisms

$$\mathrm{Cl}_\mathfrak{m}^{\bar{\Gamma}} := \mathcal{I}_\mathfrak{m}/i(K_{\mathfrak{m},\Gamma}) \cong \mathrm{Cl}_\mathfrak{m}/(i(K_{\mathfrak{m},\Gamma})/i(K_{\mathfrak{m},1})) \cong \mathrm{Gal}(K(\mathfrak{m})/K)/\bar{\Gamma} \cong \mathrm{Gal}(K(\mathfrak{m})^{\bar{\Gamma}}/K). \tag{3}$$

2.4. **Reconstruction of initial data in number-theoretic context.** We now give several results that will be used in the proofs of our reconstruction theorems. We are interested in the question how much of the congruence monoid $R_{\mathfrak{m},\Gamma}$ we can recover from $K(\mathfrak{m})^{\bar{\Gamma}}$.

Remark 2.1. The map $(\mathfrak{m}, \Gamma) \mapsto R_{\mathfrak{m},\Gamma}$ is far from injective. However, from a number-theoretic perspective, it is natural to fix $\mathfrak{m}$ and let Γ vary; in terms of class fields, this corresponds to considering the intermediate extensions $K(1) \subseteq L \subseteq K(\mathfrak{m})$ for a fixed modulus $\mathfrak{m}$.

We will continue using the notation from Section 2.3. As we have seen, the number-theoretic data $(\mathfrak{m}, \Gamma)$ used to define the congruence monoid $R_{\mathfrak{m},\Gamma}$ also defines a class field of K, namely the intermediate extension $K(1) \subseteq K(\mathfrak{m})^{\bar{\Gamma}} \subseteq K(\mathfrak{m})$. From the discussion following (2), the extension $K(\mathfrak{m})^{\bar{\Gamma}}$ only depends on the image of Γ under the quotient map $(R/\mathfrak{m})^* \to (R/\mathfrak{m})^*/[R^*]_\mathfrak{m}$, so one should not expect to be able to recover the monoid $R_{\mathfrak{m},\Gamma}$ from $K(\mathfrak{m})^{\bar{\Gamma}}$. The following result shows exactly how much information is lost when passing from $R_{\mathfrak{m},\Gamma}$ to $K(\mathfrak{m})^{\bar{\Gamma}}$.

Proposition 2.2. *Suppose that $\mathfrak{m}$ and $\mathfrak{n}$ are moduli for K and that Γ and Λ are subgroups of $(R/\mathfrak{m})^*$ and $(R/\mathfrak{n})^*$, respectively. Then $K(\mathfrak{m})^{\bar{\Gamma}} = K(\mathfrak{n})^{\bar{\Lambda}}$ (equality in any algebraically closed field containing both $K(\mathfrak{m})^{\bar{\Gamma}}$ and $K(\mathfrak{n})^{\bar{\Lambda}}$) if and only if $R^* \cdot (R_{\mathfrak{n}} \cap R_{\mathfrak{m},\Gamma}) = R^* \cdot (R_{\mathfrak{m}} \cap R_{\mathfrak{n},\Lambda})$. In particular, if $\mathrm{supp}(\mathfrak{m}_0) = \mathrm{supp}(\mathfrak{n}_0)$, then $K(\mathfrak{m})^{\bar{\Gamma}} = K(\mathfrak{n})^{\bar{\Lambda}}$ if and only if $R^* \cdot R_{\mathfrak{m},\Gamma} = R^* \cdot R_{\mathfrak{n},\Lambda}$.*

Proof. It follows from [4, Theorem 3.5.1] that $K(\mathfrak{m})^{\bar{\Gamma}} = K(\mathfrak{n})^{\bar{\Lambda}}$ if and only if $\mathcal{I}_{\mathfrak{n}} \cap i(K_{\mathfrak{m},\Gamma}) = \mathcal{I}_{\mathfrak{m}} \cap i(K_{\mathfrak{n},\Lambda})$. This is equivalent to having $\mathcal{I}_{\mathfrak{n}}^+ \cap i(K_{\mathfrak{m},\Gamma}) = \mathcal{I}_{\mathfrak{m}}^+ \cap i(K_{\mathfrak{n},\Lambda})$, and since $\mathcal{I}_n^+ \cap i(K_{\mathfrak{m},\Gamma}) = \mathcal{I}_{\mathfrak{n}}^+ \cap i(R_{\mathfrak{m},\Gamma})$ and $\mathcal{I}_{\mathfrak{m}}^+ \cap i(K_{\mathfrak{n},\Lambda}) = \mathcal{I}_{\mathfrak{m}}^+ \cap i(R_{\mathfrak{n},\Lambda})$, this is also equivalent to $\mathcal{I}_{\mathfrak{n}}^+ \cap i(R_{\mathfrak{m},\Gamma}) = \mathcal{I}_{\mathfrak{m}}^+ \cap i(R_{\mathfrak{n},\Lambda})$. Since $a \in R^* \cdot (R_{\mathfrak{n}} \cap R_{\mathfrak{m},\Gamma})$ if and only if $(a) \in \mathcal{I}_{\mathfrak{n}}^+ \cap i(R_{\mathfrak{m},\Gamma})$, and $a \in R^* \cdot (R_{\mathfrak{m}} \cap R_{\mathfrak{n},\Lambda})$ if and only if $(a) \in \mathcal{I}_{\mathfrak{m}}^+ \cap i(R_{\mathfrak{n},\Lambda})$, we are done. □

The following observation shows that, if we know $\mathrm{supp}(\mathfrak{m}_0)$, then the class field $K(\mathfrak{m})^{\bar{\Gamma}}$ remembers as much as possible about $R_{\mathfrak{m},\Gamma}$.

Lemma 2.3. *We have $R^* \cdot R_{\mathfrak{m},\Gamma} = R_{\mathfrak{m},[R^*]_{\mathfrak{m}} \cdot \Gamma}$ where $[R^*]_{\mathfrak{m}} \cdot \Gamma$ is the subgroup of $(R/\mathfrak{m})^*$ generated by Γ and $[R^*]_{\mathfrak{m}}$, the image of the unit group.*

Proof. The containment "$\subseteq$" is obvious. Suppose that $a \in R_{\mathfrak{m}}$ such that $[a]_{\mathfrak{m}} \in [R^*]_{\mathfrak{m}} \cdot \Gamma$. Then there exists $u \in R^*$ and $b \in R_{\mathfrak{m},\Gamma}$ such that $[a]_{\mathfrak{m}} = [ub]_{\mathfrak{m}}$. That is,

- $(\mathrm{sign}(w(a)))_{w|\mathfrak{m}_\infty} = (\mathrm{sign}(w(u)))_{w|\mathfrak{m}_\infty} (\mathrm{sign}(w(b)))_{w|\mathfrak{m}_\infty}$, and
- $a + \mathfrak{m}_0 = ub + \mathfrak{m}_0$.

By the second item above, there exists $x \in \mathfrak{m}_0$ such that $a = ub + x = u(b + u^{-1}x)$. Now the first item implies that $(\mathrm{sign}(w(b + u^{-1}x)))_{w|\mathfrak{m}_\infty} = (\mathrm{sign}(w(b)))_{w|\mathfrak{m}_\infty}$, so we have $[b + u^{-1}x]_{\mathfrak{m}} = [b]_{\mathfrak{m}}$, that is, $b + u^{-1}x \in R_{\mathfrak{m},\Gamma}$. □

We now turn to the natural question whether conversely $R_{\mathfrak{m},\Gamma}$ determines $K(\mathfrak{m})^{\bar{\Gamma}}$.

Lemma 2.4. *For each prime $\mathfrak{p}$ not dividing $\mathfrak{m}_0$, $\mathfrak{p}$ is unramified in $K(\mathfrak{m})^{\bar{\Gamma}}$. Let $f_{\mathfrak{p}}^{\Gamma}$ denote the order of $[\mathfrak{p}]$ in $\mathrm{Cl}_{\mathfrak{m}}^{\bar{\Gamma}}$. Then $f_{\mathfrak{p}}^{\Gamma} = f_{K(\mathfrak{m})^{\bar{\Gamma}}/K}(\mathfrak{p})$, and $f_{\mathfrak{p}}^{\Gamma} = 1$ if and only if $\mathfrak{p}$ splits completely in $K(\mathfrak{m})^{\bar{\Gamma}}$.*

Proof. If $\mathfrak{p}$ is relatively prime to $\mathfrak{m}_0$, then $\mathfrak{p}$ is unramified in $K(\mathfrak{m})$ by property (b) of $K(\mathfrak{m})$ from § 2.3, and thus $\mathfrak{p}$ is also unramified in $K(\mathfrak{m})^{\bar{\Gamma}}$.

Under the isomorphism from (3), $[\mathfrak{p}]$ is taken to the Frobenius automorphism $(\mathfrak{p}, K(\mathfrak{m})^{\bar{\Gamma}}/K)$ whose order is precisely $f_{K(\mathfrak{m})^{\bar{\Gamma}}/K}(\mathfrak{p})$. Since $\mathfrak{p}$ splits in $K(\mathfrak{m})^{\bar{\Gamma}}$ if and only if $(\mathfrak{p}, K(\mathfrak{m})^{\bar{\Gamma}}/K) = \mathrm{id}$, we are done. □

Proposition 2.5. *Let $\mathfrak{m}$ and $\mathfrak{n}$ be moduli for K, and let Γ and Λ be subgroups of $(R/\mathfrak{m})^*$ and $(R/\mathfrak{n})^*$, respectively. For $\mathfrak{p} \in \mathcal{P}_K^{\mathfrak{mn}}$, let $f_{\mathfrak{p}}^{\Gamma}$ denote the order of $[\mathfrak{p}]$ in $\mathrm{Cl}_{\mathfrak{m}}^{\bar{\Gamma}}$ and let $f_{\mathfrak{p}}^{\Lambda}$ be the order of $[\mathfrak{p}]$ in $\mathrm{Cl}_{\mathfrak{n}}^{\bar{\Lambda}}$. If $f_{\mathfrak{p}}^{\Gamma} = f_{\mathfrak{p}}^{\Lambda}$ for all but finitely many $\mathfrak{p}$ in $\mathcal{P}_K^{\mathfrak{mn}}$, then $K(\mathfrak{m})^{\bar{\Gamma}} = K(\mathfrak{n})^{\bar{\Lambda}}$ (equality in any algebraic closure of K that contains both $K(\mathfrak{m})^{\bar{\Gamma}}$ and $K(\mathfrak{n})^{\bar{\Lambda}}$).*

Proof. Suppose that $f_{\mathfrak{p}}^{\Gamma} = f_{\mathfrak{p}}^{\Lambda}$ for all but finitely many $\mathfrak{p}$ in $\mathcal{P}_K^{\mathfrak{mn}}$. Then Lemma 2.4 implies that for all but finitely many $\mathfrak{p}$ in $\mathcal{P}_K^{\mathfrak{mn}}$, $\mathfrak{p}$ splits completely in $K(\mathfrak{m})^{\bar{\Gamma}}$ if and only if $\mathfrak{p}$ splits completely in $K(\mathfrak{n})^{\bar{\Lambda}}$. Hence, $K(\mathfrak{m})^{\bar{\Gamma}} = K(\mathfrak{n})^{\bar{\Lambda}}$ by [35, Chapter V, Theorem 3.25]. □

Corollary 2.6. *Suppose $\mathfrak{m}$ and $\mathfrak{n}$ are moduli for K and Γ and Λ are subgroups of $(R/\mathfrak{m})^*$ and $(R/\mathfrak{n})^*$, respectively. If $R_{\mathfrak{m},\Gamma} = R_{\mathfrak{n},\Lambda}$, then $K(\mathfrak{m})^{\bar{\Gamma}} = K(\mathfrak{n})^{\bar{\Lambda}}$ (equality in any algebraically closed field containing both $K(\mathfrak{m})^{\bar{\Gamma}}$ and $K(\mathfrak{n})^{\bar{\Lambda}}$).*

Proof. If $R_{\mathfrak{m},\Gamma} = R_{\mathfrak{n},\Lambda}$, then $\mathrm{Cl}_{\mathfrak{m}}^{\bar{\Gamma}} = \mathrm{Cl}_{\mathfrak{n}}^{\bar{\Lambda}}$, so that for each $\mathfrak{p} \in \mathcal{P}_K^{\mathfrak{mn}}$, $f_{\mathfrak{p}}^{\Gamma} = 1$ if and only if $f_{\mathfrak{p}}^{\Lambda} = 1$. Hence, $K(\mathfrak{m})^{\bar{\Gamma}} = K(\mathfrak{n})^{\bar{\Lambda}}$ by Proposition 2.5. □

The class field $\mathbb{K} := K(\mathfrak{m})^{\bar{\Gamma}}$ is always Galois over K, but we will need to know when $\mathbb{K}$ is Galois over $\mathbb{Q}$. Let $\overline{\mathbb{Q}} \subseteq \mathbb{C}$ denote the field of algebraic numbers.

Proposition 2.7. *Let K be a number field. Suppose that $\mathfrak{m}$ is a modulus for K and that Γ a group of residues modulo $\mathfrak{m}$. Let $K \subseteq \overline{\mathbb{Q}}$ be any embedding, so that we can view $\mathbb{K}$ as a subfield of $\overline{\mathbb{Q}}$. If $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, then we denote by $\sigma(\mathfrak{m})$ the modulus for $\sigma(K)$ defined by $\sigma(\mathfrak{m})_0 := \sigma(\mathfrak{m}_0)$ and $w \mid \sigma(\mathfrak{m})_\infty$ if and only if $w \circ \sigma \mid \mathfrak{m}_\infty$. Then $\sigma(\mathbb{K})$ is the class field of $\sigma(K)$ corresponding to $(\sigma(\mathfrak{m}), \sigma(\Gamma))$.*

Proof. Let $L = \sigma(K)$ and let S denote the ring of algebraic integers in L. The isomorphism $R \to S$, $a \mapsto \sigma(a)$, defines an isomorphism $(R/\mathfrak{m})^* \cong (S/\sigma(\mathfrak{m}))^*$ that we shall also denote by σ. Observe that $\sigma([R^*]_{\mathfrak{m}}) = [S^*]_{\sigma(\mathfrak{m})}$, so that $\overline{\sigma(\Gamma)} = \sigma(\bar{\Gamma})$.

We need to show that $\sigma(\mathbb{K})$ and $\mathbb{L} := L(\sigma(\mathfrak{m}))^{\sigma(\bar{\Gamma})}$ are equal (as subfields of $\overline{\mathbb{Q}}$). Now σ induces an isomorphism $\mathcal{I}_K^{\mathfrak{m}} \cong \mathcal{I}_L^{\sigma(\mathfrak{m})}$ where $\mathcal{I}_K^{\mathfrak{m}}$ denotes the group of fractional ideals of K relatively prime to $\mathfrak{m}_0$ and $\mathcal{I}_L^{\sigma(\mathfrak{m})}$ denotes the group of fractional ideals of L relatively prime to $\sigma(\mathfrak{m})_0$. If $x \in K^\times$, then x is relatively prime to $\mathfrak{m}_0$ if and only if $\sigma(x)$ is relatively prime to $\sigma(\mathfrak{m})_0$, and $[x]_{\mathfrak{m}} \in \Gamma$ if and only if $[\sigma(x)]_{\sigma(\mathfrak{m})} \in \sigma(\Gamma)$. So the isomorphism $K \cong L$ carries $K_{\mathfrak{m},\Gamma}$ onto $L_{\sigma(\mathfrak{m}),\sigma(\Gamma)}$. Thus, we have an isomorphism $\mathrm{Cl}_{\mathfrak{m}}^{\bar{\Gamma}}(K) \cong \mathrm{Cl}_{\sigma(\mathfrak{m})}^{\sigma(\bar{\Gamma})}(L)$ given by $[\mathfrak{a}] \mapsto [\sigma(\mathfrak{a})]$. It follows that $\mathfrak{q} \in \mathcal{P}_L^{\sigma(\mathfrak{m})}$ splits completely in $\mathbb{L}$ if and only if $\sigma^{-1}(\mathfrak{q})$ splits completely in $\mathbb{K}$.

For $\mathfrak{a} \in \mathcal{I}_K^{\mathfrak{m}}$, we have $\psi_{\sigma(\mathbb{K})/\sigma(K)}(\sigma(\mathfrak{a})) = \sigma \circ \psi_{\mathbb{K}/K}(\mathfrak{a}) \circ \sigma^{-1}$ (see, for example, [24, Chapter X, § 1]). Hence, the following diagram commutes:

$$\begin{array}{ccc} \mathrm{Cl}_{\mathfrak{m}}^{\bar{\Gamma}}(K) & \xrightarrow[\cong]{\psi_{\mathbb{K}/K}} & \mathrm{Gal}(\mathbb{K}/K) \\ \cong \big\downarrow {\scriptstyle [\mathfrak{a}]\mapsto[\sigma(\mathfrak{a})]} & & \cong \big\downarrow {\scriptstyle \tau \mapsto \sigma\circ\tau\circ\sigma^{-1}} \\ \mathrm{Cl}_{\sigma(\mathfrak{m})}^{\sigma(\bar{\Gamma})}(L) & \xrightarrow[\cong]{\psi_{\sigma(\mathbb{K})/L}} & \mathrm{Gal}(\sigma(\mathbb{K})/L). \end{array}$$

Thus Lemma 2.4 implies that $\mathfrak{p} \in \mathcal{P}_K^{\mathfrak{m}}$ splits completely in $\mathbb{K}$ if and only if $\sigma(\mathfrak{p})$ splits completely in $\sigma(\mathbb{K})$.

All in all, we have that $\mathfrak{q} \in \mathcal{P}_L^{\sigma(\mathfrak{m})}$ splits completely in $\mathbb{L}$ if and only if $\mathfrak{q}$ splits completely in $\sigma(\mathbb{K})$. Hence, $\mathbb{L} = \sigma(\mathbb{K})$ by [35, Chapter V, Theorem 3.25]. □

Corollary 2.8. *Suppose that K is a finite Galois extension of $\mathbb{Q}$, $\mathfrak{m}$ is a modulus for K, and Γ is a group of residues modulo $\mathfrak{m}$. Then $\mathbb{K}$ is Galois over $\mathbb{Q}$ if and only if $R^* \cdot (R_{\sigma(\mathfrak{m})} \cap R_{\mathfrak{m},\Gamma}) = R^* \cdot (R_{\mathfrak{m}} \cap R_{\sigma(\mathfrak{m}),\sigma(\Gamma)})$ for all $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$. Hence, if $\sigma(\mathfrak{m}) = \mathfrak{m}$ and $\sigma(\Gamma) = \Gamma$ for all $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, then $\mathbb{K}$ is Galois over $\mathbb{Q}$.*

Proof. Since K is Galois over $\mathbb{Q}$, we may view K as a subfield of $\overline{\mathbb{Q}}$, and thus also view $\mathbb{K}$ as a subfield of $\overline{\mathbb{Q}}$. The field $\mathbb{K}$ is Galois over $\mathbb{Q}$ if and only if $\sigma(\mathbb{K}) = \mathbb{K}$ for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Combining Proposition 2.7 and Proposition 2.2, we see that $\sigma(\mathbb{K}) = \mathbb{K}$ for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ if and only if $R^* \cdot (R_{\sigma(\mathfrak{m})} \cap R_{\mathfrak{m},\Gamma}) = R^* \cdot (R_{\mathfrak{m}} \cap R_{\sigma(\mathfrak{m}),\sigma(\Gamma)})$ for every $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Since K is Galois, each $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ maps K onto itself and thus determines an element of $\mathrm{Gal}(K/\mathbb{Q})$. Moreover, every element of $\mathrm{Gal}(K/\mathbb{Q})$ is the restriction of an element in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, so the above condition is equivalent to $R^* \cdot (R_{\sigma(\mathfrak{m})} \cap R_{\mathfrak{m},\Gamma}) = R^* \cdot (R_{\mathfrak{m}} \cap R_{\sigma(\mathfrak{m}),\sigma(\Gamma)})$ for every $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$. □

Example 2.9. *Let K be a finite Galois extension of $\mathbb{Q}$ and let $l \in \mathbb{Z}_{>0}$. Let $\mathfrak{m}_\infty$ be either trivial or consist of all real embeddings of K, and let $\mathfrak{m}_0 = lR$. Then $\sigma(\mathfrak{m}) = \mathfrak{m}$ for all $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$. The inclusion $\mathbb{Z} \hookrightarrow R$ descends to an inclusion $(\mathbb{Z}/l\mathbb{Z})^* \hookrightarrow (R/lR)^*$; if Γ_0 is the image of any subgroup of $(\mathbb{Z}/l\mathbb{Z})^*$ under this inclusion, then $\Gamma := \prod_{w|\mathfrak{m}_\infty} \langle \pm 1 \rangle \times \Gamma_0$ is a $\mathrm{Gal}(K/\mathbb{Q})$-invariant subgroup of $(R/\mathfrak{m})^*$. Now the corresponding class field $\mathbb{K}$ is Galois over $\mathbb{Q}$ by Corollary 2.8.*

3. Pure infiniteness

Notational conventions: To simplify notations, we will from now on and throughout this paper – when it is safe to do so – drop sub- and superscripts and write $M := R_{\mathfrak{m},\Gamma}$, $Q = M^{-1} \cdot R$, $G = M^{-1}M$, $\mu := \mu_{\mathfrak{m},\Gamma} := \mathrm{tor}(M^*)$, $m := \#\mu$, $C := \mathrm{Cl}_{\mathfrak{m}}^{\bar{\Gamma}}$ ($:= \mathrm{Cl}_{\mathfrak{m}}(K)/\bar{\Gamma}$), $\mathbb{K} := K(\mathfrak{m})^{\bar{\Gamma}}$, and $f(\mathfrak{p}) := f_{\mathfrak{p}}^{\Gamma}$.

In this section, we show that $C^*_\lambda(R \rtimes M)$ is strongly purely infinite.

Theorem 3.1. *For every congruence monoid M as in § 2.2, we have $C^*_\lambda(R \rtimes M) \cong \mathcal{O}_\infty \otimes C^*_\lambda(R \rtimes M)$.*

Proof. First of all, as explained in § 2.2, $C^*_\lambda(R \rtimes M)$ is isomorphic to the reduced groupoid C*-algebra of the partial transformation groupoid $(Q \rtimes G) \ltimes \Omega$. Now the same proof as for [30, Theorem 4.6] – with the following slight modifications – shows that $(Q \rtimes G) \ltimes \Omega$ is purely infinite in the sense of [34]: Replace the ideal J defined as $\bigcap_{i=1}^n I_i$ in the proof of [30, Theorem 4.6] by $J := (\bigcap_{i=1}^n I_i) \cap \mathfrak{m}_0$ (where $\mathfrak{m}_0$ is as in § 2.2). Then follow the proof of [30, Theorem 4.6] to find an element $a \in (1 + J) \setminus R^*$. The point is that because of our modified definition of J, we will always be able to find a suitable power a^ε of a such that a^ε lies in M (and a^ε still lies in $(1 + J) \setminus R^*$ because this set is multiplicatively closed). With a^ε in place of a, the same proof as for [30, Theorem 4.6] shows that $(Q \rtimes G) \ltimes \Omega$ is purely infinite. As observed in [34, § 4.2], this implies that $C^*_\lambda(R \rtimes M) \cong C^*_r((Q \rtimes G) \ltimes \Omega)$ is purely infinite. As explained in § 2.2, the primitive ideal space of $C^*_\lambda(R \rtimes M)$ is given by $2^{\mathcal{P}^{\mathfrak{m}}_K}$. And since $2^{\mathcal{P}^{\mathfrak{m}}_K}$ has a basis for its topology of compact-open subsets given by $U_F := \big\{T \in 2^{\mathcal{P}^{\mathfrak{m}}_K} \colon T \cap F = \emptyset\big\}$, where F runs through all finite subsets of $\mathcal{P}^{\mathfrak{m}}_K$, and because $C^*_\lambda(R \rtimes M)$ is separable and purely infinite, it follows from [39, Proposition 2.11] that $C^*_\lambda(R \rtimes M)$ has the ideal property from [39]. Hence [39, Proposition 2.14] implies that $C^*_\lambda(R \rtimes M)$ is strongly purely infinite. Finally, as $C^*_\lambda(R \rtimes M)$ is separable, nuclear and unital, [22, Theorem 8.6] implies that $C^*_\lambda(R \rtimes M) \cong \mathcal{O}_\infty \otimes C^*_\lambda(R \rtimes M)$, as desired. □

4. K-theory

4.1. **K-theory for our semigroup C*-algebras.** First of all, let us compute K-theory for our semigroup C*-algebras. For each class $\mathfrak{k} \in C$, choose an integral ideal $\mathfrak{a}_\mathfrak{k} \in \mathfrak{k}$; for $\mathfrak{k} = [R]$, take $\mathfrak{a}_\mathfrak{k} = R$. Let $\iota_\mathfrak{k}$ denote the homomorphism $C^*(\mathfrak{a}_\mathfrak{k} \rtimes M^*) \to C^*_\lambda(R \rtimes M)$ determined by $u_x \mapsto \lambda(x)e_{\mathfrak{a}_\mathfrak{k}}$ where, for $x \in \mathfrak{a}_\mathfrak{k} \rtimes M^*$, u_x denotes the corresponding unitary in $C^*(\mathfrak{a}_\mathfrak{k} \rtimes M^*)$ and $e_\mathfrak{a}$ is the projection in $C^*_\lambda(R \rtimes M)$ corresponding to the constructible right ideal $\mathfrak{a} \times (\mathfrak{a} \cap R_{\mathfrak{m},\Gamma})$ of $R \rtimes M$.

Theorem 4.1. *The homomorphisms $\iota_\mathfrak{k}$ induce an isomorphism*

$$\sum_{\mathfrak{k} \in C} (\iota_\mathfrak{k})_* : \bigoplus_{\mathfrak{k} \in C} K_*(C^*(\mathfrak{a}_\mathfrak{k} \rtimes M^*)) \cong K_*(C^*_\lambda(R \rtimes M)).$$

Here K_* denotes $K_0 \oplus K_1$ as a $\mathbb{Z}/2\mathbb{Z}$-graded abelian group.

Proof. The group $G(R \rtimes M) = Q \rtimes G$ is solvable, hence amenable, so $Q \rtimes G$ satisfies the Baum-Connes conjecture with arbitrary coefficients by [17]. Since $R \rtimes M \subseteq Q \rtimes G$ is left Ore by [1, Proposition 3.2], $R \rtimes M \subseteq Q \rtimes G$ satisfies the left Toeplitz condition; by [1, Proposition 3.4], $\mathcal{J}_{R \rtimes M}$ is independent, so $\mathcal{J}_{R \rtimes M \subseteq Q \rtimes G}$ is independent by [27, Lemma 4.2]. Thus, we can apply [10, Corollary 3.14] (take for the group G in [10] our group $Q \rtimes G$ and for I in [10] the set $\mathcal{J}^\times_{R \rtimes M \subseteq Q \rtimes G}$). □

Remark 4.2. There is a parallel between the K-theory formula for $C^*_\lambda(R \rtimes M)$ given by Theorem 4.1 and the parameterization of the low temperature KMS states on $C^*_\lambda(R \rtimes M)$ with respect to the canonical time evolution coming from the norm map on K. Indeed, [2, Theorem 3.2(iii)] implies that for each fixed $\beta > 2$, the simplex of KMS_β states on $C^*_\lambda(R \rtimes M)$ is isomorphic to the simplex of tracial states on the C*-algebra $\bigoplus_{\mathfrak{k} \in C} C^*(\mathfrak{a}_\mathfrak{k} \rtimes M^*)$.

This connection has been observed in the case of the full $ax + b$-semigroup $R \rtimes R^\times$ (see the discussion following [11, Theorem 6.6.1]).

4.1.1. *The case of the rational number field.* Consider the case $K = \mathbb{Q}$. Then the group C*-algebras appearing in the K-theory formula given by Theorem 4.1 are all isomorphic to either $\mathbb{Z} \rtimes \langle \pm 1 \rangle$ or $\mathbb{Z}$ according to whether or not $-1 \in \mathbb{Z}_{\mathfrak{m},\Gamma}$. Hence,

- $K_\bullet(C^*_\lambda(\mathbb{Z} \rtimes \mathbb{Z}_{\mathfrak{m},\Gamma})) \cong \begin{cases} \mathbb{Z}^{3 \cdot \#C} & \text{if } \bullet = 0, \\ \{0\} & \text{if } \bullet = 1 \end{cases}$ when $-1 \in \mathbb{Z}_{\mathfrak{m},\Gamma}$;

- $K_\bullet(C^*_\lambda(\mathbb{Z} \rtimes \mathbb{Z}_{\mathfrak{m},\Gamma})) \cong \begin{cases} \mathbb{Z}^{\#C} & \text{if } \bullet = 0, \\ \mathbb{Z}^{\#C} & \text{if } \bullet = 1 \end{cases}$ when $-1 \notin \mathbb{Z}_{\mathfrak{m},\Gamma}$.

4.1.2. *On the summands in the K-theory formula for our semigroup C*-algebras.* Let us now compare the summands in the K-theory formula in Theorem 4.1.

Proposition 4.3. *For every non-zero ideal $\mathfrak{a}$ of R, we have that $K_*(C^*(\mathfrak{a} \rtimes M^*))$ and $K_*(C^*(R \rtimes M^*))$ are isomorphic up to inverting m, i.e.,*

$$\mathbb{Z}[\tfrac{1}{m}] \otimes K_*(C^*(\mathfrak{a} \rtimes M^*)) \cong \mathbb{Z}[\tfrac{1}{m}] \otimes K_*(C^*(R \rtimes M^*)).$$

For the proof, we recall the main result from [25], as it is stated for $\mathfrak{a} = R$ and even m in [32].

Let $\mathfrak{a}$ be a non-zero ideal of R, $\iota : \mathfrak{a} \to \mathfrak{a} \rtimes \mu$ the canonical inclusion, and denote by ι_* the homomorphism $K_\bullet(C^*(\mathfrak{a})) \to K_\bullet(C^*(\mathfrak{a} \rtimes \mu))$ induced by ι on $K_\bullet$ ($\bullet = 0, 1$). Moreover, given a finite subgroup F of $\mathfrak{a} \rtimes \mu$, consider the canonical projection $F \twoheadrightarrow \{e\}$ from F onto the trivial group. This projection induces a homomorphism $C^*(F) \to \mathbb{C}$ of group C*-algebras, hence a homomorphism on K_0, $K_0(C^*(F)) \to K_0(\mathbb{C})$. Let us denote the kernel of this homomorphism by $\widetilde{R}_{\mathbb{C}}(F)$. The canonical inclusion $F \to \mathfrak{a} \rtimes \mu$ induces a homomorphism $\iota_F : C^*(F) \to C^*(\mathfrak{a} \rtimes \mu)$, hence a homomorphism $K_0(C^*(F)) \to K_0(C^*(\mathfrak{a} \rtimes \mu))$. Restricting this homomorphism to $\widetilde{R}_{\mathbb{C}}(F)$, we obtain $(\iota_F)_* : \widetilde{R}_{\mathbb{C}}(F) \to K_0(C^*(\mathfrak{a} \rtimes \mu))$. Here are the main results from [25]:

Theorem 4.4 (Langer-Lück)**.** *With the notations from above, we have*

- *$K_0(C^*(\mathfrak{a} \rtimes \mu))$ is finitely generated and torsion-free.*
  - *$\mathrm{rk}_{\mathbb{Z}}(\mathrm{im}\,(\iota_*)) = \mathrm{rk}_{\mathbb{Z}}((K_0(C^*(\mathfrak{a})))^\mu)$, and if $\mathcal{M}$ denotes the set of conjugacy classes of maximal finite subgroups of $\mathfrak{a} \rtimes \mu$, then $\sum_{(F)\in\mathcal{M}} (\iota_F)_* : \bigoplus_{(F)\in\mathcal{M}} \widetilde{R}_{\mathbb{C}}(F) \to K_0(C^*(\mathfrak{a} \rtimes \mu))$ is injective.*
  - *We have $\mathrm{im}\,(\iota_*) \cap \left(\sum_{(F)\in\mathcal{M}} \mathrm{im}\,((\iota_F)_*)\right) = \{0\}$, and $\iota_* \oplus \left(\sum_{(F)\in\mathcal{M}} (\iota_F)_*\right)$ is surjective after inverting m.*
- *$K_1(C^*(\mathfrak{a} \rtimes \mu))$ is finitely generated and torsion-free.*
  - *The map $K_1(C^*(\mathfrak{a}))^\mu \to K_1(C^*(\mathfrak{a} \rtimes \mu))$ induced by ι_* is an isomorphism after inverting m.*

As above, let $\mathfrak{a}$ be a non-zero ideal of R. We obtain canonical inclusions $\mathfrak{a} \hookrightarrow R$ and $\mathfrak{a} \rtimes \mu \hookrightarrow R \rtimes \mu$, both of which are denoted by i. Let $K^{\mathfrak{a}}_{\mathrm{fin}} \subseteq K_0(C^*(\mathfrak{a} \rtimes \mu))$ be defined by

$$K^{\mathfrak{a}}_{\mathrm{fin}} := \Big(\sum_{(F)\in\mathcal{M}} \mathrm{im}\,((\iota_F)_*) \Big).$$

Moreover, for $\bullet = 0, 1$, let $K^{\mathfrak{a}}_{\bullet,\mathrm{inf}} \subseteq K_\bullet(C^*(\mathfrak{a} \rtimes \mu))$ be given by $K^{\mathfrak{a}}_{\bullet,\mathrm{inf}} := \mathrm{im}\,(\iota_*)$. Here we use the same notation as in the Theorem 4.4. Moreover, let $N(\mathfrak{a}) := \#R/\mathfrak{a}$.

Lemma 4.5. *For every non-zero ideal $\mathfrak{a}$ of R, we have $\mathrm{rk}_{\mathbb{Z}}(K^{\mathfrak{a}}_{\bullet,\mathrm{inf}}) = \mathrm{rk}_{\mathbb{Z}}(K^R_{\bullet,\mathrm{inf}})$ for $\bullet = 0, 1$.*

Proof. Clearly, $i_* : K_\bullet(C^*(\mathfrak{a})) \to K_\bullet(C^*(R))$ is injective and μ-equivariant, so that it induces an embedding $(K_\bullet(C^*(\mathfrak{a})))^\mu \to (K_\bullet(C^*(R)))^\mu$. By Theorem 4.4, this shows $\mathrm{rk}_{\mathbb{Z}}(K^{\mathfrak{a}}_{\bullet,\mathrm{inf}}) \leq \mathrm{rk}_{\mathbb{Z}}(K^R_{\bullet,\mathrm{inf}})$. For the reverse inequality, take $x \in (K_\bullet(C^*(R)))^\mu$. Recall that $N(\mathfrak{a}) = \#R/\mathfrak{a}$. Set $n := [K : \mathbb{Q}] = \mathrm{rk}_{\mathbb{Z}}(R)$. Then $N(\mathfrak{a})^n \cdot x$ lies in $\mathrm{im}\,(i_*)$, say $N(\mathfrak{a})^n \cdot x = i_*(y)$. Since i_* is injective and μ-equivariant, y must be fixed by μ. Hence the image of $(K_\bullet(C^*(\mathfrak{a})))^\mu \to (K_\bullet(C^*(R)))^\mu$ has finite index. This shows $\mathrm{rk}_{\mathbb{Z}}(K^{\mathfrak{a}}_{\bullet,\mathrm{inf}}) \geq \mathrm{rk}_{\mathbb{Z}}(K^R_{\bullet,\mathrm{inf}})$. □

It is straighforward to check that $i_*(K^{\mathfrak{a}}_{\bullet,\mathrm{inf}}) \subseteq K^R_{\bullet,\mathrm{inf}}$. Since $i_* : K_\bullet(C^*(\mathfrak{a})) \to K_\bullet(C^*(R))$ is surjective after inverting $N(\mathfrak{a})$, Lemma 4.5 has the following immediate consequence:

Corollary 4.6. *$i_*|_{K^{\mathfrak{a}}_{\bullet,\mathrm{inf}}} : K^{\mathfrak{a}}_{\bullet,\mathrm{inf}} \to K^R_{\bullet,\mathrm{inf}}$ is an isomorphism after inverting $N(\mathfrak{a})$.*

Similarly, we have that $i_*(K^{\mathfrak{a}}_{\mathrm{fin}}) \subseteq K^R_{\mathrm{fin}}$. Our goal is to show that for particular choices of $\mathfrak{a}$, $i_*|_{K^{\mathfrak{a}}_{\mathrm{fin}}} : K^{\mathfrak{a}}_{\mathrm{fin}} \to K^R_{\mathrm{fin}}$ is an isomorphism.

Let $\pi : \mathfrak{a} \rtimes \mu \twoheadrightarrow \mu$ be the canonical projection.

Lemma 4.7. *For every finite subgroup $F \subseteq \mathfrak{a} \rtimes \mu$, $\pi|_F : F \to \mu$ is injective.*

Proof. Take $x \in \ker(\pi|_F)$. Then $x \in \ker(\pi) = \mathfrak{a}$ and $x \in F$. However, every non-zero element in $\mathfrak{a}$ has infinite order as $\mathfrak{a}$ is torsion-free. Hence x must be trivial, so that $\pi|_F$ is indeed injective. □

Let ζ be a root of unity such that $\mu = \langle\zeta\rangle$.

Corollary 4.8. *Every finite subgroup F is of the form $F = \langle(r, \zeta^i)\rangle$ for some natural number $0 \leq i \leq m-1$ and $r \in \mathfrak{a}$.*

Lemma 4.9. *Two elements (r, ζ^i) and (s, ζ^j) are conjugate in $\mathfrak{a} \rtimes \mu$ if and only if $i = j$ and there exist $\xi \in \mu$ and $t \in \mathfrak{a}$ such that $s = \xi(r + (1 - \zeta^i)t)$.*

Proof. (r, ζ^i) and (s, ζ^j) are conjugate if and only if there is $(b, a) \in \mathfrak{a} \rtimes \mu$ such that

$$(s, \zeta^j) = (b, a)(r, \zeta^i)(b, a)^{-1} = (ar + (1 - \zeta^i)b, \zeta^i),$$

which holds if and only if $i = j$ and $s = ar + (1 - \zeta^i)b$. Set $\xi := a$ and $t := a^{-1}b$. □

Now take $\mathfrak{a}$ such that, for every $1 \neq \xi \in \mu$, $\mathfrak{a}$ and $(1 - \xi)$ are relatively prime (as ideals of R). Let $\mathcal{M}^{\mathfrak{a}}$ be the set of conjugacy classes of maximal finite subgroups of $\mathfrak{a} \rtimes \mu$.

Lemma 4.10. *For every such $\mathfrak{a}$, $\mathcal{M}^{\mathfrak{a}} \to \mathcal{M}^R$, $(F) \mapsto (F)$ is a bijection.*

Proof. We write $\sim_{\mathfrak{a}}$ for conjugacy in $\mathfrak{a} \rtimes \mu$.

We first show that for a finite subgroup $F' = \langle(r, \xi)\rangle$ of $R \rtimes \mu$, there exists a finite subgroup $\tilde{F}$ of $\mathfrak{a} \rtimes \mu$ such that $F \sim_R \tilde{F}$. The point is that since $\mathfrak{a}$ and $(1 - \xi)$ are relatively prime, we have $R = \mathfrak{a} + (1 - \xi)$, so that there exists $t \in R$ and $s \in \mathfrak{a}$ such that $r = s + (1 - \xi)t$. Now set $\tilde{F} := \langle(s, \xi)\rangle$. Then $\tilde{F} \subseteq \mathfrak{a} \rtimes \mu$, and by Lemma 4.9, we have $F' \sim_R \tilde{F}$.

Secondly, we show that given $r, s \in \mathfrak{a}$ and $1 \neq \xi \in \mu$ with $(r, \xi) \sim_R (s, \xi)$, say $(s, \xi) = (b, a)(r, \xi)(b, a)^{-1}$, we must have $(b, a) \in \mathfrak{a} \rtimes \mu$, i.e., $(r, \xi) \sim_{\mathfrak{a}} (s, \xi)$. Namely, by the same computation as in Lemma 4.9, $(s, \xi) = (b, a)(r, \xi)(b, a)^{-1}$ implies that $s = ar + (1 - \xi)b$. But then $(1 - \xi)b = s - ar \in \mathfrak{a}$, so that $b \in ((1 - \xi)^{-1} \cdot \mathfrak{a}) \cap R = \mathfrak{a}$ since $\mathfrak{a}$ and $(1 - \xi)$ are relatively prime.

With these two observations, we show that the map $\mathcal{M}^{\mathfrak{a}} \to \mathcal{M}^R$, $(F) \mapsto (F)$ is well-defined: Assume that $\{e\} \neq F \subseteq \mathfrak{a} \rtimes \mu$ and $F' \subseteq R \rtimes \mu$ are finite subgroups with $F \subseteq F'$. By our first observation, there exists $\tilde{F} \subseteq \mathfrak{a} \rtimes \mu$ such that $F \sim_R \tilde{F}$, say $F = (b, a)\tilde{F}(b, a)^{-1}$. Suppose $F = \langle(r, \xi)\rangle$, where $\xi \neq 1$ as $F \neq \{e\}$. As $F \subseteq F'$, we must have $(b, a)^{-1}(r, \xi)(b, a) \in \mathfrak{a} \rtimes \mu$. By our second observation, this implies $(b, a) \in \mathfrak{a} \rtimes \mu$, so that $F' \subseteq (b, a)(\mathfrak{a} \rtimes \mu)(b, a)^{-1} = \mathfrak{a} \rtimes \mu$. This shows that maximal finite subgroups of $\mathfrak{a} \rtimes \mu$ are still maximal in $R \rtimes \mu$. So $\mathcal{M}^{\mathfrak{a}} \to \mathcal{M}^R$, $(F) \mapsto (F)$ is well-defined.

By our first observation, $\mathcal{M}^{\mathfrak{a}} \to \mathcal{M}^R$, $(F) \mapsto (F)$ is surjective. To see injectivity, let F and F' be maximal finite subgroups of $\mathfrak{a} \rtimes \mu$, and suppose that $F \sim_R F'$, say $\gamma F \gamma^{-1} = F'$ for some $\gamma \in R \rtimes \mu$. Suppose $F = \langle(r, \xi)\rangle$. Let $(s, \xi) = \gamma(r, \xi)\gamma^{-1}$. Then $F' = \langle(s, \xi)\rangle$. In particular, $(s, \xi) \in \mathfrak{a} \rtimes \mu$, and by our second observation, we must have $(r, \xi) \sim_{\mathfrak{a}} (s, \xi)$, i.e., $F \sim_{\mathfrak{a}} F'$. □

Corollary 4.11. *For every $\mathfrak{a}$ as in Lemma 4.10, $i_*|_{K^{\mathfrak{a}}_{\mathrm{fin}}} : K^{\mathfrak{a}}_{\mathrm{fin}} \to K^R_{\mathrm{fin}}$ is an isomorphism.*

We are now ready for

Proof of Proposition 4.3. By Corollary 4.6 and 4.11, for very ideal $\mathfrak{a}$ as in Lemma 4.10, we have in K_0 that

$$i_*|_{K^{\mathfrak{a}}_{0,\inf}+K^{\mathfrak{a}}_{\mathrm{fin}}} : K^{\mathfrak{a}}_{0,\inf} + K^{\mathfrak{a}}_{\mathrm{fin}} \to K^{R}_{0,\inf} + K^{R}_{\mathrm{fin}}$$

is an isomorphism after inverting $N(\mathfrak{a})$. By Theorem 4.4, $i_* : K_0(C^*(\mathfrak{a} \rtimes \mu)) \to K_0(C^*(R \rtimes \mu))$ is an isomorphism after inverting $m \cdot N(\mathfrak{a})$.
In K_1, consider the commutative diagram

$$\begin{array}{ccc} K_1(C^*(\mathfrak{a})) & \xrightarrow{i_*} & K_1(C^*(R)) \\ \downarrow & & \downarrow \\ K_1(C^*(\mathfrak{a} \rtimes \mu)) & \xrightarrow{i_*} & K_1(C^*(R \rtimes \mu)) \end{array}$$

The upper horizontal arrow is bijective after inverting $N(\mathfrak{a})$, and the vertical arrows are surjective after inverting m, so that the lower horizontal arrow must be surjective after inverting $m \cdot N(\mathfrak{a})$. This together with Lemma 4.5 implies that the lower horizontal arrow must be an isomorphism after inverting $m \cdot N(\mathfrak{a})$. Hence, by applying the Pimsner-Voiculescu sequence, we see that $i_* : K_*(C^*(\mathfrak{a} \rtimes M^*)) \to K_*(C^*(R \rtimes M^*))$ is an isomorphism after inverting $m \cdot N(\mathfrak{a})$. In particular, $\mathrm{rk}_{\mathbb{Z}}(K_*(C^*(\mathfrak{a} \rtimes M^*))) = \mathrm{rk}_{\mathbb{Z}}(K_*(C^*(R \rtimes M^*)))$. Now given an arbitrary non-zero ideal $\mathfrak{a}$ of R, we can choose another ideal $\mathfrak{b}$ of R in the same ideal class of $\mathfrak{a}$ such that $\mathfrak{b}$ is relatively prime to $(1-\xi)$ for all $1 \neq \xi \in \mu$, and such that $N(\mathfrak{b})$ is relatively prime to the order of every torsion element in $K_*(C^*(\mathfrak{a} \rtimes M^*))$ and $K_*(C^*(R \rtimes M^*))$. Then i_* must be already injective after inverting m, so that i_* induces an isomorphism on the torsion parts after inverting m. Since we already know $\mathrm{rk}_{\mathbb{Z}}(K_*(C^*(\mathfrak{a} \rtimes M^*))) = \mathrm{rk}_{\mathbb{Z}}(K_*(C^*(R \rtimes M^*)))$, we are done. □

Remark 4.12. Already in Theorem 4.4, we have to invert m. This seems to be difficult to avoid.

Corollary 4.13. *We have* $\mathrm{rk}(\mathbb{Q} \otimes K_0(C^*_\lambda(R \rtimes M))) = (\#C) \cdot \mathrm{rk}(\mathbb{Q} \otimes K_0(C^*_\lambda(R \rtimes M^*)))$. *In particular,* $\infty > \mathrm{rk}(\mathbb{Q} \otimes K_0(C^*_\lambda(R \rtimes M))) \geq \#C$.

Proof. The first claim follows immediately from the K-theory formula in Theorem 4.1 and Proposition 4.3. The second claim follows from the first once we know that $\infty > \mathrm{rk}(\mathbb{Q} \otimes K_0(C^*_\lambda(R \rtimes M^*))) > 0$. The latter holds because the canonical maps $C^*(M^*) \to C^*(R \rtimes M^*) \to C^*(M^*)$ compose to the identity, so that $K_0(C^*(M^*)) \to K_0(C^*(R \rtimes M^*))$ is injective, and $K_0(C^*(M^*))$ is always free abelian of finite (but strictly positive) rank. This shows $\mathrm{rk}(\mathbb{Q} \otimes K_0(C^*_\lambda(R \rtimes M^*))) > 0$. Moreover, we have $\mathrm{rk}(\mathbb{Q} \otimes K_0(C^*_\lambda(R \rtimes M^*))) < \infty$ because of Theorem 4.4 and the Pimsner-Voiculescu exact sequence. □

4.1.3. *The case of real quadratic fields and totally positive elements.* Now consider a real quadratic field K with ring of algebraic integers R. Suppose $K = \mathbb{Q}(\sqrt{d}) \subseteq \mathbb{R}$ where $d > 1$ is a square-free natural number. Let $\mathfrak{m} = \mathfrak{m}_\infty$ be given by all infinite places of K, i.e., the real embeddings determined by $\sqrt{d} \mapsto \sqrt{d}$ and $\sqrt{d} \mapsto -\sqrt{d}$. Let $\Gamma \subseteq (R/\mathfrak{m})^*$ be the trivial subgroup. Then the congruence monoid $M = R_{\mathfrak{m},\Gamma}$ is given by $R^\times_+$, the set of (non-zero) totally positive elements in R. Our goal is to explicitly compute K-theory for $C^*_\lambda(R \rtimes R^\times_+)$.

The following result is a special case of the analysis from [19], but we give a slightly different presentation here. Let ϵ be the generator of R^*_+ with $\epsilon > 1$. Then $\epsilon = \frac{t+u\sqrt{D}}{2}$ where D is the discriminant of R and (t,u) is the smallest positive solution to the Pell equation $x^2 - Dy^2 = 4$ (see [38, Chapter I, § 7, Exercise 1].)

Let $\mathfrak{a}$ be a fractional ideal of K, and denote by β_ϵ the automorphism of $C^*(\mathfrak{a})$ determined by $\beta_\epsilon(u_x) = u_{\epsilon x}$ where u_x denotes the unitary in $C^*(\mathfrak{a})$ corresponding to $x \in \mathfrak{a}$.

Proposition 4.14. *The induction map*

$$\mathrm{ind}\,_{\mathfrak{a}}^{\mathfrak{a} \rtimes \langle \epsilon \rangle} : K_0(C^*(\mathfrak{a})) \to K_0(C^*(\mathfrak{a} \rtimes \langle \epsilon \rangle))$$

is an isomorphism of K_0-groups, and there is an isomorphism

$$K_1(C^*(\mathfrak{a} \rtimes \langle \epsilon \rangle)) \cong K_0(C^*(\mathfrak{a})) \oplus \mathfrak{a}/(1-\epsilon)\mathfrak{a}$$

of abelian groups. Indeed, the following sequence is exact:

$$0 \longrightarrow K_1(C^*(\mathfrak{a})) \overset{\mathrm{id}-(\beta_\epsilon)_*}{\longrightarrow} K_1(C^*(\mathfrak{a})) \overset{\mathrm{ind}_{\mathfrak{a}}^{\mathfrak{a}\rtimes\langle\epsilon\rangle}}{\longrightarrow} K_1(C^*(\mathfrak{a}\rtimes\langle\epsilon\rangle)) \overset{\partial}{\longrightarrow} K_0(C^*(\mathfrak{a})) \longrightarrow 0$$

where ∂ is the boundary map from the Pimsner-Voiculescu exact sequence for $\beta_\epsilon : \mathbb{Z} \curvearrowright C^*(\mathfrak{a})$.

Proof. Let w_1, w_2 be a $\mathbb{Z}$-basis for $\mathfrak{a}$. Then $K_1(C^*(\mathfrak{a})) \cong \mathbb{Z}^2$ has a $\mathbb{Z}$-basis given by $\{[u_{w_1}]_1, [u_{w_2}]_1\}$, and $K_0(C^*(\mathfrak{a})) \cong \mathbb{Z}^2$ has a $\mathbb{Z}$-basis given by $\{[1]_0, [u_{w_1}]_1 \times [u_{w_2}]_1\}$, were "$\times$" denotes the product in K-theory (see [18, Chapter 4.7]). Let $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ be the matrix for β_ϵ with respect to the basis w_1, w_2. Then $(\beta_\epsilon)_*$ is simply given by applying the matrix γ on K_1, and is trivial on K_0 since $(\beta_w)_*([1]_0) = [1]_0$, and $(\beta_\epsilon)_*([u_{w_1}]_1 \times [u_{w_2}]_1) = \det(\gamma)([u_{w_1}]_1 \times [u_{w_2}]_1) = [u_{w_1}]_1 \times [u_{w_2}]_1$. Now, $\mathrm{trace}(\gamma) = t$, and $t^2 = 4 + Du^2$ with $t, u > 0$, so we must have $t > 2$. Since $\det(\mathrm{id} - \gamma) = 2 - \mathrm{trace}(\gamma)$ is non-zero, we see that $\mathrm{id} - (\beta_\epsilon)_*$ is injective on $K_1(C^*(\mathfrak{a}))$, so the Pimsner-Voiculescu exact sequence implies the results after noting that $K_1(C^*(\mathfrak{a}))/\mathrm{im}(\mathrm{id} - (\beta_\epsilon)_*) \cong \mathfrak{a}/(1-\epsilon)\mathfrak{a}$ as abelian groups. □

Theorem 4.15. *Let K be a real quadratic field with ring of algebraic integers R. Then*

$$K_0(C^*(R \rtimes R_+^\times)) \cong \mathbb{Z}^{2h_K^+} \quad \text{and} \quad K_1(C^*(R \rtimes R_+^\times)) \cong \mathbb{Z}^{2h_K^+} \oplus (R/(1-\epsilon)R)^{h_K^+}$$

where h_K^+ is the narrow class number of K.

Proof. This follows from Theorem 4.1, Proposition 4.3 and Proposition 4.14. □

Let us present an immediate consequence. Suppose K and K' are real quadratic fields with rings of algebraic integers R and R', and write $K = \mathbb{Q}(\sqrt{d})$ and $K' = \mathbb{Q}(\sqrt{d'})$ where d and d' are (uniquely determined) positive, square-free integers.

Corollary 4.16. *If $K_*(C^*(R \rtimes R_+^\times)) \cong K_*(C^*(R' \rtimes R_+'^\times))$, then $K = K'$. In particular, $K_*(C^*(R \rtimes R_+^\times)) \cong K_*(C^*(R' \rtimes R_+'^\times))$ if and only if $C^*(R \rtimes R_+^\times) \cong C^*(R' \rtimes R_+'^\times)$ if and only if $K = K'$.*

Proof. We have $\#(R/(1-\epsilon)R) = |\det(1-\epsilon)| = \mathrm{trace}(\epsilon) - 2$, so Theorem 4.15 allows us to retrieve $\mathrm{trace}(\epsilon)$ from the K-theory of our semigroup C*-algebra. Now let D and D' be the discriminants of R_K and $R_{K'}$, respectively, and let (t, u) and (t', u') be the minimal positive solutions to the Pell equations $x^2 - Dy^2 = 4$ and $x^2 - D'y^2 = 4$, respectively, so that $\epsilon = \frac{t+u\sqrt{D}}{2}$ and $\epsilon' = \frac{t'+u'\sqrt{D'}}{2}$. The equality $\mathrm{trace}(\epsilon) = \mathrm{trace}(\epsilon')$ means that $t = t'$, which forces $Du^2 = D'u'^2$. Hence, $K = \mathbb{Q}(\sqrt{D}) = \mathbb{Q}(\sqrt{Du^2}) = \mathbb{Q}(\sqrt{D'u'^2}) = \mathbb{Q}(\sqrt{D'}) = K'$. □

Actually, the last equivalence in Corollary 4.16 generalizes to Galois extensions of $\mathbb{Q}$ (see Section 5.1).

4.2. **K-theory for boundary quotients.**

4.2.1. *Duality Theorems.* Let $\mathcal{S} = \mathrm{supp}(\mathfrak{m}_0)$, and set $\boldsymbol{R}_\mathcal{S} = \prod_{v \in \mathcal{S}^c, v\nmid\infty} R_v$, $\mathbb{A}_\mathcal{S} = \prod'_{v \in \mathcal{S}^c, v\nmid\infty} K_v$. Here the restricted product is taken with respect to the subrings $R_v \subseteq K_v$, i.e., almost all coordinates of elements in $\mathbb{A}_\mathcal{S}$ belong to R_v.

Our goal is to prove the following generalization of [12, Theorem 4.1]:

Theorem 4.17. *$C_0(\mathbb{A}_\infty) \rtimes Q$ and $C(\boldsymbol{R}_\mathcal{S}) \rtimes R$ are M-equivariantly Morita equivalent.*

We refer to [31, § 3.4] for the notion of Morita equivalence equivariant under semigroup actions.

Before we explain the proof, let us first record the following consequences:

Corollary 4.18. *The Morita equivalence from Theorem 4.17 induces an M-equivariant Morita equivalence $C_0(\mathbb{A}_\infty) \rtimes Q \rtimes \mu \sim_M C(\mathbb{A}_\mathcal{S}) \rtimes Q \rtimes \mu$, which in turn induces (M-equivariant) isomorphisms*

(4) $K_*(C_0(\mathbb{A}_\infty) \rtimes Q \rtimes \langle M' \rangle) \cong K_*(C(\boldsymbol{R}_\mathcal{S}) \rtimes R \rtimes^e M')$ for every subsemigroup $M' \subseteq M$ with $\mu \subseteq M'$.

Corollary 4.19. *We have $C_0(\mathbb{A}_\infty) \rtimes Q \rtimes G \sim_M C(\mathbb{A}_\mathcal{S}) \rtimes Q \rtimes G$.*

Let us now prove Theorem 4.17. The idea is to apply [31, Proposition 3.30] following the comment immediately after that proposition. The key observation is as follows: Let $\chi = \prod_v \chi_v$ be a character on $\mathbb{A}_K$ inducing identifications $\widehat{\mathbb{A}_K} \cong \mathbb{A}_K$, $\widehat{\mathbb{A}_\infty} \cong \mathbb{A}_\infty$ and $\widehat{K} \cong \mathbb{A}_K/K$ as constructed in Tate's thesis (see [43] and [24, Chapter XIV]). Write $\chi_{\mathcal{S}} = \prod_{v \in \mathcal{S}^c} \chi_v$, so that $\chi_{\mathcal{S}}$ is a character on $\mathbb{A}_\infty \times \mathbb{A}_{\mathcal{S}}$.

Lemma 4.20. *There exists $a \in K^\times$ such that the character $\chi_{\mathcal{S}} \cdot a : \mathbb{A}_\infty \times \mathbb{A}_{\mathcal{S}} \to \mathbb{T}$, $\boldsymbol{x} \mapsto \chi_{\mathcal{S}}(a\boldsymbol{x})$ and the corresponding pairing $(\mathbb{A}_\infty \times \mathbb{A}_{\mathcal{S}}) \times (\mathbb{A}_\infty \times \mathbb{A}_{\mathcal{S}}) \to \mathbb{T}$, $(\boldsymbol{x}, \boldsymbol{y}) \mapsto (\chi_{\mathcal{S}} \cdot a)(\boldsymbol{xy})$ induce identifications $\widehat{\mathbb{A}_\infty} \cong \mathbb{A}_\infty$ and $\widehat{Q} \cong (\mathbb{A}_\infty \times \mathbb{A}_{\mathcal{S}})/Q$.*

Proof. $Q \subseteq \mathbb{A}_\infty \times \mathbb{A}_{\mathcal{S}}$ is cocompact: Choose a compact subset $C_\infty \subseteq \mathbb{A}_\infty$ such that $\mathbb{A}_\infty = C_\infty + R$. Then let $C = C_\infty \times \boldsymbol{R}_{\mathcal{S}}$. Given $\boldsymbol{x} \in \mathbb{A}_\infty \times \mathbb{A}_{\mathcal{S}}$, by Strong Approximation we can find $t \in Q$ such that $\boldsymbol{x} - t \in \mathbb{A}_\infty \times \boldsymbol{R}_{\mathcal{S}}$. Now find $s \in R$ such that $\boldsymbol{x} - t - s \in C$. This shows that $\mathbb{A}_\infty \times \mathbb{A}_{\mathcal{S}} = C + Q$.

Now let $\check{Q} = \{\boldsymbol{x} \in \mathbb{A}_\infty \times \mathbb{A}_{\mathcal{S}} \colon \chi_{\mathcal{S}}(\boldsymbol{x}t) = 1 \text{ for all } t \in Q\}$. Then $\check{Q} \cong ((\mathbb{A}_\infty \times \mathbb{A}_{\mathcal{S}})/Q)\widehat{\ }$ is discrete (as a dual group of a compact group). Moreover, we have $Q \subseteq \check{Q}$ because for every $t \in Q$, we have $\chi_v(t) = 1$ whenever $v \in \mathcal{S}$ as $t \in R_v$, so that $\chi_{\mathcal{S}}(t) = \chi(t) = 1$. Now $\check{Q}/Q \subseteq (\mathbb{A}_\infty \times \mathbb{A}_{\mathcal{S}})/Q$ is compact. Hence, being discrete and compact, $\check{Q}/Q$ must be finite. Thus there exists a positive integer N such that $N \cdot \check{Q} \subseteq Q$, so that $\check{Q} \subseteq N^{-1} \cdot Q \subseteq K$. Let $\mathfrak{C}_v = \{x \in K_v \colon \mathrm{Tr}_v(xy) \in \mathbb{Z}_p \text{ for all } y \in R_v\}$, where $v \mid p$. This is (the local version of) Dedekind's complementary module in the sense of [38, Chapter III, § 2, Definition (2.1)]. Let us now prove that $\check{Q} = \{x \in K \colon x \in \mathfrak{C}_v \text{ for all } v \in \mathcal{S}\}$. Surely, if $x \in K$ satisfies $x \in \mathfrak{C}_v$ for all $v \in \mathcal{S}$, then $\chi_v(x \cdot R_v) = 1$ for all $v \in \mathcal{S}$, so that $\chi_v(x \cdot Q) = \chi_v(x \cdot R_v) = 1$ for all $v \in \mathcal{S}$, and thus $\chi_{\mathcal{S}}(x \cdot Q) = \chi(x \cdot Q) = 1$. This proves "$\supseteq$". For "$\subseteq$", take $x \in \check{Q}$. Then $\chi_{\mathcal{S}}(x \cdot Q) = 1$ and $\chi(x \cdot Q) = 1$. It follows that $(\chi \cdot \chi_{\mathcal{S}}^{-1})(x \cdot Q) = 1$. As Q is dense in $\prod_{v \in \mathcal{S}} R_v$, we conclude that $\chi_v(x \cdot R_v) = 1$ for all $v \in \mathcal{S}$. But this implies that $x \in \mathfrak{C}_v$ for all $v \in \mathcal{S}$ because $\chi_v(x \cdot R_v) = \chi_p(\mathrm{Tr}_v(x \cdot R_v)) = 1$ if and only if $\mathrm{Tr}_v(x \cdot R_v) \subseteq \mathbb{Z}_p$ (where $v \mid p$). This proves "$\subseteq$".

Now choose $a \in K^\times$ such that $a \cdot R_v = \mathfrak{C}_v$ for all $v \in \mathcal{S}$. Here we are using Strong Approximation, and that $\mathcal{S}$ is always finite. Then we have $\chi_{\mathcal{S}}(a\boldsymbol{x}t) = 1$ for all $t \in Q$ if and only if $a\boldsymbol{x} \in \check{Q}$ if and only if $\boldsymbol{x} \in K$ and $a\boldsymbol{x} \in \mathfrak{C}_v = a \cdot R_v$ for all $v \in \mathcal{S}$ if and only if $\boldsymbol{x} \in K$ and $\boldsymbol{x} \in R_v$ for all $v \in \mathcal{S}$ if and only if $\boldsymbol{x} \in Q$. Thus under the pairing induced by $\chi_{\mathcal{S}} \cdot a$, Q is dual to itself, and hence we obtain the desired identification $\widehat{Q} \cong (\mathbb{A}_\infty \times \mathbb{A}_{\mathcal{S}})/Q$. The identification $\widehat{\mathbb{A}_\infty} \cong \mathbb{A}_\infty$ is already given by our choice of χ. □

Proof of Theorem 4.17. Using Lemma 4.20, the proof now proceeds as in [12, § 4]. First, observe that

$$C_0(\mathbb{A}_\infty) \rtimes Q \cong C^*(\mathbb{A}_\infty) \rtimes Q \cong C^*(Q) \rtimes \mathbb{A}_\infty \cong C(\widehat{Q}) \rtimes \mathbb{A}_\infty \cong C((\mathbb{A}_\infty \times \mathbb{A}_{\mathcal{S}})/Q) \rtimes \mathbb{A}_\infty,$$

where we used Lemma 4.20 in the last step. The (inverse of the) canonical multiplicative M-action on $C_0(\mathbb{A}_\infty) \rtimes Q$ corresponds to the M-action $a.[t \mapsto f_t] = [t \mapsto |N(a)|_\infty^{-1} f_{a^{-1}t}(a^{-1}\sqcup)]$ on $C((\mathbb{A}_\infty \times \mathbb{A}_{\mathcal{S}})/Q) \rtimes \mathbb{A}_\infty$. The second step is to prove that $C_c(\mathcal{G}_N)$, equipped with analogous inner products and M-action as in [31], is an M-equivariant pre-imprimitivity bimodule in the sense of [31], which induces an M-equivariant $C((\mathbb{A}_\infty \times \mathbb{A}_{\mathcal{S}})/Q) \rtimes \mathbb{A}_\infty$-$C(\boldsymbol{R}_{\mathcal{S}}) \rtimes R$-imprimitivity bimodule. Here $\mathcal{G}$ is the transformation groupoid $((\mathbb{A}_\infty \times \mathbb{A}_{\mathcal{S}})/Q) \rtimes \mathbb{A}_\infty$ and N is the image of $\{0\} \times \boldsymbol{R}_{\mathcal{S}} \subseteq \mathbb{A}_\infty \times \mathbb{A}_{\mathcal{S}}$ under the canonical projection $\mathbb{A}_\infty \times \mathbb{A}_{\mathcal{S}} \twoheadrightarrow (\mathbb{A}_\infty \times \mathbb{A}_{\mathcal{S}})/Q$. These two steps together yield the desired M-equivariant Morita equivalence $C_0(\mathbb{A}_\infty) \rtimes Q \sim_M C(\boldsymbol{R}_{\mathcal{S}}) \rtimes R$. □

4.2.2. *Rational K-theory computations for boundary quotients.* Using the duality theorem, we now compute the K-theory of the boundary quotient $\partial C_\lambda^*(R \rtimes M) \cong C(\boldsymbol{R}_{\mathcal{S}}) \rtimes R \rtimes^e M$ rationally, under the assumption that

$$\gcd\Big(\prod_{1 \neq \xi \in \mu} (1 - \xi),\ \mathfrak{m}_0 \Big) = (1). \tag{5}$$

Note that the boundary quotient corresponds to the maximal primitive ideal (see § 2.2 for the primitive ideal space computation), and its crossed product description can be derived as in [28, 15] (see [1, § 8]).

Here is the final result of our rational K-theory computation:

Theorem 4.21. *Assume that condition* (5) *holds. Then we have*

$$\begin{aligned} & \mathbb{Q} \otimes K_*(\partial C^*_\lambda(R \rtimes M)) \cong \mathbb{Q} \otimes K_*(C(\boldsymbol{R}_{\mathcal{S}}) \rtimes R \rtimes^e M) \cong \mathbb{Q} \otimes K_*(C_0(\mathbb{A}_{\mathcal{S}}) \rtimes Q \rtimes G) \\ \cong \quad & \mathbb{Q} \otimes K_*(C_0(\mathbb{A}_\infty) \rtimes Q \rtimes G) \cong \mathbb{Q} \otimes K_*(C_0(\mathbb{A}_\infty) \rtimes G), \text{ and} \end{aligned}$$

$$\mathbb{Q} \otimes K_*(C_0(\mathbb{A}_\infty) \rtimes G) \cong \begin{cases} \mathbb{Q} \otimes \bigwedge^*(G) & \text{if } m = 1, \\ \mathbb{Q} \otimes K_0(C^*(\mu)) \otimes \bigwedge^*(G/\mu) & \text{if } n \text{ even}, m > 1, \end{cases}$$

if for every $c \in M$*, the number* $\#\{v_{\mathbb{R}}\colon v_{\mathbb{R}}(c) < 0\}$ *is even, whereas*

$$\mathbb{Q} \otimes K_*(C_0(\mathbb{A}_\infty) \rtimes G) \cong \begin{cases} \{0\} & \text{if } m = 1, \\ \mathbb{Q} \otimes \bigwedge^*(G/\mu) & \text{if } m = 2, \end{cases}$$

if there exists $c \in M$ *with* $\#\{v_{\mathbb{R}}\colon v_{\mathbb{R}}(c) < 0\}$ *odd.*

Note that in all the cases where we get a non-zero answer, we always get $\bigoplus_{\mathbb{N}} \mathbb{Q}$ as abstract vector spaces over $\mathbb{Q}$. Moreover, the exterior algebras are equipped with their canonical gradings in all cases unless n is odd, $m = 1$, and for every $c \in M$, the number $\#\{v_{\mathbb{R}}\colon v_{\mathbb{R}}(c) < 0\}$ is even. In that case, our computations yield an exterior algebra with reversed grading.

Proof. The strategy is the one explained in [12, Remark 3.16], which is also used in [32]. First, using an inductive limit decomposition, compute (rational) K-theory for $C(\boldsymbol{R}_{\mathcal{S}}) \rtimes R \rtimes \mu$. Then, for a convenient choice of $c \in M$, compute (rationally) the multiplicative action of c on $C(\boldsymbol{R}_{\mathcal{S}}) \rtimes R \rtimes \mu$ in K-theory. Next, use this computation together with Theorem 4.17 (or rather (4)) to show that the canonical inclusion $C_0(\mathbb{A}_\infty) \rtimes G \hookrightarrow C_0(\mathbb{A}_\infty) \rtimes Q \rtimes G$ induces a rational isomorphism. Finally, compute (rational) K-theory for $C_0(\mathbb{A}_\infty) \rtimes G$ using a homotopy argument.

In the following, we explain how to carry out each of these steps and summarize the final results. First, as in [32, § 4.2], we find a decomposition $K_0(C^*(R \rtimes \mu)) = K_{\mathrm{inf}} \oplus K^c_{\mathrm{fin}} \oplus K^\mu_{\mathrm{fin}}$ such that $K_0(C(\boldsymbol{R}_{\mathcal{S}}) \rtimes R \rtimes \mu) \cong \varinjlim_M \{K_0(C^*(R \rtimes \mu), \eta_c\}$ and for general $c \in M$ with $\prod_{1 \neq \xi \in \mu}(1 - \xi) \mid c$, $\mathrm{id}_{\mathbb{Q}} \otimes \eta_c$ is of the form

$$\left(\begin{array}{c|c|c} A_c & * & 0 \\ \hline 0 & 0 & 0 \\ \hline 0 & 0 & \mathrm{id} \end{array}\right),$$

whereas for $c \in \mathbb{Z}_{>1}$, $c \in M$ with $\prod_{1 \neq \xi \in \mu}(1 - \xi) \mid c$, $\mathrm{id}_{\mathbb{Q}} \otimes \eta_c$ is of the form

$$\left(\begin{array}{ccc|c|c} c^n & & 0 & & \\ & \ddots & & * & 0 \\ 0 & & c^? & & \\ \hline & 0 & & 0 & 0 \\ \hline & 0 & & 0 & \mathrm{id} \end{array}\right)$$

with respect to the above decomposition of K_0 and suitable bases. Here $A_c : K_{\mathrm{inf}} \to K_{\mathrm{inf}}$ is an isomorphism. Moreover, the exponents of c on the diagonal in the upper left box are non-negative and decreasing, and all the exponents are positive if n is odd, while there is exactly one exponent equal to 0 if n is even.

For K_1, we also have $K_1(C(\boldsymbol{R}_{\mathcal{S}}) \rtimes R \rtimes \mu) \cong \varinjlim_M \{K_1(C^*(R \rtimes \mu), \theta_c\}$. It follows from Theorem 4.4 that K_1 vanishes if m is even. If m is odd, we know that $\mathrm{id}_{\mathbb{Q}} \otimes \theta_c$ is an isomorphism for all $c \in M$, and for $c \in M$ with $c \in \mathbb{Z}_{>1}$, $\mathrm{id}_{\mathbb{Q}} \otimes \theta_c$ is of the form

$$\left(\begin{array}{ccc} c^? & & 0 \\ & \ddots & \\ 0 & & c^? \end{array}\right)$$

with respect to a suitable basis, where again the exponents of c on the diagonal are non-negative and decreasing, and there is exactly one exponent equal to 0 if n is odd, while all the exponents are positive if n is even.

It follows that $\mathbb{Q} \otimes K_0(C(\boldsymbol{R}_{\mathcal{S}}) \rtimes R \rtimes \mu) \cong \mathbb{Q}^{r_0} \oplus \mathbb{Q}^{m-1}$, and with respect to this decomposition, the multiplicative action of $c \in M$ with $c \in \mathbb{Z}_{>1}$ and $\prod_{1 \neq \xi \in \mu}(1-\xi) \mid c$ is given on K_0 by

$$\beta_c^{\mathrm{fin}} = \left(\begin{array}{ccc|c} c^n & & 0 & \\ & \ddots & & 0 \\ 0 & & c^? & \\ \hline & 0 & & \mathrm{id} \end{array}\right).$$

For K_1, we obtain $\mathbb{Q} \otimes K_1(C(\boldsymbol{R}_{\mathcal{S}}) \rtimes R \rtimes \mu) \cong \mathbb{Q}^{r_1}$, and the multiplicative action of $c \in M$ with $c \in \mathbb{Z}_{>1}$ is given on K_1 by

$$\gamma_c^{\mathrm{fin}} = \begin{pmatrix} c^? & & 0 \\ & \ddots & \\ 0 & & c^? \end{pmatrix},$$

the same matrix from above describing $\mathrm{id}_{\mathbb{Q}} \otimes \theta_c$. Hence the subgroup of $\mathbb{Q} \otimes K_*(C(\boldsymbol{R}_{\mathcal{S}}) \rtimes R \rtimes \mu)$ which is left invariant under $(\beta_c^{\mathrm{fin}}, \gamma_c^{\mathrm{fin}})$ is precisely given by a one-dimensional subspace of $\mathbb{Q} \otimes K_1$ (i.e., $\mathbb{Q} \subseteq \mathbb{Q} \otimes K_1$) if n is odd and $m = 1$, a one-dimensional subspace of $\mathbb{Q} \otimes K_0$ (i.e., $\mathbb{Q} \subseteq \mathbb{Q} \otimes K_0$) if n is even and $m = 2$, and an m-dimensional subspace of $\mathbb{Q} \otimes K_0$ (i.e., $\mathbb{Q}^m \subseteq \mathbb{Q} \otimes K_0$) in all other cases.

Because of the equivariant K-theory identification in (4), the same description is valid for the multiplicative action corresponding to our element c on $\mathbb{Q} \otimes K_*(C_0(\mathbb{A}_\infty) \rtimes Q \rtimes \mu)$. Comparing with the computation

$$\mathbb{Q} \otimes K_*(C_0(\mathbb{A}_\infty) \rtimes \mu) \cong \begin{cases} (\{0\}, \mathbb{Q}) & \text{if } n \text{ odd, } m = 1, \\ (\mathbb{Q}, \{0\}) & \text{if } n \text{ odd, } m = 2, \\ (\mathbb{Q}^m, \{0\}) & \text{else,} \end{cases}$$

we see that the canonical inclusion $C_0(\mathbb{A}_\infty) \rtimes \mu \hookrightarrow C_0(\mathbb{A}_\infty) \rtimes Q \rtimes \mu$ induces a rational isomorphism onto the $\langle c \rangle$-invariant part of $\mathbb{Q} \otimes K_*(C_0(\mathbb{A}_\infty) \rtimes Q \rtimes \mu)$. Extending $c \in M$ to a $\mathbb{Z}$-basis $\{c, c_1, c_2, \ldots\}$ of G/μ, an iterative application of the Pimsner-Voiculescu exact sequence yields that the canonical inclusion $C_0(\mathbb{A}_\infty) \rtimes \mu \rtimes \langle c, c_1, \ldots, c_i \rangle \hookrightarrow C_0(\mathbb{A}_\infty) \rtimes Q \rtimes \mu \rtimes \langle c, c_1, \ldots, c_i \rangle$ induces a rational isomorphism in K-theory.

All in all, we obtain

$$\begin{aligned} & \mathbb{Q} \otimes K_*(\partial C_\lambda^*(R \rtimes M)) \cong \mathbb{Q} \otimes K_*(C(\boldsymbol{R}_{\mathcal{S}}) \rtimes R \rtimes^e M) \cong \mathbb{Q} \otimes K_*(C_0(\mathbb{A}_{\mathcal{S}}) \rtimes Q \rtimes G) \\ \cong \quad & \mathbb{Q} \otimes K_*(C_0(\mathbb{A}_\infty) \rtimes Q \rtimes G) \cong \mathbb{Q} \otimes K_*(C_0(\mathbb{A}_\infty) \rtimes G). \end{aligned}$$

We now complete the proof by computing

$$\mathbb{Q} \otimes K_*(C_0(\mathbb{A}_\infty) \rtimes G) \cong \begin{cases} \mathbb{Q} \otimes \bigwedge^*(G) & \text{if } m = 1, \\ \mathbb{Q} \otimes K_0(C^*(\mu)) \otimes \bigwedge^*(G/\mu) & \text{if } n \text{ even, } m > 1, \end{cases}$$

if for every $c \in M$, the number $\#\{v_{\mathbb{R}} \colon v_{\mathbb{R}}(c) < 0\}$ is even, and

$$\mathbb{Q} \otimes K_*(C_0(\mathbb{A}_\infty) \rtimes G) \cong \begin{cases} \{0\} & \text{if } m = 1, \\ \mathbb{Q} \otimes \bigwedge^*(G/\mu) & \text{if } m = 2, \end{cases}$$

if there exists $c \in M$ with $\#\{v_{\mathbb{R}} \colon v_{\mathbb{R}}(c) < 0\}$ odd. □

Let us now present an example showing why we only carry out rational computations.

Example 4.22. *Consider the case $K = \mathbb{Q}$, $\mathfrak{m}_0 = (2)$, $\mathfrak{m}_\infty(\infty) = 1$, and $\Gamma = \{+1\} \times (\mathbb{Z}/(2))^*$. Then $M = \{c \in \mathbb{Z}_{>0} \colon 2 \nmid c\}$, $Q = \{c \in \mathbb{Q}_{>0} \colon v_2(c) \geq 0\}$ and $G = \{c \in \mathbb{Q}_{>0} \colon v_2(c) = 0\}$. A similar computation as in* [8, § 5] *and* [12, § 5.1] *yields*

$$K_\bullet(C(\boldsymbol{R}_{\mathcal{S}}) \rtimes R) \cong \begin{cases} Q & \text{if } \bullet = 0, \\ \mathbb{Z} & \text{if } \bullet = 1. \end{cases}$$

Moreover, for $c = 3$, the multiplicative action corresponding to c is given by $3 \cdot \mathrm{id}_Q$ on K_0 and by id *on K_1. Hence we obtain*

$$K_\bullet(C(\boldsymbol{R}_\mathcal{S}) \rtimes R \rtimes^e [c\rangle) \cong \begin{cases} (\mathbb{Z}/2\mathbb{Z}) \oplus \mathbb{Z} & \text{if } \bullet = 0, \\ \mathbb{Z} & \text{if } \bullet = 1. \end{cases}$$

This example illustrates one of the reasons why we only carry out rational computations: Along the way of our computations, it could happen that torsion appears, which causes complications. Another reason is that the connecting maps in the inductive limit decomposition of $C(\boldsymbol{R}_\mathcal{S}) \rtimes R \rtimes \mu$ are difficult to determine if we do not work over $\mathbb{Q}$.

Remark 4.23. However, it is possible to carry out precise K-theory computations for boundary quotients in some cases. For instance, assume condition (5) holds and that we can find $a, c \in M \cap \mathbb{Z}_{>1}$ such that $c - a = 1$. Then we can compute K-theory without tensoring with $\mathbb{Q}$. The point is that if we can find such elements a and c, then the K-groups will be free abelian, so that they are completely determined by our rational computations.

Here is an example which explains why we need assumption (5).

Example 4.24. *Consider the case $K = \mathbb{Q}$, $\mathfrak{m}_0 = (2)$, $\mathfrak{m}_\infty(\infty) = 0$, and $\Gamma = (\mathbb{Z}/(2))^*$. Then $M = \{c \in \mathbb{Z}^\times \colon 2 \nmid c\}$, $Q = \{c \in \mathbb{Q}^\times \colon v_2(c) \geq 0\}$ and $G = \{c \in \mathbb{Q}^\times \colon v_2(c) = 0\}$. A similar computation as in* [8, § 7] *and* [12, § 3.1] *yields*

$$K_\bullet(C(\boldsymbol{R}_\mathcal{S}) \rtimes R \rtimes \mu) \cong \begin{cases} Q \oplus \mathbb{Z} \oplus \mathbb{Z} & \text{if } \bullet = 0, \\ \{0\} & \text{if } \bullet = 1. \end{cases}$$

Moreover, for $c = 3$, the multiplicative action corresponding to c is given by the matrix

$$\begin{pmatrix} 3 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Plugging this into the Pimsner-Voiculescu exact sequence, we obtain

$$K_\bullet(C(\boldsymbol{R}_\mathcal{S}) \rtimes R \rtimes^e [c\rangle) \cong \mathbb{Z} \oplus \mathbb{Z}$$

for $\bullet = 0, 1$. At the same time, we have $\mathbb{A}_\infty = \mathbb{R}$ and $K_0(C_0(\mathbb{R}) \rtimes \mu) \cong \mathbb{Z}$ and $K_1(C_0(\mathbb{R}) \rtimes \mu) \cong \{0\}$. This shows that the canonical embedding $C_0(\mathbb{R}) \rtimes \mu \hookrightarrow C_0(\mathbb{R}) \rtimes Q \rtimes \mu$ does not induce a rational isomorphism onto the part fixed by the multiplicative $\langle c\rangle$-action. This also shows that for any c' such that $\{c, c'\}$ can be extended to a $\mathbb{Z}$-basis of G/μ, the canonical embedding $C_0(\mathbb{R}) \rtimes \mu \rtimes \langle c, c'\rangle \hookrightarrow C_0(\mathbb{R}) \rtimes Q \rtimes \mu \rtimes \langle c, c'\rangle$ does not induce a rational isomorphism in K-theory.

This example shows why we need condition (5)*. Otherwise we cannot compute (rational) K-theory of the boundary quotient by computing (rational) K-theory of $C_0(\mathbb{A}_\infty) \rtimes G$.*

Remark 4.25. As remarked in [11, § 5.11], it is an intriguing phenomenon that for cancellative semigroups, the left and right semigroup C*-algebras often have isomorphic K-theory. Actually, we do not know of an example where this does not happen because this phenomenon appears in all cases where we can compute K-theory. However, in general left and right semigroup C*-algebras have very different structural properties as C*-algebras (see [11, § 5.11]). In the following, we give examples where the left and right boundary quotients have different K-theories:

Let K be a number field with $r > 0$ real embeddings, choose $\mathfrak{m}_\infty$ and Λ so that $\mu = \{+1\}$, further choose $\mathfrak{m}_0$ such that there exists $c \in M$ with $\#\{v_\mathbb{R} \colon v_\mathbb{R}(c) < 0\}$ odd. Note that condition (5) is vacuous because μ is trivial. Now Theorem 4.21 implies that we have

$$\mathbb{Q} \otimes K_*(\partial C^*_\lambda(R \rtimes M)) \cong \{0\}.$$

However, for the right boundary quotient, we get $\partial C^*_\rho(R \rtimes M) \cong C^*(Q \rtimes G)$, and hence a straightforward computation shows that

$$\mathbb{Q} \otimes K_*(\partial C^*_\rho(R \rtimes M)) \cong \mathbb{Q} \otimes K_*(C^*(Q \rtimes G)) \cong \mathbb{Q} \otimes K_*(C^*(G)) \cong \mathbb{Q} \otimes (\bigwedge\nolimits^* G) \cong \bigoplus_{\mathbb{N}} \mathbb{Q}.$$

In particular,

$$K_*(\partial C^*_\lambda(R \rtimes M)) \ncong K_*(\partial C^*_\rho(R \rtimes M)).$$

Here is a concrete example: Let $K = \mathbb{Q}[\sqrt{2}]$, so that $R = \mathbb{Z}[\sqrt{2}]$. Let v_+ and v_- be the real embeddings of K determined by $v_\pm(\sqrt{2}) = \pm\sqrt{2}$. Set $\mathfrak{m}_\infty(v_+) = 0$ and $\mathfrak{m}_\infty(v_-) = 1$. Let $\Gamma = \{+1\}$ be trivial. Then $\mu = \{+1\}$ is trivial. Let $\mathfrak{m}_0 = R$ be trivial. Then $c = 1 - \sqrt{2}$ lies in M; it satisfies $\#\{v_\mathbb{R}\colon\ v_\mathbb{R}(c) < 0\} = \#\{v_+\} = 1$.

5. Reconstruction theorems

5.1. **Reconstruction using semigroup C*-algebras.** As discussed in § 2.2, the non-zero minimal primitive ideals of $C^*_\lambda(R \rtimes M)$ correspond bijectively to the primes in $\mathcal{P}^\mathfrak{m}_K$. For each $\mathfrak{p} \in \mathcal{P}^\mathfrak{m}_K$, we shall denote by $I_\mathfrak{p}$ the minimal primitive ideal corresponding to $\mathfrak{p}$.

It is straightforward to carry over the proof of [28, Proposition 4.8] to our more general situation, so that we obtain the following result.

Proposition 5.1 (generalized version of [28, Proposition 4.8])**.** *For every $\mathfrak{p} \in \mathcal{P}^\mathfrak{m}_K$ such that the canonical map $M^* \to (R/\mathfrak{p})^*$ is injective on μ, the K_0-class $[1_{C^*_\lambda(R\rtimes M)/I_\mathfrak{p}}]$ of the unit in $C^*_\lambda(R \rtimes M)/I_\mathfrak{p}$ is a torsion element of order $\frac{N(\mathfrak{p})^{f(\mathfrak{p})}-1}{m}$.*

Let $p_{\max} := \{p \in \mathbb{Z}_{>0} \text{ prime } : p \mid N(1-\zeta^i) \text{ for some } 1 \le i \le m-1\}$. For a prime $p \in \mathbb{Z}_{>0}$, let $g_K(p) = \{\mathfrak{p} \in \mathcal{P}_K : \mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}\}$ be the splitting number of p in K. We collect the following consequences of Proposition 5.1.

Corollary 5.2.

(i) *For every prime $p \in \mathbb{Z}_{>0}$ with $\frac{p-1}{m} > p_{\max}^{n\cdot\#C} - 1$, we have*

$$g_K(p) = \#\{I \in \mathrm{Prim}_{\min}(C^*_\lambda(R \rtimes M)) : p \mid (m \cdot \mathrm{ord}([1_{C^*_\lambda(R\rtimes M)/I}]) + 1)\}$$

where $\mathrm{Prim}_{\min}(C^*_\lambda(R \rtimes M))$ denotes the set of non-zero minimal primitive ideals of $C^*_\lambda(R \rtimes M)$.

(ii) *We have the following formula for the degree of K:*

$$[K : \mathbb{Q}] = \limsup_{T\to\infty} \#\{I \in \mathrm{Prim}_{\min}(C^*_\lambda(R \rtimes M)) : \mathrm{ord}(C^*_\lambda(R \rtimes M)/I) = T\}.$$

Proof. (i) and (ii) are generalized versions of [28, Lemma 4.9] and [28, Lemma 5.1], respectively, and the proofs in [28] carry over. □

Let K, R, $\mathfrak{m}$, μ, and Γ, M be as above. Let $\mathfrak{X} := \mathrm{Prim}_{\min}$ be the set of minimal non-zero primitive ideals of $C^*_\lambda(R \rtimes M)$. Define a function o on $\mathfrak{X}$ by setting $o(I) := \mathrm{ord}(1_{C^*_r(R\rtimes M)/I})$. Let $n = [K : \mathbb{Q}]$. Let $\mathrm{rk} = \mathrm{rk}(\mathbb{Q} \otimes K_0(C^*_\lambda(R \rtimes M)))$ and set $e := n + \mathrm{rk}$. Let $\mathcal{P}$ denote the set of prime numbers (i.e., $\mathcal{P} = \mathcal{P}_\mathbb{Q}$).

The following allows us to read off the number of roots of unity:

Theorem 5.3. *$m = \#\mu$ is the unique positive integer m for which there exist functions $\mathfrak{X} \to \mathcal{P}$, $I \mapsto p_I$ and $\mathfrak{X} \to \{1, \dots, e\}$, $I \mapsto i_I$ such that $I \mapsto p_I$ is finite-to-one and $\mathcal{P} \setminus \{p_I\colon\ I \in \mathfrak{X}\}$ is finite, and we have*

$$m \cdot o(I) + 1 = p_I^{i_I} \text{ for almost all } I \in \mathfrak{X}.$$

Proof. It follows immediately from Proposition 5.1 and Corollary 4.13 that m has the desired properties. Note that Corollary 4.13 ensures that the codomain of i is finite.

All we have to do is to prove uniqueness. Suppose m' is another positive integer with $m \ne m'$ for which we can also find functions $\mathfrak{X} \to \mathcal{P}$, $I \mapsto q_I$ and $\mathfrak{X} \to \{1, \dots, e\}$, $I \mapsto j_I$ with the above properties. Then

we have for almost all $I \in \mathfrak{X}$:

$$\frac{p_I^{i_I}-1}{m} = \frac{q_I^{j_I}-1}{m'} \;\Rightarrow\; m'p_I^{i_I} = mq_I^{j_I} + (m'-m). \tag{6}$$

For every $j \in \{1,\dots,e\}$, consider $f_j(q) = mq^j + (m'-m)$ as a polynomial in q. For every non-constant polynomial f with integer coefficients, there exist infinitely many primes p for which there exists $z \in \mathbb{Z}$ such that $f(z) \equiv 0 \pmod{p}$ (see for instance [37, Chapter III, Theorem 45]). Thus there exist pairwise distinct primes p_j, $1 \le j \le e$, and integers z_j, $1 \le j \le e$, such that, for all $1 \le j \le e$, $p_j \nmid m'$, $p_j \nmid m$, $p_j \nmid (m'-m)$, and $f_j(z_j) \equiv 0 \pmod{p_j}$. In particular, we must have $p_j \nmid z_j$ for all $1 \le j \le e$. Here we used that $m \neq m'$, so that $m' - m \neq 0$.

Now set $N := p_1 \cdots p_e$ and find $z \in \mathbb{Z}$ with $z \equiv z_j \pmod{p_j}$ for all $1 \le j \le e$. Such z exists by the Chinese Remainder Theorem. As $\gcd(z_j, p_j) = 1$ for all $1 \le j \le e$, we must have $\gcd(z, N) = 1$. Hence Dirichlet's Prime Number Theorem (see for instance [38, Chapter VII, (5.14)]) implies that $\mathcal{Q} := \{q \in \mathcal{P}\colon q \equiv z \pmod{N}\}$ is infinite. As $\{q_I\colon I \in \mathfrak{X}\}$ contains almost all primes, $\{I \in \mathfrak{X}\colon q_I \in \mathcal{Q}\}$ must be infinite. By (6), we have

$$m'p_I^{i_I} = mq_I^{j_I} + (m'-m) \equiv 0 \pmod{p_{j_I}}$$

for almost all $I \in \mathfrak{X}$ with $q_I \in \mathcal{Q}$. As $p_{j_I} \nmid m'$, this implies $p_{j_I} \mid p_I^{i_I}$ and hence $p_I = p_{j_I}$ for almost all $I \in \mathfrak{X}$ with $q_I \in \mathcal{Q}$. But $\{I \in \mathfrak{X}\colon q_I \in \mathcal{Q}\}$ is infinite whereas $\{p_{j_I}\colon I \in \mathfrak{X}_{\mathcal{Q}}\} \subseteq \{p_j\colon 1 \le j \le e\}$ is finite, while $I \mapsto p_I$ is finite-to-one. This is a contradiction. □

Corollary 5.4. *Let L be a another number field with ring of algebraic integers S, and data $\mathfrak{n}$, Λ as above giving rise to the congruence monoid N. Let ν be the set of roots of unity in N. If $C_\lambda^*(R \rtimes M) \cong C_\lambda^*(S \rtimes N)$, then we must have $\#\mu = \#\nu$.*

This answers the open question from [28] whether it is possible to read off the number of roots of unity from our semigroup C*-algebras in the affirmative.

Our next result shows that we can recover both the Dedekind zeta function of K and the Kronecker set of $\mathbb{K}$ from K-theoretic invariants of $C_\lambda^*(R \rtimes M)$ (see [40] for the definition of arithmetic equivalence and its formulation in terms of Dedekind zeta functions and [20] for the definition of Kronecker equivalence). Under some additional assumptions on the number-theoretic input for our construction, this allows us to recover information about the congruence monoid M, the class field $\mathbb{K}$, and the class group C.

Theorem 5.5. *Suppose that K and L are number fields with rings of algebraic integers R and S. Let $\mathfrak{m}$ and $\mathfrak{n}$ be moduli for K and L, and let Γ and Λ be subgroups of $(R/\mathfrak{m})^*$ and $(S/\mathfrak{n})^*$, respectively. Suppose that there is an isomorphism $C_\lambda^*(R \rtimes R_{\mathfrak{m},\Gamma}) \cong C_\lambda^*(S \rtimes S_{\mathfrak{n},\Lambda})$. Then*

(i) *K and L are arithmetically equivalent, and $K(\mathfrak{m})^{\bar\Gamma}$ and $L(\mathfrak{n})^{\bar\Lambda}$ are Kronecker equivalent;*
(ii) *if the class fields $K(\mathfrak{m})^{\bar\Gamma}$ and $L(\mathfrak{n})^{\bar\Lambda}$ of K and L are both Galois over $\mathbb{Q}$, then $\#\mathrm{Cl}_{\mathfrak{m}}^{\bar\Gamma} = \#\mathrm{Cl}_{\mathfrak{n}}^{\bar\Lambda}$;*
(iii) *if K or L is Galois, then $K = L$; in particular, K is Galois if and only if L is Galois;*
(iv) *if K or L is Galois and both the class fields $K(\mathfrak{m})^{\bar\Gamma}$ and $L(\mathfrak{n})^{\bar\Lambda}$ are Galois over $\mathbb{Q}$, then*
  (a) *$K = L$;*
  (b) *$K(\mathfrak{m})^{\bar\Gamma} = L(\mathfrak{n})^{\bar\Lambda}$ (in any algebraically closed field containing both $K(\mathfrak{m})^{\bar\Gamma}$ and $L(\mathfrak{n})^{\bar\Lambda}$);*
  (c) *$R^* \cdot (R_{\mathfrak{n}} \cap R_{\mathfrak{m},\Gamma}) = S^* \cdot (S_{\mathfrak{m}} \cap S_{\mathfrak{n},\Lambda})$;*
  (d) *$\mathrm{Cl}_{\mathfrak{m}}^{\bar\Gamma} \cong \mathrm{Cl}_{\mathfrak{n}}^{\bar\Lambda}$ (as abelian groups).*

Here (and throughout our paper) we consider arithmetic equivalence and Kronecker equivalence over $\mathbb{Q}$.

Proof. (i): By Corollary 5.4, $R_{\mathfrak{m},\Gamma}$ and $S_{\mathfrak{n},\Lambda}$ have the same number of roots of unity. Hence, combining Proposition 5.1 and Corollary 5.2(i), we see that $g_K(p) = g_L(p)$ for all but finitely many primes. Therefore, K and L are arithmetically equivalent by [41, Main Theorem].

Now let $\mathbb{K} = K(\mathfrak{m})^{\bar\Gamma}$ and $C = \mathrm{Cl}_{\mathfrak{m}}^{\bar\Gamma}$. To show our claim about Kronecker equivalence, we need to show that we can recover, up to finitely many exceptions, the Kronecker set

$$D(\mathbb{K}|\mathbb{Q}) := \{p \in \mathcal{P}_{\mathbb{Q}} : \exists \mathfrak{P} \in \mathcal{P}_{\mathbb{K}} \text{ such that } \mathfrak{P} \mid p \text{ and } f_{\mathbb{K}/\mathbb{Q}}(\mathfrak{P}|p) = 1\}$$

from K-theoretic invariants of $C^*_\lambda(R \rtimes R_{\mathfrak{m},\Gamma})$. By Corollary 5.4, we can read off the number of roots of unity in $R_{\mathfrak{m},\Gamma}$, so it follows from Proposition 5.1 that we can recover the set $\{N(\mathfrak{p})^{f(\mathfrak{p})} : \mathfrak{p} \in \mathcal{P}_K^{\mathfrak{m}}\}$ up to finitely many exceptions. Thus, we will be done if we show that $D(\mathbb{K}|\mathbb{Q})$ and $\mathcal{P}_\mathbb{Q} \cap \{N(\mathfrak{p})^{f(\mathfrak{p})} : \mathfrak{p} \in \mathcal{P}_K^{\mathfrak{m}}\}$ differ by only finitely many elements. Our proof of this fact is inspired by [16, Proof of Main Theorem (II)]. Let $\mathcal{R} := \mathcal{P}_\mathbb{Q} \setminus \{p \in \mathcal{P}_\mathbb{Q} : p \notin \mathfrak{p} \text{ for all } \mathfrak{p} \in \operatorname{supp}(\mathfrak{m}_0)\}$. Then $\mathcal{R}$ is finite, and every rational prime $p \in \mathcal{R}$ is unramified in $\mathbb{K}$ by Lemma 2.4. We will show that $D(\mathbb{K}|\mathbb{Q}) \setminus \mathcal{R} = \mathcal{P}_\mathbb{Q} \cap \{N(\mathfrak{p})^{f(\mathfrak{p})} : \mathfrak{p} \in \mathcal{P}_K^{\mathfrak{m}}\} \setminus \mathcal{R}$.

"$\subseteq$": Suppose $p \in D(\mathbb{K}|\mathbb{Q}) \setminus \mathcal{R}$. Since $N(\mathfrak{p}) = p^{f_{K/\mathbb{Q}}(\mathfrak{p}|p)}$, we need to show that $f(\mathfrak{p}) = 1 = f_{K/\mathbb{Q}}(\mathfrak{p}|p)$. Choose any prime $\mathfrak{P} \in \mathcal{P}_\mathbb{K}$ such that $\mathfrak{P} \mid p$ and $f_{\mathbb{K}/\mathbb{Q}}(\mathfrak{P}|p) = 1$, and let $\mathfrak{p} := \mathfrak{P} \cap R$. Then $\mathfrak{p} \in \mathcal{P}_K^{\mathfrak{m}}$, and $\mathfrak{p}$ lies over p. Since $f_{\mathbb{K}/\mathbb{Q}}(\mathfrak{P}|p) = f_{\mathbb{K}/K}(\mathfrak{P}|\mathfrak{p}) f_{K/\mathbb{Q}}(\mathfrak{p}|p)$, we see that $f_{\mathbb{K}/K}(\mathfrak{P}|\mathfrak{p}) = f_{K/\mathbb{Q}}(\mathfrak{p}|p) = 1$. Since $\mathfrak{p} \in \mathcal{P}_K^{\mathfrak{m}}$, $\mathfrak{p}$ is unramified in $\mathbb{K}$ by Lemma 2.4. Thus, $f(\mathfrak{p}) = f_{\mathbb{K}/\mathbb{Q}}(\mathfrak{P}|\mathfrak{p}) = 1$ (see the proof of Lemma 2.4).

"$\supseteq$": Now let $p \in \mathcal{P}_\mathbb{Q} \cap \{N(\mathfrak{p})^{f(\mathfrak{p})} : \mathfrak{p} \in \mathcal{P}_K^{\mathfrak{m}}\} \setminus \mathcal{R}$. Then there exists $\mathfrak{p} \in \mathcal{P}_K^{\mathfrak{m}}$ lying over p with $f_{K/\mathbb{Q}}(\mathfrak{p}|p) = f(\mathfrak{p}) = 1$. Since $\mathfrak{p} \in \mathcal{P}_K^{\mathfrak{m}}$, $\mathfrak{p}$ is also unramified in $\mathbb{K}$, so $f(\mathfrak{p}) = f_{\mathbb{K}/K}(\mathfrak{p})$. Now we have, for any prime $\mathfrak{P}$ of $\mathbb{K}$ lying over $\mathfrak{p}$, that $f_{\mathbb{K}/\mathbb{Q}}(\mathfrak{P}|p) = f_{\mathbb{K}/K}(\mathfrak{P}|\mathfrak{p}) f_{K/\mathbb{Q}}(\mathfrak{p}|p) = f_{\mathbb{K}/K}(\mathfrak{p}) f_{K/\mathbb{Q}}(\mathfrak{p}|p) = 1$.

(ii): By part (i), we can recover the set $D(\mathbb{K}|\mathbb{Q})$, at least up to finitely many exceptions, from $C^*_\lambda(R \rtimes R_{\mathfrak{m},\Gamma})$. An application of the Chebotarev density theorem ([38, Chapter VII, (13.4) Theorem]) shows that $D(\mathbb{K}|\mathbb{Q})$ has a Dirichlet density $\delta(D(\mathbb{K}|\mathbb{Q}))$ (see, for instance, [38, Chapter VII, Definition 13.1]) for the definition). Since $\mathbb{K}$ is Galois over $\mathbb{Q}$, this Dirichlet density is given by $\delta(D(\mathbb{K}|\mathbb{Q})) = \frac{1}{[K:\mathbb{Q}] \cdot \#C}$ (see [20, § 3, equation 3.1]). By Corollary 5.2(ii), we can read off $[K : \mathbb{Q}]$ from K-theoretic invariants associated with $C^*_\lambda(R \rtimes R_{\mathfrak{m},\Gamma})$, so we can extract $\#C$.

(iii): By part (i), K and L are arithmetically equivalent, so K and L have the same Galois closure and degree by [40, Theorem 1]. Hence, if K or L is Galois, so that it equals its Galois closure, then $K = L$.

(iv): By part (iii), $K = L$, and by part (ii), the fields $K(\mathfrak{m})^{\bar{\Gamma}}$ and $K(\mathfrak{n})^{\bar{\Lambda}}$ are Kronecker equivalent. Since $K(\mathfrak{m})^{\bar{\Gamma}}$ and $K(\mathfrak{n})^{\bar{\Lambda}}$ are Galois over $\mathbb{Q}$, a rational prime p lies in the Kronecker set $D(K(\mathfrak{m})^{\bar{\Gamma}}|\mathbb{Q})$ if and only if p splits completely in $K(\mathfrak{m})^{\bar{\Gamma}}$, and similarly for $K(\mathfrak{n})^{\bar{\Lambda}}$. This implies that a rational prime p splits completely in $K(\mathfrak{m})^{\bar{\Gamma}}$ if and only if it splits completely $K(\mathfrak{n})^{\bar{\Lambda}}$. Therefore, $K(\mathfrak{m})^{\bar{\Gamma}} = K(\mathfrak{n})^{\bar{\Lambda}}$ in $\overline{\mathbb{Q}}$ by [35, Chapter V, Theorem 3.25]. Now $R^* \cdot (R_\mathfrak{n} \cap R_{\mathfrak{m},\Gamma}) = R^* \cdot (R_\mathfrak{m} \cap R_{\mathfrak{n},\Lambda})$ by Proposition 2.2, and we have $\mathrm{Cl}_\mathfrak{m}^{\bar{\Gamma}} \cong \mathrm{Gal}(K(\mathfrak{m})^{\bar{\Gamma}}/K) = \mathrm{Gal}(K(\mathfrak{n})^{\bar{\Lambda}}/K) \cong \mathrm{Cl}_\mathfrak{n}^{\bar{\Lambda}}$. □

Remark 5.6. A necessary and sufficient condition for $\mathbb{K}$ to be Galois over $\mathbb{Q}$ is given in Corollary 2.8.

In light of Theorem 5.5(iv), a natural question would be whether the existence of an isomorphism $C^*_\lambda(R \rtimes R_{\mathfrak{m},\Gamma}) \cong C^*_\lambda(R \rtimes R_{\mathfrak{n},\Lambda})$ implies that $\operatorname{supp}(\mathfrak{m}_0) = \operatorname{supp}(\mathfrak{n}_0)$. The following partial answer is an immediate consequence of Proposition 5.1.

Lemma 5.7. *Assume that $\mu_{\mathfrak{m},\Gamma}$ reduces injectively modulo $\mathfrak{p}$ for all $\mathfrak{p} \notin \operatorname{supp}(\mathfrak{m}_0)$ and that $\mu_{\mathfrak{n},\Lambda}$ reduces injectively modulo $\mathfrak{p}$ for every $\mathfrak{p} \notin \operatorname{supp}(\mathfrak{n}_0)$. Also assume that for every rational prime p, $\mathfrak{m}_0$ is either divisible by every prime of K over $\mathfrak{p}$ or no primes of K over $\mathfrak{p}$, and similarly for $\mathfrak{n}_0$. If there is an isomorphism $C^*_\lambda(R \rtimes R_{\mathfrak{m},\Gamma}) \cong C^*_\lambda(R \rtimes R_{\mathfrak{n},\Lambda})$, then $\operatorname{supp}(\mathfrak{m}_0) = \operatorname{supp}(\mathfrak{n}_0)$.*

Remark 5.8. The hypothesis of Lemma 5.7 is satisfied, for example, if K is Galois, and $\sigma(\mathfrak{m}_0) = \mathfrak{m}_0$, $\sigma(\mathfrak{n}_0) = \mathfrak{n}_0$ for all $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, which is related to $\mathbb{K}$ being Galois over $\mathbb{Q}$ (cf. Corollary 2.8).

For the case $K = \mathbb{Q}$, the above results can be strengthened. Indeed, we have the following result.

Theorem 5.9. *Let $\mathfrak{m}$ and $\mathfrak{n}$ be moduli for $\mathbb{Q}$, and let Γ and Λ be subgroups of $(\mathbb{Z}/\mathfrak{m})^*$ and $(\mathbb{Z}/\mathfrak{n})^*$, respectively. If there is an isomorphism $C^*_\lambda(\mathbb{Z} \rtimes \mathbb{Z}_{\mathfrak{m},\Gamma}) \cong C^*_\lambda(\mathbb{Z} \rtimes \mathbb{Z}_{\mathfrak{n},\Lambda})$, then*

(i) $\mathbb{Q}(\mathfrak{m})^{\bar{\Gamma}} = \mathbb{Q}(\mathfrak{n})^{\bar{\Lambda}}$ *(equality in $\overline{\mathbb{Q}}$) and* $\mathrm{Cl}_\mathfrak{m}^{\bar{\Gamma}} \cong \mathrm{Cl}_\mathfrak{n}^{\bar{\Lambda}}$*;*

(ii) *if $-1 \notin \mathbb{Z}_{\mathfrak{m},\Gamma}$, then $-1 \notin \mathbb{Z}_{\mathfrak{n},\Lambda}$, $\langle \pm 1 \rangle \cdot \mathbb{Z}_{\mathfrak{m},\Gamma} = \langle \pm 1 \rangle \cdot \mathbb{Z}_{\mathfrak{n},\Lambda}$, and $\mathbb{Z}_{\mathfrak{m},\Gamma} \subseteq \mathbb{Z}_{>0}$ if and only if $\mathbb{Z}_{\mathfrak{n},\Lambda} \subseteq \mathbb{Z}_{>0}$.*

(iii) *if* $-1 \in \mathbb{Z}_{\mathfrak{m},\Gamma}$*, then* $-1 \in \mathbb{Z}_{\mathfrak{n},\Lambda}$ *and*
- $\mathbb{Z}_{\mathfrak{m},\Gamma} = \mathbb{Z}_{\mathfrak{n},\Lambda}$ *provided that either* $2 \mid \mathfrak{m}_0$ *and* $2 \mid \mathfrak{n}_0$*, or* $2 \nmid \mathfrak{m}_0$ *and* $2 \nmid \mathfrak{n}_0$*;*
- $\{a \in \mathbb{Z}_{\mathfrak{m},\Gamma} : \gcd(a, 2q) = 1\} = \{a \in \mathbb{Z}_{\mathfrak{n},\Lambda} : \gcd(a, 2q) = 1\}$ *for some odd prime* q *if* 2 *divides exactly one of* $\mathfrak{m}_0$ *and* $\mathfrak{n}_0$*.*

Proof. (i): This follows immediately from Theorem 5.5(iv) since $\mathbb{Q}(\mathfrak{m})^{\bar{\Gamma}}$ and $\mathbb{Q}(\mathfrak{n})^{\bar{\Lambda}}$ are Galois over $\mathbb{Q}$.

(ii): If $-1 \notin \mathbb{Z}_{\mathfrak{m},\Gamma}$, then it follows from Corollary 5.4 that $-1 \notin \mathbb{Z}_{\mathfrak{n},\Lambda}$ (another way to see this is to note that $K_1(C^*_\lambda(\mathbb{Z} \rtimes \mathbb{Z}_{\mathfrak{m},\Gamma}))$ vanishes if and only if $-1 \in \mathbb{Z}_{\mathfrak{m},\Gamma}$, and similarly for $\mathbb{Z}_{\mathfrak{n},\Lambda}$, see § 4.1.1).

Since $-1 \notin \mathbb{Z}_{\mathfrak{m},\Gamma} \cup \mathbb{Z}_{\mathfrak{n},\Lambda}$, Lemma 5.7 implies that $\mathrm{supp}(\mathfrak{m}_0) = \mathrm{supp}(\mathfrak{n}_0)$. Hence, Theorem 5.5(iv) implies that $\langle \pm 1 \rangle \mathbb{Z}_{\mathfrak{m},\Gamma} = \langle \pm 1 \rangle \mathbb{Z}_{\mathfrak{n},\Lambda}$.

Now Theorem 4.21 implies that $\mathbb{Q} \otimes K_*(\partial C^*_\lambda(\mathbb{Z} \rtimes \mathbb{Z}_{\mathfrak{m},\Gamma})) \neq \{0\}$ if and only if $\mathbb{Z}_{\mathfrak{m},\Gamma} \subseteq \mathbb{Z}_{>0}$ (and similarly for $\mathbb{Z}_{\mathfrak{n},\Lambda}$). Thus, $\mathbb{Z}_{\mathfrak{m},\Gamma} \subseteq \mathbb{Z}_{>0}$ if and only if $\mathbb{Z}_{\mathfrak{n},\Lambda} \subseteq \mathbb{Z}_{>0}$.

(iii): If $-1 \in \mathbb{Z}_{\mathfrak{m},\Gamma}$, then it follows from Corollary 5.4 that $-1 \in \mathbb{Z}_{\mathfrak{n},\Lambda}$. We have three cases to consider.

Suppose $2 \mid \mathfrak{m}_0$ and $2 \mid \mathfrak{n}_0$. Since $\langle \pm 1 \rangle$ reduces injectively modulo p for every odd prime p, Lemma 5.7 implies that $\mathrm{supp}(\mathfrak{m}_0) = \mathrm{supp}(\mathfrak{n}_0)$, so that Theorem 5.5(iv) implies that $\langle \pm 1 \rangle \mathbb{Z}_{\mathfrak{m},\Gamma} = \langle \pm 1 \rangle \mathbb{Z}_{\mathfrak{n},\Lambda}$. Since $-1 \in \mathbb{Z}_{\mathfrak{m},\Gamma} \cap \mathbb{Z}_{\mathfrak{n},\Lambda}$, it follows that $\mathbb{Z}_{\mathfrak{m},\Gamma} = \mathbb{Z}_{\mathfrak{n},\Lambda}$.

From the primitive ideal space computation discussed in § 2.2, we see that the isomorphism $C^*_\lambda(\mathbb{Z} \rtimes \mathbb{Z}_{\mathfrak{m},\Gamma}) \cong C^*_\lambda(\mathbb{Z} \rtimes \mathbb{Z}_{\mathfrak{n},\Lambda})$ induces a bijection $\varphi : \mathcal{P}^{\mathfrak{m}}_{\mathbb{Q}} \cong \mathcal{P}^{\mathfrak{n}}_{\mathbb{Q}}$ such that $C^*_\lambda(\mathbb{Z} \rtimes \mathbb{Z}_{\mathfrak{m},\Gamma})/I_p \cong C^*_\lambda(\mathbb{Z} \rtimes \mathbb{Z}_{\mathfrak{n},\Lambda})/J_{\varphi(p)}$ for all $p \in \mathcal{P}^{\mathfrak{m}}_{\mathbb{Q}}$ where I_p is the minimal primitive ideal of $C^*_\lambda(\mathbb{Z} \rtimes \mathbb{Z}_{\mathfrak{m},\Gamma})$ corresponding to $p \in \mathcal{P}^{\mathfrak{m}}_{\mathbb{Q}}$ and $J_{\varphi(p)}$ is the minimal primitive ideal of $C^*_\lambda(\mathbb{Z} \rtimes \mathbb{Z}_{\mathfrak{n},\Lambda})$ corresponding to $\varphi(p) \in \mathcal{P}^{\mathfrak{n}}_{\mathbb{Q}}$.

Now suppose $2 \nmid \mathfrak{m}_0$ and $2 \nmid \mathfrak{n}_0$, so that $2 \in \mathcal{P}^{\mathfrak{m}}_{\mathbb{Q}} \cap \mathcal{P}^{\mathfrak{n}}_{\mathbb{Q}}$. Since I_2 contains the projection

$$1 - \sum_{k \in \mathbb{Z}/(2^{f_2^\Gamma})} \lambda(k, 2^{f_2^\Gamma}) \lambda(k, 2^{f_2^\Gamma})^*$$

(see [1, Theorem 7.1]), it follows that $\mathrm{ord}([1_{C^*_\lambda(\mathbb{Z} \rtimes \mathbb{Z}_{\mathfrak{m},\Gamma})/I_2}]_0)$ divides $2^{f_2^\Gamma} - 1$. Arguing as in the proof of [28, Proposition 4.8] and using analogues of [28, Lemmas 4.3 & 4.5] shows that $\frac{2^{f_2^\Gamma} - 1}{\gcd(2, 2^{f_2^\Gamma} - 1)} = 2^{f_2^\Gamma} - 1$ divides $\mathrm{ord}([1_{C^*_\lambda(\mathbb{Z} \rtimes \mathbb{Z}_{\mathfrak{m},\Gamma})/I_2}]_0)$, and thus $\mathrm{ord}([1_{C^*_\lambda(\mathbb{Z} \rtimes \mathbb{Z}_{\mathfrak{m},\Gamma})/I_2}]_0) = 2^{f_2^\Gamma} - 1$. Similarly, we have $\mathrm{ord}([1_{C^*_\lambda(\mathbb{Z} \rtimes \mathbb{Z}_{\mathfrak{n},\Lambda})/J_2}]) = 2^{f_2^\Lambda} - 1$. There are now two sub-cases to consider.

If $\varphi(2) = q$ for some odd prime $q \in \mathcal{P}^{\mathfrak{n}}_{\mathbb{Q}}$, and $\varphi^{-1}(2) = q'$ for some odd prime $q' \in \mathcal{P}^{\mathfrak{m}}_{\mathbb{Q}}$, then, from the above discussion and Proposition 5.1, $2^{f_2^\Gamma} - 1 = \frac{q^{f_q^\Lambda} - 1}{2}$ and $2^{f_2^\Lambda} - 1 = \frac{q'^{f_{q'}^\Gamma} - 1}{2}$. Using (i), we have $f_2^\Gamma = \mathrm{ord}((2, \mathbb{Q}(\mathfrak{m})^{\bar{\Gamma}})) = \mathrm{ord}((2, \mathbb{Q}(\mathfrak{n})^{\bar{\Lambda}})) = f_2^\Lambda$, so we must have $q = q'$. Now φ restricts to a bijection $\mathcal{P}^{\mathfrak{m}}_{\mathbb{Q}} \setminus \{2, q\} \cong \mathcal{P}^{\mathfrak{n}}_{\mathbb{Q}} \setminus \{2, q\}$ which must be the identity by Proposition 5.1; hence, $\mathrm{supp}(\mathfrak{m}_0) \cup \{2, q\} = \mathrm{supp}(\mathfrak{n}_0) \cup \{2, q\}$. Since $2, q \in \mathcal{P}^{\mathfrak{m}}_{\mathbb{Q}} \cap \mathcal{P}^{\mathfrak{n}}_{\mathbb{Q}}$, this implies $\mathrm{supp}(\mathfrak{m}_0) = \mathrm{supp}(\mathfrak{n}_0)$. As in the first case above, Theorem 5.5(iv) and the fact that $-1 \in \mathbb{Z}_{\mathfrak{m},\Gamma} \cap \mathbb{Z}_{\mathfrak{n},\Lambda}$ imply that $\mathbb{Z}_{\mathfrak{m},\Gamma} = \mathbb{Z}_{\mathfrak{n},\Lambda}$.

If $\varphi(2) = 2$, then Proposition 5.1 implies that φ must be the identity map which forces $\mathrm{supp}(\mathfrak{m}_0) = \mathrm{supp}(\mathfrak{n}_0)$, so that Theorem 5.5(iv) implies that $\langle \pm 1 \rangle \mathbb{Z}_{\mathfrak{m},\Gamma} = \langle \pm 1 \rangle \mathbb{Z}_{\mathfrak{n},\Lambda}$. Since $-1 \in \mathbb{Z}_{\mathfrak{m},\Gamma} \cap \mathbb{Z}_{\mathfrak{n},\Lambda}$, it follows that $\mathbb{Z}_{\mathfrak{m},\Gamma} = \mathbb{Z}_{\mathfrak{n},\Lambda}$.

For the last case, suppose without loss of generality that $2 \nmid \mathfrak{m}_0$ and $2 \mid \mathfrak{n}_0$. Let $q \in \mathcal{P}^{\mathfrak{n}}_{\mathbb{Q}}$ be the odd prime such that $\varphi(2) = q$. Then, by Proposition 5.1, φ restricts to the identity map from $\mathcal{P}^{\mathfrak{m}}_{\mathbb{Q}} \setminus \{2\}$

onto $\mathcal{P}^{\mathfrak{n}}_{\mathbb{Q}} \setminus \{q\}$, which implies that $\mathrm{supp}(\mathfrak{m}_0) \cup \{2\} = \mathrm{supp}(\mathfrak{n}_0) \cup \{q\}$. Now Theorem 5.5(iv) implies that $\langle \pm 1 \rangle \cdot (\{a \in \mathbb{Z}_{\mathfrak{m},\Gamma} : \gcd(a, 2q) = 1\}) = \langle \pm 1 \rangle \cdot (\{a \in \mathbb{Z}_{\mathfrak{n},\Lambda} : \gcd(a, 2q) = 1\})$. Since -1 is in $\{a \in \mathbb{Z}_{\mathfrak{m},\Gamma} : \gcd(a, 2q) = 1\}$ and $\{a \in \mathbb{Z}_{\mathfrak{n},\Lambda} : \gcd(a, 2q) = 1\}$, we are done. □

5.2. **Reconstruction using Cartan pairs.** As discussed in § 2.2, let $D_\lambda(R \rtimes M)$ denote the canonical Cartan subalgebra of $C^*_\lambda(R \rtimes M)$.

Theorem 5.10. *Let K, L be number fields with rings of algebraic integers R, S, and suppose that we are given data $\mathfrak{m}$, Γ and $\mathfrak{n}$, Λ as in § 2.2 for K and L, respectively. Let M and N be the corresponding congruence monoids. If $(C^*_\lambda(R \rtimes M), D_\lambda(R \rtimes M)) \cong (C^*_\lambda(S \rtimes N), D_\lambda(S \rtimes N))$, then there is a bijection $\varphi : \mathcal{P}^{\mathfrak{m}}_K \cong \mathcal{P}^{\mathfrak{n}}_L$ such that $N(\mathfrak{p}) = N(\varphi(\mathfrak{p}))$, $f^\Gamma_{\mathfrak{p}} = f^\Lambda_{\varphi(\mathfrak{p})}$, and we have $\mathrm{Cl}^{\bar{\Gamma}}_{\mathfrak{m}} \cong \mathrm{Cl}^{\bar{\Lambda}}_{\mathfrak{n}}$ (as abelian groups).*

Proof. In the following, let us fix a number field K with ring of algebraic integers R and given data $\mathfrak{m}$, Γ, and let us explain how to recover the prime ideals of K that are relatively prime to $\mathfrak{m}_0$, together with the functions $N(-)$, $f(-)$, as well as the group $C := \mathrm{Cl}^{\bar{\Gamma}}_{\mathfrak{m}}$, from the Cartan pair $(C^*_\lambda(R \rtimes M), D_\lambda(R \rtimes M))$. We proceed as in [29].

To simplify notation, since the number field and all the relevant data are fixed we drop sub- and superscripts following our notational conventions (see § 3). Write $D := D_\lambda(R \rtimes M)$. For every subset $\mathcal{F}$ of $\mathcal{P} = \mathcal{P}^{\mathfrak{m}}_K$, let $I_{\mathcal{F}}$ be the primitive ideal of $C^*_\lambda(R \rtimes M)$ corresponding to $\mathcal{F}$, set $D_{\mathcal{F}} := I_{\mathcal{F}} \cap D$, and let $\iota_{\mathcal{F}} : D_{\mathcal{F}} \hookrightarrow D$, $i : D \hookrightarrow C^*_\lambda(R \rtimes M)$ be the canonical embeddings. We denote the induced homomorphisms in K_0 by $(\iota_{\mathcal{F}})_*$ and i_*. Let $\Delta := i_*(K_0(D))$, $\Delta_{\mathcal{F}} := i_*((\iota_{\mathcal{F}})_*(K_0(D_{\mathcal{F}})))$ and write $\pi_{\mathcal{F}}$ for the canonical projection $\Delta \twoheadrightarrow \Delta/\Delta_{\mathcal{F}}$. For $\mathcal{F} = \emptyset$, we set $D_{\mathcal{F}} := (0)$ and $\Delta_{\mathcal{F}} = \{0\}$. Given a collection $\mathcal{F}$ of prime ideals in $\mathcal{P}$, let $C_{\mathcal{F}}$ be the subgroup of C given by $\langle \{[\mathfrak{p}] \colon \mathfrak{p} \in \mathcal{F}\} \rangle \subseteq C$, where $C_\emptyset$ is the trivial subgroup.

It follows from the K-theory formula in Theorem 4.1 that $\Delta \cong \bigoplus_C \mathbb{Z}$. Let $M_{\mathfrak{p}}$ be the composite $\Delta \xrightarrow{\mathfrak{p}_*} \Delta \xrightarrow{N(\mathfrak{p})\,\mathrm{id}} \Delta$, $[e_{\mathfrak{a}}] \mapsto N(\mathfrak{p})[e_{\mathfrak{p}\mathfrak{a}}]$, where $e_{\mathfrak{a}}$ denotes the canonical projection in $D \subseteq C^*_\lambda(R \rtimes M)$ corresponding to $\mathfrak{a}$. Using the observation (proven as in [29])

$$\Delta_{\mathcal{F}} = \sum_{\mathfrak{p} \in \mathcal{F}} (\mathrm{id} - M_{\mathfrak{p}})(\Delta) \text{ for every subset } \mathcal{F} \subseteq \mathcal{P}, \tag{7}$$

applied to singletons $\mathcal{F} = \{\mathfrak{p}\}$, we obtain as an application of [29, Lemma 2.3] that

$$\Delta/\Delta_{\{\mathfrak{p}\}} \cong \bigoplus_{C/\langle [\mathfrak{p}] \rangle} \mathbb{Z}/(N(\mathfrak{p})^{\#\langle [\mathfrak{p}] \rangle} - 1)\mathbb{Z} \text{ for every } \mathfrak{p} \in \mathcal{P}. \tag{8}$$

Moreover, (7) and [29, Lemma 2.3] imply the following technical result (the proof is as in [29]):

Proposition 5.11 (analogue of Proposition 2.1 in [29])**.** *Let $\mathcal{F}$ be a finite collection of prime ideals $\mathfrak{p}$ in $\mathcal{P}$ with $\mathfrak{p} \nmid 2$.*

There exists $d_{\mathcal{F}} \in \mathbb{N}_0$ with $\Delta/\Delta_{\mathcal{F}} \cong \bigoplus_{C/C_{\mathcal{F}}} \mathbb{Z}/d_{\mathcal{F}}\mathbb{Z}$. For $\mathcal{F} = \emptyset$, we have $d_\emptyset = 0$, and for $\mathcal{F} \neq \emptyset$, $d_{\mathcal{F}}$ is positive and even.

Moreover, there are ideals $\mathfrak{a}_{\mathcal{F},i}$ in $\mathcal{P}$ with $C = \cup_i C_{\mathcal{F}}[\mathfrak{a}_{\mathcal{F},i}]$ and such that $\{\pi_{\mathcal{F}}[e_{\mathfrak{a}_{\mathcal{F},i}}]\}_i$ forms a $(\mathbb{Z}/d_{\mathcal{F}}\mathbb{Z})$-basis for $\Delta/\Delta_{\mathcal{F}}$. Given an ideal $\mathfrak{a}$ in $\mathcal{P}$ with $[\mathfrak{a}] \in C_{\mathcal{F}}[\mathfrak{a}_{\mathcal{F},i}]$, there exists an odd number $l_{\mathcal{F}}(a) \in \mathbb{N}$ with $\pi_{\mathcal{F}}[e_{\mathfrak{a}}] = l_{\mathcal{F}}(\mathfrak{a})\pi_{\mathcal{F}}[e_{\mathfrak{a}_{\mathcal{F},i}}]$.

Now we complete the proof of Theorem 5.10 as follows: We can read off $\mathcal{P}$ (as a set) as the minimal non-zero primitive ideals of $C^*_\lambda(R \rtimes M)$. We can further read of $\#C$ as $\#C = \mathrm{rk}_{\mathbb{Z}}(\Delta)$, and thus (8) allows us to reconstruct the functions $N(-)$ as well as $f(-)$ on $\mathcal{P}$. Finally, Proposition 5.11 together with [29, Lemma 3.2] allows us to reconstruct the group C. □

As an immediate consequence, we obtain that in the case of the rational number field, isomorphism of Cartan pairs yields a stronger conclusion compared to the one in Theorem 5.9.

Corollary 5.12. *Let $\mathfrak{m}$ and $\mathfrak{n}$ be moduli for $\mathbb{Q}$, and let Γ and Λ be subgroups of $(\mathbb{Z}/\mathfrak{m})^*$ and $(\mathbb{Z}/\mathfrak{n})^*$, respectively. If there is an isomorphism $(C^*_\lambda(\mathbb{Z} \rtimes \mathbb{Z}_{\mathfrak{m},\Gamma}), D_\lambda(\mathbb{Z} \rtimes \mathbb{Z}_{\mathfrak{m},\Gamma})) \cong (C^*_\lambda(\mathbb{Z} \rtimes \mathbb{Z}_{\mathfrak{n},\Lambda}), D_\lambda(\mathbb{Z} \rtimes \mathbb{Z}_{\mathfrak{n},\Lambda}))$, then $\langle \pm 1 \rangle \mathbb{Z}_{\mathfrak{m},\Gamma} = \langle \pm 1 \rangle \mathbb{Z}_{\mathfrak{n},\Lambda}$.*

Proof. By Theorem 5.10, there exists a bijection $\varphi : \mathcal{P}^{\mathfrak{m}}_{\mathbb{Q}} \cong \mathcal{P}^{\mathfrak{n}}_{\mathbb{Q}}$ such that $N(p) = N(\varphi(p))$. Hence, φ must be the identity map, so $\mathrm{supp}(\mathfrak{m}_0) = \mathrm{supp}(\mathfrak{n}_0)$. Now, as in the proof of Theorem 5.9, Theorem 5.5(iv) implies that $\langle \pm 1 \rangle \mathbb{Z}_{\mathfrak{m},\Gamma} = \langle \pm 1 \rangle \mathbb{Z}_{\mathfrak{n},\Lambda}$. □

Let us combine Theorem 5.10 with the following number-theoretic result.

Proposition 5.13. *Assume that $[K(\mathfrak{m})^{\bar{\Gamma}} : K] = [L(\mathfrak{n})^{\bar{\Lambda}} : L]$ and that there is a bijection $\varphi : \mathcal{P}^{\mathfrak{m}}_K \to \mathcal{P}^{\mathfrak{n}}_L$ such that $N(\mathfrak{p}) = N(\varphi(\mathfrak{p}))$ and $f^{\Gamma}_{\mathfrak{p}} = f^{\Lambda}_{\varphi(\mathfrak{p})}$ for all $\mathfrak{p} \in \mathcal{P}^{\mathfrak{m}}_K$. Then K and L are arithmetically equivalent, and $K(\mathfrak{m})^{\bar{\Gamma}}$ and $L(\mathfrak{n})^{\bar{\Lambda}}$ are arithmetically equivalent.*

Proof. For all but finitely many rational primes p, we have

$$g_{K/\mathbb{Q}}(p) = \#\{\mathfrak{p} \in \mathcal{P}^{\mathfrak{m}}_K : p \mid N(\mathfrak{p})\} = \#\{\varphi(\mathfrak{p}) \in \mathcal{P}^{\mathfrak{n}}_L : p \mid N(\varphi(\mathfrak{p}))\} = g_{L/\mathbb{Q}}(p).$$

Hence, K and L are arithmetically equivalent by [41, Main Theorem].

Since every prime $\mathfrak{p} \in \mathcal{P}^{\mathfrak{m}}_K$ is unramifed in $K(\mathfrak{m})^{\bar{\Gamma}}$ by (b) in § 2.3, we have, for each $\mathfrak{p} \in \mathcal{P}^{\mathfrak{m}}_K$,

$$g_{K(\mathfrak{m})^{\bar{\Gamma}}/K}(\mathfrak{p}) f_{K(\mathfrak{m})^{\bar{\Gamma}}/K}(\mathfrak{p}) = [K(\mathfrak{m})^{\bar{\Gamma}} : K]$$

where $g_{K(\mathfrak{m})^{\bar{\Gamma}}/K}(\mathfrak{p})$ denotes the splitting number of $\mathfrak{p}$ in $K(\mathfrak{m})^{\bar{\Gamma}}$, and similarly

$$g_{L(\mathfrak{n})^{\bar{\Lambda}}/L}(\mathfrak{q}) f_{L(\mathfrak{n})^{\bar{\Lambda}}/L}(\mathfrak{q}) = [L(\mathfrak{n})^{\bar{\Lambda}} : L]$$

for all $\mathfrak{q} \in \mathcal{P}^{\mathfrak{n}}_L$. Since $N(\mathfrak{p}) = N(\varphi(\mathfrak{p}))$, we see that, for a rational prime p, we have $\mathfrak{p} \mid p$ if and only if $\varphi(\mathfrak{p}) \mid p$. Thus, for all but finitely many rational primes p, φ restricts to a bijection from the set of primes of K lying over p onto the set of primes of L lying over p. That is, for all but finitely many rational primes p, if $pR = \prod_{i=1}^k \mathfrak{p}_i$ is the prime factorization of pR in R with the $\mathfrak{p}_i$ distinct primes, then the prime factorization of pS in S is given by $pS = \prod_{i=1}^k \varphi(\mathfrak{p}_i)$, and the $\varphi(\mathfrak{p}_i)$ are distinct. For any such prime p, we have

$$\begin{aligned} g_{K(\mathfrak{m})^{\bar{\Gamma}}/\mathbb{Q}}(p) &= \sum_{i=1}^k g_{K(\mathfrak{m})^{\bar{\Gamma}}/K}(\mathfrak{p}_i) = \sum_{i=1}^k \frac{[K(\mathfrak{m})^{\bar{\Gamma}} : K]}{f_{K(\mathfrak{m})^{\bar{\Gamma}}/K}(\mathfrak{p})} = \sum_{i=1}^k \frac{[L(\mathfrak{n})^{\bar{\Lambda}} : L]}{f_{L(\mathfrak{n})^{\bar{\Lambda}}/L}(\varphi(\mathfrak{p}))} = \sum_{i=1}^k g_{L(\mathfrak{n})^{\bar{\Lambda}}/L}(\varphi(\mathfrak{p}_i)) \\ &= g_{L(\mathfrak{n})^{\bar{\Lambda}}/\mathbb{Q}}(p). \end{aligned}$$

where the middle equality used our assumption that $[K(\mathfrak{m})^{\bar{\Gamma}} : K] = [L(\mathfrak{n})^{\bar{\Lambda}} : L]$. Hence, $K(\mathfrak{m})^{\bar{\Gamma}}$ and $L(\mathfrak{n})^{\bar{\Lambda}}$ are split equivalent, so $K(\mathfrak{m})^{\bar{\Gamma}}$ and $L(\mathfrak{n})^{\bar{\Lambda}}$ are arithmetically equivalent by [41, Main Theorem]. □

Corollary 5.14. *Let K, L be number fields with rings of algebraic integers R, S, and suppose we are given data $\mathfrak{m}$, Γ and $\mathfrak{n}$, Λ for K and L, respectively. Let M and N be the corresponding congruence monoids. If $(C^*_\lambda(R \rtimes M), D_\lambda(R \rtimes M)) \cong (C^*_\lambda(S \rtimes N), D_\lambda(S \rtimes N))$, then K and L are arithmetically equivalent, $K(\mathfrak{m})^{\bar{\Gamma}}$ and $L(\mathfrak{n})^{\bar{\Lambda}}$ are arithmetically equivalent and we have $\mathrm{Cl}^{\bar{\Gamma}}_{\mathfrak{m}} \cong \mathrm{Cl}^{\bar{\Lambda}}_{\mathfrak{n}}$.*

Remark 5.15. We can reformulate Corollary 5.14 in terms of continuous orbit equivalence of partial dynamical systems as in [29, Theorem 1.2].

References

[1] C. Bruce, *C*-algebras from actions of congruence monoids on rings of algebraic integers*, Trans. Amer. Math. Soc. *373* (2020), no. 1, 699–726.

[2] C. Bruce, *Phase transitions on C*-algebras from actions of congruence monoids on rings of algebraic integers*, Int. Math. Res. Not. IMRN *2021*, no. 5, 3653–3697.

[3] L.A. Coburn, *The C^*-algebra generated by an isometry*, Bull. Amer. Math. Soc. *73* (1967), 722–726.

[4] H. Cohen, *Advanced topics in computational number theory*. Graduate Texts in Mathematics, 193. Springer-Verlag, New York, 2000.

[5] J. Crisp and M. Laca, *On the Toeplitz algebras of right-angled and finite-type Artin groups*, J. Aust. Math. Soc. *72* (2002), no. 2, 223–245.

[6] J. Crisp and M. Laca, *Boundary quotients and ideals of Toeplitz C^*-algebras of Artin groups*, J. Funct. Anal. *242* (2007), no. 1, 127–156.

[7] J. Cuntz, C. Deninger and M. Laca, *C^*-algebras of Toeplitz type associated with algebraic number fields*, Math. Ann. *355* (2013), no. 4, 1383–1423.

[8] J. Cuntz, *C^*-algebras associated with the $ax+b$-semigroup over $\mathbb{N}$*, in K-theory and noncommutative geometry, EMS Ser. Congr. Rep., Eur. Math. Soc., Zürich 2008, 201–215.

[9] J. Cuntz, S. Echterhoff and X. Li, *On the K-theory of the C*-algebra generated by the left regular representation of an Ore semigroup*, J. Eur. Math. Soc. *17* (2015), no. 3, 645–687.

[10] J. Cuntz, S. Echterhoff and X. Li, *On the K-theory of crossed products by automorphic semigroup actions*, Quart. J. Math. *64* (2013), no. 3, 747–784.

[11] J. Cuntz, S. Echterhoff, X. Li and G. Yu, *K-theory for group C^*-algebras and semigroup C^*-algebras*, Oberwolfach Seminars, 47, Birkhäuser/Springer, Cham, 2017.

[12] J. Cuntz and X. Li, *C*-algebras associated with integral domains and crossed products by actions on adele spaces*, J. Noncommut. Geom. *5* (2011), 1–37.

[13] J. Cuntz and X. Li, *Erratum to "C*-algebras associated with integral domains and crossed products by actions on adele spaces"*, J. Noncommut. Geom. *6* (2012), 819–821.

[14] R.G. Douglas, *On the C^*-algebra of a one-parameter semigroup of isometries*, Acta Math. *128* (1972), no. 3-4, 143–151.

[15] S. Echterhoff and M. Laca, *The primitive ideal space of the C^*-algebra of the affine semigroup of algebraic integers*, Math. Proc. Cambridge Philos. Soc. *154* (2013), no. 1, 119–126.

[16] D. Glasscock, *Norm forms represent few integers but relatively many primes*, preprint. `https://arxiv.org/abs/1705.00531`

[17] N. Higson and G. Kasparov, *E-theory and KK-theory for groups which act properly and isometrically on Hilbert space*, Invent. Math. **144** (2001), 23–74.

[18] N. Higson and J. Roe, *Analytic K-homology*, Oxford Mathematical Monographs, Oxford Science Publications, Oxford University Press, Oxford, 2000.

[19] O. Isely, *K-theory and K-homology for semi-direct products of $\mathbb{Z}^2$ by $\mathbb{Z}$*, Ph.D. thesis, 2011.

[20] W. Jehne, *Kronecker classes of algebraic number fields*, J. Number Theory *9* (1977), no. 3, 279–320.

[21] E. Kirchberg, *Das nicht-kommutative Michael-Auswahlprinzip und die Klassifikation nicht-einfacher Algebren*, C^*-algebras (Münster, 1999), 92–141, Springer, Berlin, 2000.

[22] E. Kirchberg and M. Rørdam, *Infinite non-simple C^*-algebras: absorbing the Cuntz algebras $\mathcal{O}_\infty$*, Adv. Math. *167* (2002), no. 2, 195–264.

[23] M Laca and I Raeburn, *Phase transition on the Toeplitz algebra of the affine semigroup over the natural numbers*, Adv. Math. *225* (2010), no. 2, 643–688.

[24] S. Lang, *Algebraic Number Theory*, 2nd ed., Springer-Verlag, Berlin Heidelberg New York, 1986.

[25] M. Langer and W. Lück, *Topological K-theory of the group C^*-algebra of a semi-direct product $\mathbb{Z}^n \rtimes \mathbb{Z}/m$ for a free conjugation action*, J. Topol. Anal. *4* (2012), no. 2, 121–172.

[26] X. Li, *Semigroup C*-algebras and amenability of semigroups*, J. Funct. Anal. *262* (2012), no. 10, 4302–4340.

[27] X. Li, *Nuclearity of semigroup C*-algebras and the connection to amenability*, Adv. Math. *244* (2013) 626–662.

[28] X. Li, *On K-theoretic invariants of semigroup C*-algebras attached to number fields*, Adv. Math. *264* (2014), 371–395.

[29] X. Li, *On K-theoretic invariants of semigroup C*-algebras attached to number fields*, Part II. Adv. Math. *291* (2016), 1–11.

[30] X. Li, *Partial transformation groupoids attached to graphs and semigroups*, Int. Math. Res. Not. IMRN *2017*, no. 17, 5233–5259.

[31] X. Li and W. Lück, *K-theory for ring C^*-algebras: the case of number fields with higher roots of unity*, unpublished complete preprint version of [32], arXiv:1201.4296v1.

[32] X. Li and W. Lück, *K-theory for ring C^*-algebras: the case of number fields with higher roots of unity*, J. Topol. Anal. *4* (2012), no. 4, 449–479.

[33] X. Li, T. Omland and J. Spielberg, *C*-algebras of right LCM one-relator monoids and Artin-Tits monoids of finite type*, Comm. Math. Phys. *381* (2021), no. 3, 1263–1308.

[34] H. Matui, *Topological full groups of one-sided shifts of finite type*, J. Reine Angew. Math. *705* (2015), 35–84.

[35] J.S. Milne, *Class Field Theory (v4.02)*, `www.jmilne.org/math/` (2013)

[36] G.J. Murphy, *Ordered groups and Toeplitz algebras*, J. Operator Theory *18* (1987), no. 2, 303–326.

[37] T. Nagell, *Introduction to Number Theory*, John Wiley & Sons, Inc., New York; Almqvist & Wiksell, Stockholm, 1951.

[38] J. Neukirch, *Algebraic number theory*, Die Grundlehren der mathematischen Wissenschaften, Springer-Verlag, Berlin, 1999.

[39] C. Pasnicu and M. Rørdam, *Purely infinite C^*-algebras of real rank zero*, J. Reine Angew. Math. *613* (2007), 51–73.

[40] R. Perlis, *On the equation $\zeta_K(s) = \zeta_{K'}(s)$*, J. Number Theory *9* (1977), no. 3, 342–360.

[41] R. Perlis and D. Stuart, *A new characterization of arithmetic equivalence*, J. Number Theory *53* (1995), no. 2, 300–308.

[42] J. Spielberg, *C*-algebras for categories of paths associated to the Baumslag-Solitar groups*, J. Lond. Math. Soc. (2) *86* (2012), no. 3, 728–754.

[43] J.T. Tate, *Fourier analysis in number fields and Hecke's zeta-functions*, Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965), Thompson, Washington, D.C., 1967, 305–347.

(Chris Bruce) School of Mathematical Sciences, Queen Mary University of London, Mile End Road, E1 4NS London, United Kingdom, and School of Mathematics and Statistics, University of Glasgow, University Place, Glasgow G12 8QQ, United Kingdom

Email address: Chris.Bruce@glasgow.ac.uk

(Xin Li) School of Mathematics and Statistics, University of Glasgow, University Place, Glasgow G12 8QQ, United Kingdom

Email address: xin.li@glasgow.ac.uk