DECIDABILITY OF THE ISOMORPHISM PROBLEM FOR STATIONARY AF-ALGEBRAS AND THE ASSOCIATED ORDERED SIMPLE DIMENSION GROUPS

OLA BRATTELI, PALLE E. T. JORGENSEN, KI HANG KIM, AND FRED ROUSH

ABSTRACT. The notion of isomorphism of stable AF-C^*-algebras is considered in this paper in the case when the corresponding Bratteli diagram is stationary, i.e., is associated with a single square primitive incidence matrix. C^*-isomorphism induces an equivalence relation on these matrices, called C^*-equivalence. We show that the associated isomorphism equivalence problem is decidable, i.e., there is an algorithm that can be used to check in a finite number of steps whether two given primitive matrices are C^*-equivalent or not.

INTRODUCTION

In [BJKR98] we studied isomorphism of the stable AF-algebras associated with constant square primitive nonsingular incidence matrices. This isomorphism is called C^*-equivalence of the matrices in [BJKR98] and weak equivalence of the (transposed) matrices in [SwVo00]. In this paper we prove that the isomorphism problem in this setting is decidable, even when the assumption of nonsingularity is removed. The decision procedure is spelled out explicitly in Section 6. This result was announced in [BJKR98], and it is interesting in view of the fact that the corresponding problem for non-constant incidence matrices is undecidable [MuPa98]. That isomorphism is decidable means that there is an algorithm that can be used to decide, in a finite number of steps, whether two given primitive matrices are C^*-equivalent or not. (See below.)

The significance of this result goes well beyond the theory of AF-algebras, since the result may be viewed as a decision procedure for isomorphism of the ordered simple dimension groups associated to the AF-algebras, and this class of groups is important for a variety of other problems, especially in symbolic and topological dynamics, see [PaTa95], [Han81], [BMT87] and [Kit98]. The decision result is a fundamental and nontrivial fact one wants in all these applications.

Bratteli diagrams were introduced in [Bra72] with a view to understanding the structure and the classification of those C^*-algebras which arise as inductive limits of finite-dimensional C^*-algebras, the so-called AF-algebras. In fact, the equivalence relation on Bratteli diagrams which is generated by the operation of telescoping is a complete C^*-isomorphism invariant for the AF-algebras; see [BJO99,

1991 *Mathematics Subject Classification.* 16D70, 46L35, 58B25.

Key words and phrases. C^*-algebras, integral matrices, shifts, isomorphisms, classification, Bratteli diagram, decidability, algorithm, p-adic integers, dimension groups, AF-algebras.

Work supported by U.S. N.S.F. grants DMS9900265 (K.H.K., F.R.) and DMS9700130 (P.E.T.J.), and by the Norwegian N.F.R. (Norges Forskningsråd) and the University of Oslo, Norway (O.B., P.E.T.J.).

Remark 5.6]. It is the decidability of this isomorphism problem in the case of stationary Bratteli diagrams which is our main result here. The diagrams are called *stationary* if the incidence matrix is constant; in the general case it is not constant, but varies from one level to the next. However, it was the stationary class of AF-algebras which came from the problem addressed in [BJO99], and while special, this subfamily is still general enough for the study of substitution dynamical systems, as noted in [DHS99]. Consider, for example, a substitution dynamical system σ (letters to words) derived from a given alphabet S of size N. For $i, j \in S$, let a_{ij} count the number of occurrences of i in the word $\sigma(j)$, resulting from the substitution σ, and let A be the corresponding matrix with dimension group $G(A)$ (see (1.10)). In [DHS99], the co-authors use $G(A)$ in their classification of these systems, which may also be realized as shift dynamical systems on the paths in the corresponding Bratteli diagrams. These systems have significance in formal languages, quasi-crystals, aperiodic tilings of the plane [Rad99], and p-recognizable sets of numbers. Hence the classification we address here has some bearing not only on the original setting of AF-algebras, but also on recent developments in dynamical systems. For a survey of other dynamical system classifications related to more standard shifts than those considered in [DHS99], and the relation of our present classification to these, see [BJKR98]. In particular, it is explained in [BJKR98] that the notion of C^*-equivalence of two primitive nonsingular matrices is strictly weaker than shift equivalence, strong shift equivalence, or elementary shift equivalence. Specifically, formula (1.2) below shows that C^*-equivalence may be expressed also as a certain system of matrix factorizations, but these conditions for C^*-equivalence are less restrictive than those which define shift equivalence [BJKR98, Proposition 2]. This means that some techniques which are common in the study of shift equivalence, see, e.g., [BMT87], are also common in the study of isomorphism of C^*-algebras. The dimension group is one such tool, see [Ell76], [Eff81].

Our approach is based on studying isomorphism of ordered dimension groups (the order is essential!). We introduce those groups in (1.6)–(1.11), and we formulate the associated isomorphism problem. We then go on to prove that this problem is decidable, in Theorem 5.9. A general algorithm which can be used to decide whether or not two primitive matrices A, B are C^*-equivalent is spelled out point by point in Section 6.

After decidability, the next question is a presentation of the answer in terms of numerical invariants. We take this up in Sections 7–10, which are a continuation of [BJO99]. Here the answers are not yet complete, so we present in Section 7 (Proposition 7.1 and Corollary 7.2) a subclass of incidence matrices for which the C^*-equivalence question is decided by the value of a numerical invariant. The matrices A in the subclass allow a direct-sum decomposition, $A = A_0 \oplus (\lambda)$, such that A_0 is unimodular up to sign, and (λ) is multiplication by the Perron–Frobenius eigenvalue λ on the one-dimensional subspace spanned by the right Perron–Frobenius eigenvector. This property is equivalent to $|\det A| = \lambda$.

Section 9 and Section 12 address symmetry properties, pointing out that there are nonsymmetric primitive incidence matrices A which are C^*-equivalent to A^{tr}, the transposed matrix. But even in the 2-by-2 case, there are also examples where A and A^{tr} are not C^*-equivalent. The related symmetry question for shift equivalence comes from the issue of reversibility for topological Markov chains, which was studied in [PaTu82] and [CuKr80].

While the dimension group $G(A)$ associated with an incidence matrix A is torsion-free, it has a certain torsion group quotient $G(A)/L$ by a lattice L in $G(A)$. We show in Proposition 10.2 that this quotient is natural in the sense that it is an invariant. It is well known that abelian torsion groups have explicitly computable and complete numerical invariants, and these invariants are thus also invariants for the dimension group (but not complete because they do not reflect order and some of the group structure). In this case they take an especially simple form, and they can be read off from the characteristic polynomial. This is proved in Section 10. Section 12 presents a formulation of C^*-equivalence for matrices A, B in terms of a certain explicit matrix factorization $B = CAD$, where the two factors C, D are specified in the statement of the result, Theorem 12.2.

By decidability of a class of problems, we will here mean that there is an algorithm (which could be converted into a computer program) to solve the problem [Her69, Her78, Knu81]. There may be no simple way to tell how many steps the algorithm will use, but it must eventually terminate in all cases. This is equivalent to saying that there is a Turing machine, which given the necessary inputs (two matrices here), will give an output which here is zero or one accordingly as the problem has an answer "No" or "Yes". The theory of algorithmic decidability begins essentially with the proof that the halting problem, the problem of whether an arbitrary Turing machine on a given input will halt, is algorithmically undecidable; a result equivalent to this was proved by Gödel, though the theory was cast into different forms by Church, Kleene, and Turing. Its high-water mark was the proof by Davis, Matijasevič, Putnam, and Robinson [DMR76] that diophantine equations over the integers are algorithmically unsolvable (Hilbert's Tenth Problem). Since then many other problems have been proved undecidable (such as the result of [MuPa98] on a different class of C^*-algebras), though others like the diophantine problem over $\mathbb{Q}$, have resisted all efforts. On the other hand, major decidability results have appeared too, such as the proof by Ax and Kochen [AxKo65a, AxKo65b, AxKo66] that it is decidable whether a given system of diophantine equations is solvable simultaneously over every p-adic field or ring, results on power series rings, Rabin's result on the theory of the Cantor set, and the Grunewald–Segal result [GrSe80a, GrSe80b] that isomorphism of forms over algebraic number rings is decidable (which is related to our work here as well as the proof in [KiRo79] that shift equivalence is decidable). Many conjectured decidability results remain open, such as the question of whether abelian and hyperbolic algebraic varieties have a rational point [HiSi00, Parts C and F4].

The classical treatise on decidability in the context of algorithmic algebraic number theory is the book [PoZa97], and we will, sharing the view of those authors, not try to give a definition of algorithm in terms of mathematical logic.

There are some general blanket references which we will use throughout the paper: [Wei98] and [BoSh66] on algebraic number theory, [PoZa97] on algorithms of algebraic number theory, [New72] on integral matrices and their factorizations, and [Kit98], [Wag99] on symbolic dynamics. Especially [PoZa97], [Wei98], and [New72] are used frequently in the proofs to follow, each one containing algorithmic constructions which we cite as they are needed. The proofs involve diverse areas of mathematics which are not always thought to be directly related. They fall at the interface of techniques from these different subjects. For that reason, we include a bit more detail and discussion than is customary in a paper which does not cut across boundaries between fields.

1. Equivalent isomorphism conditions

Recall from [BJKR98] that two matrices A, B with nonnegative integer matrix entries are said to be C^*-equivalent if there exist two sequences $n_1, n_2, \dots$ and $m_1, m_2, \dots$ of natural numbers and two sequences of matrices $J(1), J(2), \dots$ and $K(1), K(2), \dots$ with nonnegative integer matrix entries such that the diagram (1.1) below commutes.

(1.1)
$$\begin{tikzcd}
\bullet \arrow[dd, "A^{n_1}"'] \arrow[dr, "J(1)"] & \\
& \bullet \arrow[dl, "K(1)"'] \arrow[dd, "B^{m_1}"] \\
\bullet \arrow[dd, "A^{n_2}"'] \arrow[dr, "J(2)"] & \\
& \bullet \arrow[dl, "K(2)"'] \arrow[dd, "B^{m_2}"] \\
\bullet \arrow[dd, "A^{n_3}"'] \arrow[dr, "J(3)"] & \\
& \bullet \arrow[dl, "K(3)"'] \arrow[dd, "B^{m_3}"] \\
\bullet \arrow[dd] \arrow[dr, "J(4)"] & \\
& \bullet \arrow[dl] \arrow[dd] \\
\vdots & \\
& \vdots
\end{tikzcd}$$

The diagram expresses the following two identities:

$$A^{n_k} = K(k) J(k), \qquad B^{m_k} = J(k+1) K(k), \tag{1.2}$$

for $k = 1, 2, \dots$. This corresponds to isomorphism of the associated stable AF-algebras [BJKR98, Bra72], and it corresponds to homeomorphism of one-dimensional connected orientable hyperbolic attractors of diffeomorphisms of manifolds by [Jac97]; see also [SwVo00]. We will assume throughout that A and B are primitive square matrices (i.e., sufficiently high powers have only strictly positive matrix entries). For the rest of this section we will also assume that A and B are nonsingular, but this extra condition can be dispensed with by a remedy described in Section 2. So assume that A and B are nonsingular, and hence C^*-equivalence implies that they have the same dimension N, because N is the rank of the associated dimension group [BJO99]. (We will argue in Section 11 that the class of AF-algebras we obtain in this manner will no longer be the same if A and B are merely required to be primitive but not necessarily nonsingular. This does not contradict the results in Section 2, because the matrices replacing A, B there no longer have positive matrix entries, and the order is defined in a different manner.) In this case we note that $J(1)$ and the sequences $n_1, \dots$ and $m_1, \dots$ determine all other $K(k)$ and $J(j)$ from (1.1), i.e.,

$$\begin{aligned} K(1) &= A^{n_1} J(1)^{-1}, \\ J(2) &= B^{m_1} J(1) A^{-n_1}, \\ K(2) &= A^{n_1+n_2} J(1)^{-1} B^{-m_1}, \\ J(3) &= B^{m_1+m_2} J(1) A^{-n_1-n_2}, \\ &\vdots \end{aligned} \tag{1.3}$$

etc. If n is a nonzero integer, let $\operatorname{Prim}(n)$ denote the set of prime factors of n. Then (1.2) implies

$$\operatorname{Prim}(\det(A)) = \operatorname{Prim}(\det(B)), \tag{1.4}$$

and thus (1.3) implies

$$\operatorname{Prim}(\det(J(1))) \subseteq \operatorname{Prim}(\det(A)) = \operatorname{Prim}(\det(B)). \tag{1.5}$$

Thus a necessary and sufficient condition for C^*-equivalence of two primitive, nonsingular $N \times N$ matrices A, B with nonnegative integer matrix entries, is the existence of a (necessarily nonsingular) matrix $J(1)$ with nonnegative integer matrix entries and sequences $n_1, n_2, \dots$ and $m_1, m_2, \dots$ of natural numbers such that the matrices $K(1), J(2), \dots$ defined by (1.3) have positive integer matrix entries.

Another way of formulating this is in terms of dimension groups (see [Bla86], [Eff81], and [BMT87] for details). Let $G(A)$ be the inductive limit of the sequence

$$\mathbb{Z}^N \xrightarrow{A} \mathbb{Z}^N \xrightarrow{A} \mathbb{Z}^N \longrightarrow \cdots \tag{1.6}$$

of free abelian groups with order generated by the order defined on each $\mathbb{Z}^N$ by

$$(m_1, \dots, m_N) \geq 0 \iff m_i \geq 0, \qquad i = 1, \dots, N. \tag{1.7}$$

Since we assume $\det A \neq 0$, we may realize $G(A)$ concretely as a subgroup of $\mathbb{Q}^N$ as follows: Put

$$G_n(A) = A^{-n}\left(\mathbb{Z}^N\right), \tag{1.8}$$

and equip $G_n(A)$ with the order

$$(G_n)_+(A) = A^{-n}\left((\mathbb{Z}_+)^N\right). \tag{1.9}$$

(Here and through the rest of the paper we use the dynamical-systems convention that $\mathbb{Z}^+$ means the strictly positive integers and $\mathbb{Z}_+$ the nonnegative integers, and correspondingly, G^+ means the nonzero positive elements of G and $G_+ = G^+ \cup \{0\}$.) Then $G_0 \subseteq G_1 \subseteq G_2 \subseteq \cdots$ and we define

$$G(A) = \bigcup_{n=0}^{\infty} G_n \tag{1.10}$$

with the order defined by

$$g \geq 0 \qquad \text{if and only if } g \geq 0 \text{ in some } G_n(A). \tag{1.11}$$

Then one fundamental characterization of C^*-equivalence is that there exists a (necessarily nonsingular) matrix $J(1)$ in $M_N(\mathbb{Q})$ such that

$$J(1)\, G(A) = G(B) \tag{1.12}$$

and

$$J(1)\, G^+(A) = G^+(B); \tag{1.13}$$

see [BJO99, Proposition 11.7]. The 1–1 correspondence between group isomorphism θ and matrix J referred to in [BJO99] is as follows: If a matrix $J = J(1)$ is specified as above, then $\theta\colon G(A) \to G(B)$, given by $\theta(g) = Jg$, $g \in G(A)$, will be an isomorphism. Here the product Jg is matrix multiplication, and each g is viewed as a column vector. Conversely, the observation in [BJO99] is that every isomorphism arises this way. This can also be formulated in other ways, as we shall presently do.

If A is a given primitive $N \times N$ matrix, let $\lambda_{(A)}$ denote its Perron–Frobenius eigenvalue, and let $v(A)$ denote a corresponding left (row) eigenvector with strictly positive components and $w(A)$ a corresponding right (column) eigenvector with strictly positive components, and in both cases use a normalization such that the components are contained in the field $\mathbb{Q}\left[\lambda_{(A)}\right]$. Define $V(A)$ as the orthogonal complement of $v(A)$, i.e., $V(A) = \left\{x \in \mathbb{Q}\left[\lambda_{(A)}\right]^N \mid \langle v(A) \,|\, x\rangle = 0\right\} = v(A)^{\perp}$. Then $V(A)$ is an $(N-1)$-dimensional vector space of column vectors which will sometimes be referred to, somewhat informally, as the linear span of the nonmaximal generalized eigenvectors of A; see (1.28). Thus

$$\begin{aligned} &v(A)\, A = \lambda_{(A)} v(A), \quad Aw(A) = \lambda_{(A)} w(A), \text{ and} \\ &\qquad \langle v(A) \,|\, V(A)\rangle = \{0\}, \quad \langle v(A) \,|\, w(A)\rangle \in \mathbb{Q}\left[\lambda_{(A)}\right] \cap (0,\infty). \end{aligned} \tag{1.14}$$

In particular, A leaves $V(A)$ invariant, for if $u \in V(A)$, then

$$\langle v(A) \,|\, Au\rangle = \langle v(A)\, A \,|\, u\rangle = \lambda_{(A)} \langle v(A) \,|\, u\rangle = 0, \tag{1.15}$$

and it follows that $Au \in V(A)$. The same argument applies to the matrix J from (1.16) below. It shows that any J satisfying (1.16) must map $V(A)$ onto $V(B)$; i.e., $JV(A) = V(B)$. The number $\langle v(A) \,|\, w(A)\rangle$ from (1.14) plays an important role in the discussion of the isomorphism problem here (Section 7) and in [BJO99].

Let us mention an alternative form of the isomorphism criterion (1.12)–(1.13), formulated in [BJO99, Proposition 11.7]. Two primitive nonsingular $N \times N$ matrices

A, B with positive integer matrix entries are C^*-equivalent if and only if there is a nonsingular $N \times N$ matrix $J = J(1)$ in $M_N(\mathbb{Z})$ satisfying the two conditions:

$$v(B)\,J = \mu v(A) \qquad \text{for some } \mu \in (0, \infty), \tag{1.16}$$

(1.17) for all $n \in \mathbb{Z}_+$, there is an $m \in \mathbb{Z}_+$ such that

$B^m J A^{-n}$ and $A^m J^{-1} B^{-n}$ both have integer matrix entries;

and then J^{-1} has matrix entries in $\mathbb{Z}[1/\det(A)] = \mathbb{Z}[1/\det(B)]$. It suffices to assume that $J \in \mathrm{GL}(N, \mathbb{R})$, but then (1.17) forces J, J^{-1} to lie in $M_N(\mathbb{Z}[1/\det A]) = M_N(\mathbb{Z}[1/\det B])$. So J is not unique: one may, for example, replace the given J with $B^m J A^{-n}$ for any $m, n \in \mathbb{Z}_+$. By choosing m large enough, one may assure that $B^m J$ has integer matrix entries, and choosing it even larger one may also assure that these entries are positive, and in fact (1.16) may be replaced by the condition

$$J \text{ has positive matrix entries.} \tag{1.16$'$}$$

(But again, a given J may satisfy (1.16)–(1.17) without having positive or integer matrix entries.) The combined two conditions (1.16), (1.17) are equivalent to the two conditions (1.16)$'$, (1.17), and to (1.12), (1.13). For this one uses Perron–Frobenius theory (see, e.g., [New72]): asymptotically when $m \to \infty$, B^m behaves like $\lambda_{(B)}^m$ times the projection onto $w(B)$, and $w(B)$ has strictly positive components.

In the two conditions (1.16)–(1.17) on J, positivity of the matrix entries is just hidden away in the first of the subconditions. However, from (1.1), one may merge the two conditions into the joint condition: There is a nonsingular $N \times N$ matrix $J = J(1)$ in $M_N(\mathbb{Z})$ such that,

(1.18) for all $n \in \mathbb{Z}_+$, there is an $m \in \mathbb{Z}_+$ such that

$B^m J A^{-n}$ and $A^m J^{-1} B^{-n}$ both have positive integer matrix entries.

Thus the single condition (1.18) is equivalent to each of the three pairs of conditions (1.12)–(1.13), (1.16)$'$–(1.17), and (1.16)–(1.17).

Let us record a fact which was not mentioned in [BJO99], namely that the m in (1.18) can be taken to depend linearly on n:

Proposition 1.1. *Let A, B be nonsingular primitive $N \times N$ matrices with positive integer matrix entries, and assume that there is a nonsingular matrix $J \in \mathrm{GL}(N, \mathbb{R})$ such that* (1.18) *holds. It follows that there exists a positive integer k and an integer l such that*

(1.19) *for all positive integers n, the matrices*

$B^{kn+l} J A^{-n}$ *and* $A^{kn+l} J^{-1} B^{-n}$ *both have positive integer matrix entries.*

Proof. To show the existence of k, l giving positivity we may modify the proof of Theorem 6 in [BJKR98] so as to make some specific estimates, i.e., we show that if a solution to (1.1) exists, then the sequences n_i, m_i may be taken to grow at most linearly. Let λ_1, λ_2 be the maximum eigenvalues of B, A. Let $\lambda_3 < \lambda_1, \lambda_2$ exceed the largest absolute value of any other eigenvalue, and let λ_4 be the largest absolute value of the reciprocal of any eigenvalue. Consider $B^m J A^{-n}$. Using the above-mentioned (see (1.14)) two invariant complex vector-space (column vectors) decompositions

$$\mathbb{C}^N = V(A) \oplus \mathbb{C}w(A) \quad \text{and} \quad \mathbb{C}^N = V(B) \oplus \mathbb{C}w(B), \tag{1.20}$$

we note that the contribution of the maximum eigenvector in (JA^{-n}) will be at least $C\lambda_2^{-n}$ for some positive C. When we multiply it by B^m we get $\lambda_1^m C \lambda_2^{-n}$. The largest magnitude of any other term will be some $\lambda_3^m C_1 \lambda_4^n$. We want the former terms to dominate the sum of all the others, say to be N^2 times the largest, where N is the dimension of the matrices. Take logarithms, and we want

$$m \log \lambda_1 + \log C - n \log \lambda_2 > m \log \lambda_3 + \log \left(C_1 N^2\right) + n \log \lambda_4 \tag{1.21}$$

or rearranged equivalently as

$$m \left(\log \lambda_1 - \log \lambda_3\right) > -\log C + \log \left(C_1 N^2\right) + n \left(\log \lambda_2 + \log \lambda_4\right). \tag{1.22}$$

Then some arithmetic progression where the ratio of m to n exceeds

$$\frac{\log \lambda_2 + \log \lambda_4}{\log \lambda_1 - \log \lambda_3} \tag{1.23}$$

will give the domination.

Consider denominators in the matrix entries which have as divisor some algebraic prime p. The prime p is fixed, but we will do this for all prime divisors in $\det(A)$. (For the definition of "algebraic prime", see the end of Section 3.) For simplicity extend the coefficient field and assume we can diagonalize the matrices (the case of a standard Jordan form can be treated similarly). The maximum denominator in A^{-n} is p^{-kn} for some constant k, which for instance can be worked out from the determinant. Then consider the matrix entries in $B^m J A^{-n}$. They will be sums of constants from the diagonalizing matrices times m powers of the eigenvalues μ_i of B, i.e., $\sum_i c_i \mu_i^m$. The eigenvalues, when factored, only involve nonnegative powers of p, since they are algebraic integers.

The terms in this sum for eigenvalues not divisible by p must add up to be an integer at the prime p: otherwise, no very large powers m could make the total an integer. For the other terms, as soon as m exceeds nk plus the degrees of constants arising from diagonalization process, we will have algebraic integers. ☐

There is another general observation about solving for J and K in (1.2), with A and B given, which motivates the p-adic analysis to follow and is a key point in the decidability argument. The identities (1.2) are quadratic. Since the matrix entries on the left are all integral, solving for J and K is therefore a quadratic diophantine problem in the sense of [BoSh66, Ch. 1]: We thus have a system of quadratic equations in the respective matrix entries of J and K, and [BoSh66, Theorem 1 on p. 61, Ch. 1, Section 7.1] amounts to the assertion that the solution to a quadratic diophantine problem is equivalent to instead solving a finite system of related p-adic congruences, but for all p. (See the next paragraph.) Hence, in the following, we will be stating criteria for C^*-equivalence in terms of p-adic conditions. We will specify for which p we need the conditions, for example in Corollary 4.2, and we will show that there are finite algorithms for deciding the problem.

The simplest case of solving an equation by congruences is to replace a diophantine equation

$$F(x) = \sum_{k_1 \dots k_n} a_{k_1 \dots k_n} x_1^{k_1} \cdots x_n^{k_n} = 0 \tag{1.24}$$

where

$$a_{k_1 \dots k_n} \in \mathbb{Z}, \qquad \text{the sum is finite and } k_i \in \{0, 1, 2, \dots\},$$

by the corresponding equation over the ring $\mathbb{Z}_{p^k} = \mathbb{Z}/p^k\mathbb{Z}$ of residues modulo p^k for each prime p and each positive integer k. The latter problem amounts to checking only a finite number of cases, since $\mathbb{Z}_{p^k}$ is obviously finite. The point made in [BoSh66] under the name of Hasse–Minkowski's Theorem is that this is possible when (1.24) is quadratic, but not in general. It is, for example, noted in [BoSh66, p. 3] that the congruences

$$\left(x^2 - 13\right)\left(x^2 - 17\right)\left(x^2 - 221\right) \equiv 0 \qquad \left(\operatorname{mod} p^k\right) \tag{1.25}$$

are solvable for all p^k, i.e., with solution $x \in \mathbb{Z}_{p^k}$, while

$$\left(x^2 - 13\right)\left(x^2 - 17\right)\left(x^2 - 221\right) = 0 \tag{1.26}$$

clearly has no solution $x \in \mathbb{Z}$. When matrices A and B are given in $M_N(\mathbb{Z})$, then solving equation (1.2) for K and J (in $M_N(\mathbb{Z})$) is a quadratic diophantine problem in the matrix entries of K and J.

It seems to be difficult to convert Proposition 1.1 directly into an effective decision procedure for isomorphism, since J is not unique, and hence it is difficult to obtain *a priori* estimates on the norm of J and on the coefficients k and l. Instead we will turn to the completely different method developed in [KiRo88], which is described in the previous paragraph and in Section 5. Instead of starting with an explicit norm estimate on J, we reduce the problem to a collection of congruences and norm restrictions which are decidable by Lemma 5.1.

The simple-minded way of trying to determine the dimension group from (1.8)–(1.11) is to take the algebraic extension of $\mathbb{Q}$ determined by all the roots of the characteristic equation of A, write A in generalized Jordan form [New72], and then compute $\bigcup_m A^{-m}\left(\mathbb{Z}^N\right)$ in the new basis. Vestiges of this approach appear in our argument, but instead of using the complete Jordan form we merely use a reduction to block-diagonal form where the blocks correspond to generalized eigenspaces, first when we determine the subspaces which a rational matrix J_0 has to preserve, and then in studying the matrix giving the difference of the actual matrix J from J_0.

If A has the eigenvalues $\lambda_1, \dots, \lambda_n$ in $\mathbb{C}$ and we view A as a map on the module $V = \mathbb{Q}[\lambda_1, \dots, \lambda_n]^N$, then we have the standard direct-sum decomposition

$$V = \sum_{\lambda \in \operatorname{Sp}(A)} V_\lambda, \tag{1.27}$$

where V_λ is the *generalized eigenspace*

$$V_\lambda = \left\{ x \in V \mid \exists\, k \in \mathbb{Z}^+ \ni (\lambda - A)^k x = 0 \right\}. \tag{1.28}$$

The elements of V_λ are called the *generalized eigenvectors* corresponding to λ.

2. Reduction to nonsingular matrices

The first step in our decision procedure is to reduce the problem to the corresponding problem for two matrices A, B with integer coefficients which are no longer positive, but nonsingular, and with a different definition of positivity in $G(A)$ and $G(B)$. The discussion of the general case when A is not assumed nonsingular is resumed in Section 11.

The following result is well-known [BMT87]. We include the proof since it introduces terminology and details that we will need later.

Lemma 2.1. *Every $N \times N$ matrix A over $\mathbb{Z}$ is shift equivalent to a nonsingular matrix over $\mathbb{Z}$. Specifically, let $\mathcal{W}(A) = A^N \mathbb{Q}^N$. This is an A-invariant subspace, and A restricted to it is nonsingular. Let $\mathcal{W}_0 = \mathcal{W}(A) \cap \mathbb{Z}^N$. This is also A-invariant. Choose a basis for this free abelian group and express the restriction of A to $\mathcal{W}_0$ as a matrix C. Then A is shift equivalent to C.*

Proof. There is an $M \leq N$ such that $\mathcal{W}_0 \cong \mathbb{Z}^M$, and let $x_1, \dots, x_M$ be a column vector basis for the free abelian group $\mathcal{W}_0 \subseteq \mathbb{Z}^N$. Define a matrix R by

$$R = [x_1, \dots, x_M] : \mathbb{Z}^M \longrightarrow \mathcal{W}_0 \subseteq \mathbb{Z}^N.$$

The $N \times M$ matrix R maps $\mathbb{Z}^M$ bijectively onto $\mathcal{W}_0 \subseteq \mathbb{Z}^N$. Let R^{-1} be an $M \times N$ matrix extending the inverse of this bijective map. Then

$$C = R^{-1} A R \colon \mathbb{Z}^M \longrightarrow \mathbb{Z}^M$$

is an $M \times M$ matrix. The mapping A^N on $\mathbb{Z}^N$ has image in $\mathcal{W}_0$, and hence we may define an $M \times N$ matrix map S by

$$S = R^{-1} A^N : \mathbb{Z}^N \longrightarrow \mathbb{Z}^M.$$

Now one immediately verifies that $AR = RC$, $SA = CS$, $SR = C^N$, $RS = A^N$, the equations of shift equivalence. Over an extension field, we may triangularize A, and find that $\mathcal{W}_0$ over this field becomes the sum of all nonzero generalized eigenspaces, since on them A^N is an isomorphism, but on the zero generalized eigenspace of dimension at most N, A^N is zero. Therefore C is nonsingular. □

This mapping $A \mapsto C$ preserves unordered dimension groups. The lemma also shows that every unordered dimension group of an integer matrix (see (11.2) below) is the unordered dimension group of a nonsingular integer matrix. Moreover, the order structure is given by evaluation on a Perron-Frobenius row eigenvector. To see this, note that with the notation of the proof of Lemma 2.1, if v is a row vector in $\mathbb{R}^N$ such that

$$vA = \lambda v,$$

then it follows that

$$vRC = vAR = \lambda vR,$$

i.e., vR is a row vector in $\mathbb{R}^M$ which is an eigenvector of C with the same eigenvalue λ. Applying this on the Perron–Frobenius eigenvalue λ and corresponding eigenvector v, we see that the order structure of the dimension group, realized in $\mathbb{Z}^M$, is given by evaluation on vR. This evaluation can be considered as the projection on column vectors over an extension field which is the identity on the Perron-Frobenius column eigenvector and is zero on all other generalized eigenspaces. Note that the nonsingular matrix C has the property that it has a positive eigenvalue λ which has strictly larger modulus than any other eigenvalue, and if $G(C) = \bigcup_n C^{-n}\mathbb{Z}^M$ is the corresponding dimension group, then $G(C)$ is isomorphic to $G(A)$ as a group by an isomorphism taking strictly positive elements in $G(A)$ into elements $g' \in \bigcup_n C^{-n}\mathbb{Z}^N$ such that $\langle vR \,|\, g' \rangle > 0$. In this way we consider the ordered dimension groups of a singular matrix as the unordered dimension group of a nonsingular matrix together with an order structure which amounts to preservation of the sum of non-Perron–Frobenius generalized eigenspaces. If we start out working with a singular matrix, then we will replace it with this nonsingular matrix as we continue with the decision procedure in Section 5.

We will not need Theorems 6 and 7 from [BJKR98] directly in Section 5, as we may work directly with the dimension groups defined from C as above, but note that these theorems could also be generalized to the setting of primitive singular matrices as follows.

The argument of Theorem 7 of our first paper applies over $\mathbb{Z}$ to characterize maps giving isomorphism of unordered dimension groups. The argument of Theorem 6 will also apply over $\mathbb{Z}$; however, there is a problem with the inverses which are used in the proof. Let $M^{\langle -1 \rangle}$ denote the Drazin inverse of an $N \times N$ matrix M. The Drazin inverse is a matrix having the row and column space of M^N and is such that $MM^{\langle -1 \rangle} = M^{\langle -1 \rangle}M$ is a projection to this column space (is the identity on it). The Drazin inverse is multiplicative over matrices having the same eventual row and column space and is unique, and agrees with the ordinary inverse for nonsingular matrices. In effect, it is the ordinary inverse restricted to the nonzero generalized eigenspaces. Let D be the determinant of M restricted to the nonzero generalized eigenspaces, the product of its nonzero eigenvalues. Then the Drazin inverse has denominators which divide D^N. Use $M^{\langle -n \rangle}$ to denote the Drazin inverse of M^n.

Lemma 2.2. *For singular matrices A, B over $\mathbb{Z}$, a necessary and sufficient condition for C^*-equivalence of matrices A, B is the existence of a nonnegative matrix $J(1)$ such that for all $d \in \mathbb{Z}_+$ there is a $c \in \mathbb{Z}_+$ such that*

$$B^c J(1) A^{\langle -d \rangle}$$

and

$$A^c J(1)^{-1} B^{\langle -d \rangle}$$

are nonnegative integer matrices.

Proof. Form the matrices $J(i)$, $K(i)$, using the formulas (1.3), but now with the respective Drazin inverses in place of inverses. In doing so, we can multiply by suitably chosen higher powers of A or B, and thereby force the $J(i)$'s and $K(i)$'s to have their row and column spaces contained in those of A^N, and then we must have the same inverse formulas for them as in the nonsingular case, provided that we use the Drazin inverse. ∎

With this change, the proofs of Theorems 6 and 7 in [BJKR98] will also go over to the singular case, and characterize C^*-isomorphism of matrices.

3. Subspace structure and localization

In the proof of the main theorem, Theorem 5.9, the structure of subspaces of $\mathbb{C}^N$ which are mapped into each other by a possible intertwiner matrix $J \in M_N(\mathbb{Z})$ will be important. One general idea is the following: Consider a certain subset D_A of

$G(A)$ which is defined by a property which is invariant under group isomorphism. Then

$$\begin{aligned}\tilde{D}_A &= \{g \in G \mid \exists\, n, n_1, \dots, n_m \in \mathbb{Z},\ g_1, \dots, g_m \in D_A \ni\!\!- \ ng = \textstyle\sum_{i=1}^{m} n_i g_i\} \\ &= \text{“the subgroup of } G \text{ linearly spanned by } D_A\text{”}\end{aligned} \tag{3.1}$$

is a subgroup of G. If $G(B)$ is another subgroup of $\mathbb{C}^N$, and $G(B) = JG(A)$, and D_B and $\tilde{D}_B$ are defined as above for $G(B)$, we must have

$$D_B = JD_A, \qquad \tilde{D}_B = J\tilde{D}_A, \tag{3.2}$$

and hence

$$J\mathbb{R}D_A = \mathbb{R}D_B. \tag{3.3}$$

This idea was much exploited in [BJO99] on the subgroups

$$\begin{aligned}D_m(G(A)) &= \textstyle\bigcap_i m^i G(A) \\ &= \text{the set of elements of } G(A) \text{ which are infinitely divisible by } m,\end{aligned} \tag{3.4}$$

and we will soon give an example of this in a more general setting than in [BJO99]. Note in particular that if m is a rational eigenvalue of A, then m is an integer since the characteristic equation of A is monic, and hence $D_m(G(A))$ is nonzero and gives nontrivial information about J. We would like to exploit this idea also when λ is an irrational eigenvalue of A, but since $G(A) \subset \mathbb{Z}[1/|\det A|]^N$, $G(A)$ then clearly does not contain eigenvectors of A. To remedy this situation, we may augment or localize $G(A)$ and $G(B)$ by equipping them with coefficients outside $\mathbb{Z}$, i.e., by considering tensor products

$$\tilde{G}(A) = E \otimes G(A), \qquad \tilde{G}(B) = E \otimes G(B), \tag{3.5}$$

where E is any $\mathbb{Z}$-module, and then J still defines an isomorphism between $\tilde{G}(A)$ and $\tilde{G}(B)$. One then tries to choose E to optimize the information about subspaces. In [BJO99] this remedy was used with E finite cyclic groups, but one may use p-adic numbers, or, as we will also do, various finite algebraic extensions of $\mathbb{Z}$. Which extension is used has to be fine-tuned to the problem. For example, if $E = \mathbb{Z}[1/|\det A|]$, then $\tilde{G}(A) = \mathbb{Z}[1/|\det A|]^N$, and all information about $G(A)$ disappears (except for its rank and the prime factors of $|\det A|$, which both are invariants). Similarly, if λ is an algebraic integer which is a unit, i.e., is such that the constant term in its minimal polynomial is ± 1, then $\lambda^{-1} \in \mathbb{Z}[\lambda]$, and hence *all* elements of $\mathbb{Z}[\lambda] \otimes G(A)$ are divisible by λ, and no information on the subspace structure is obtained. One useful choice of E is based on Theorem 10 in [BJKR98]: If $G(A)$ and $G(B)$ are isomorphic and $\lambda_{(A)}$ and $\lambda_{(B)}$ are the Perron–Frobenius eigenvalues of A and B, then the fields $\mathbb{Q}[\lambda_{(A)}]$ and $\mathbb{Q}[\lambda_{(B)}]$ are the same, and $\lambda_{(A)}$ and $\lambda_{(B)}$ are the products of the same primes over this field. A prime in this context means a prime ideal in the associated subring $\mathbb{O}[\lambda]$ of algebraic integers, i.e., $\mathbb{O}[\lambda]$ is the ring of all elements of $\mathbb{Q}[\lambda]$ which satisfy equations in monic polynomials over $\mathbb{Z}$, so that

$$\mathbb{Z}[\lambda] \subset \mathbb{O}[\lambda] \subset \mathbb{Q}[\lambda]. \tag{3.6}$$

Recall that an ideal $\mathcal{I}$ in a ring is a prime ideal if whenever $\mathcal{I} = \mathcal{I}_1\mathcal{I}_2$ for two ideals $\mathcal{I}_1$, $\mathcal{I}_2$, then $\mathcal{I} = \mathcal{I}_1$ or $\mathcal{I} = \mathcal{I}_2$. One useful choice for E is thus $\mathbb{O}\left[\lambda_{(A)}\right] = \mathbb{O}\left[\lambda_{(B)}\right]$. One other choice we shall use is

$$\Omega = \mathbb{O}\left[\lambda_1, \dots, \lambda_N, \mu_1, \dots, \mu_N\right], \tag{3.7}$$

where $\lambda_1, \dots, \lambda_N, \mu_1, \dots, \mu_N$ are the respective roots in $\mathbb{C}$ of the characteristic equations of A and B:

$$\det\left(\lambda\mathbb{1} - A\right) = 0, \qquad \det\left(\mu\mathbb{1} - B\right) = 0. \tag{3.8}$$

Our decision procedure will involve even other rings and fields. For example, in Section 4 below, we will consider $\mathbb{Z}_{(p)} \subset \mathbb{Q}_{(p)}$, i.e., the p-adic integers and the p-adic numbers. More generally, the setting is $\mathcal{O} \subset \mathcal{F}$ where $\mathcal{F}$ is an algebraic number field, and $\mathcal{O}$ denotes the algebraic integers in $\mathcal{F}$. This is explained in [Wei98, Chapter 1]. There prime divisors are defined as equivalence classes of valuations, and the terminology is calibrated in such a way that a compactness argument shows that prime ideals are of the form $\pi\mathcal{O}$ for suitable elements $\pi \in \mathcal{O}$. The element π is associated with a given valuation φ by requiring that $\varphi(\pi)$ assumes the maximal value < 1 taken on by φ.

Another example of the setup $\mathcal{O} \subset \mathcal{F}$ is $\mathcal{F} = \mathbb{Q}\left(\sqrt{-5}\right)$ and $\mathcal{O} = \mathbb{Z} + \mathbb{Z}\sqrt{-5}$. In general we have unique factorization in terms of prime ideals, but the examples

$$6 = 2 \cdot 3 = \left(1 + \sqrt{-5}\right)\left(1 - \sqrt{-5}\right) \tag{3.9}$$

and

$$14 = 7 \cdot 2 = \left(3 + \sqrt{-5}\right)\left(3 - \sqrt{-5}\right) \tag{3.10}$$

show that we may have nonunique factorization in terms of irreducibles.

In general, the various field extensions are independent of one another, but there are still some embeddings (perhaps unexpected) which will be used in our analysis of p-adic eventual row spaces in Section 4. (If p is a prime number, let $\mathbb{Z}_{(p)}$ and $\mathbb{Q}_{(p)}$ denote the p-adic integers and p-adic numbers, respectively; see the first paragraph of Section 4 for definitions.) These field extensions may be identified by use of a Newton approximation scheme; see, e.g., [BoSh66, Chapter 1, Section 5] and [Wei98, Chapter 5]. For example, the field $\mathbb{Q}\left(\sqrt{-5}\right)$ of (3.9)–(3.10) is embedded in $\mathbb{Q}_{(3)}$ and in $\mathbb{Q}_{(7)}$, but not in $\mathbb{Q}_{(11)}$. This is because the equation $x^2 + 5 = 0$ has solutions in $\mathbb{Z}_{(3)}$ and $\mathbb{Z}_{(7)}$, but not in $\mathbb{Z}_{(11)}$. (The polynomial $x^2 + 5$ is irreducible in $\mathbb{Z}_{(11)}[x]$.) All the extensions $\mathbb{Q}_{(3)}$, $\mathbb{Q}_{(7)}$, and $\mathbb{Q}_{(11)}$ are, however, mutually independent; see [Wei98, Section 1-2].

To make it clear when our primes refer to those in the standard setup $\mathbb{Z} \subset \mathbb{Q}$, i.e., when the primes are just $2, 3, 5, 7, \dots$, we refer to the latter as "rational primes"; but if there is no danger of confusion, we will simply refer to them as primes. Recall that "algebraic prime" means a prime in the associated subring of algebraic integers.

We will also work with Galois field extensions $\mathbb{Q} \subset \mathcal{F}$ (see [Rot98]); for example $\mathcal{F}$ may be obtained by adjoining roots to $\mathbb{Q}$. As usual, the Galois group is defined as the group of automorphisms of $\mathcal{F}$ leaving $\mathbb{Q}$ pointwise fixed; thus, elements in the Galois group permute the roots and are uniquely determined by this permutation. The Galois group will act on vectors over $\mathcal{F}$ by $(x_i) \to (x_i^g)$, where x^g for $x \in \mathcal{F}$ and $g \in \mathcal{G}$ denotes the action of g on x. Hence $\mathcal{G}$ also acts on matrices over $\mathcal{F}$; and, either way, the respective actions will be used in defining Galois conjugacy.

4. p-ADIC CHARACTERIZATION OF J

We have already given several characterizations of the intertwiner J more or less in terms of the dimension groups $G(A)$, $G(B)$, i.e., (1.1), ((1.16) & (1.17)), ((1.16)$'$ & (1.17)), and (1.18). Here $G(A)$ and $G(B)$ are defined in terms of asymptotic properties of A^{-n} and B^{-n} as $n \to \infty$. We will now give an exposition of another property of J given in terms of asymptotic properties of the *positive* powers A^n and B^n as $n \to \infty$. Since $n \to A^n \mathbb{Z}^N$ is decreasing, and

$$\bigcap_n A^n \mathbb{Z}^N = \left\{ m \in \mathbb{Z}^N \mid q(A)\, m = 0 \right\} \tag{4.1}$$

by [BJO99, Proposition 12.1], where $q(t)$ is the product of those irreducible (over $\mathbb{Z}$) factors of $\det(t\mathbb{1} - A)$ which have constant term ± 1, the lattices $\bigcap_n A^n \mathbb{Z}^N$ give very little information except that J has to map $\bigcap_n A^n \mathbb{Z}^N$ onto $\bigcap_n B^n \mathbb{Z}^N$. However, if one replaces these intersections by p-adic limits, one can say much more. Recall that if $p \in \{2, 3, 5, 7, 11, \dots\}$ is an ordinary prime, the ring of p-adic integers $\mathbb{Z}_{(p)}$ is the projective limit

$$0 \xleftarrow{p} \mathbb{Z}_p \xleftarrow{p} \mathbb{Z}_{p^2} \xleftarrow{p} \mathbb{Z}_{p^3} \longleftarrow \cdots \longleftarrow \mathbb{Z}_{(p)}, \tag{4.2}$$

where the left maps are multiplication by p. It can be equipped with a topology making it into a compact totally disconnected ring. This is in fact the topology the additive group $\mathbb{Z}_{(p)}$ has as a dual group to $\mathbb{Z}_{p^\infty}$ viewed as the inductive limit of the discrete groups

$$0 \hookrightarrow \mathbb{Z}_p \hookrightarrow \mathbb{Z}_{p^2} \hookrightarrow \mathbb{Z}_{p^3} \hookrightarrow \cdots \hookrightarrow \mathbb{Z}_{p^\infty}, \tag{4.3}$$

where the injections come from the standard realization of $\mathbb{Z}_{p^\infty} = \mathbb{Z}[1/p]/\mathbb{Z}$ as a subgroup of the circle group $\mathbb{T}$; see [Kob84], [Ser79], [Ser98]. Koblitz uses the terminology $\mathbb{Z}_p$ for the p-adic integers, our $\mathbb{Z}_{(p)}$, while we reserve $\mathbb{Z}_p$ for $\mathbb{Z}/p\mathbb{Z}$. Other authors, e.g., [BoSh66], use O_p for the p-adic integers. In the duality consideration of the two groups $\mathbb{Z}_{(p)}$ and $\mathbb{Z}_{p^\infty}$ of (4.2)–(4.3), we use the duality notion of locally compact abelian *groups,* e.g., $\mathbb{Z}_{p^\infty}$ is realized as the group of continuous characters on $\mathbb{Z}_{(p)}$, and conversely, $\mathbb{Z}_{(p)}$ acts as the group of all characters on $\mathbb{Z}_{p^\infty}$. Now $\mathbb{Z}_{(p)}$ is a ring and thus a $\mathbb{Z}$-module, but it is not a field: If q is an integer, then $1/q \in \mathbb{Z}_{(p)}$ if and only if q is mutually prime with p. However, $\mathbb{Z}[1/p] \otimes \mathbb{Z}_{(p)} = \mathbb{Q}_{(p)}$ is a field called the p-adic numbers.

Now if $A \in M_N(\mathbb{Z})$ is a matrix, we may view A as a matrix with matrix entries in $\mathbb{Z}_{(p)}$, and we may associate a unique idempotent

$$E_{(p)}(A) = E(A) \in M_N\left(\mathbb{Z}_{(p)}\right) \tag{4.4}$$

with A by using the following presumably known lemma (we did not find a reference).

Lemma 4.1. *If $A \in M_N(\mathbb{Z}/q\mathbb{Z})$ for a $q \in \mathbb{Z}$, then the semigroup $\{A, A^2, A^3, \dots\}$ contains an idempotent E. This idempotent is unique, and $\{n \mid A^n = E\}$ is a subsemigroup of $\mathbb{Z}^+$.*

Proof. Since $M_N(\mathbb{Z}/q\mathbb{Z})$ is finite, there is an $m_0 \in \mathbb{Z}_+$ and an $n_0 \in \mathbb{Z}^+$ such that $A^{n_0+m_0} = A^{m_0}$.But then $A^{n_0+m} = A^m$ for all $m \geq m_0$ and thus $A^{kn_0+m} = A^m$ for all $k \in \mathbb{Z}^+$. Choose k such that $kn_0 \geq m_0$ and put $m = kn_0$. This gives $\left(A^{kn_0}\right)^2 = A^{kn_0}$ so A^{kn_0} is idempotent.

If A^n and A^m are idempotents, then $A^n = (A^n)^m = (A^m)^n = A^m$, so the idempotent is unique. If it is called E, then if $A^n = A^m = E$, then $A^{n+m} = E \cdot E = E$, so $\{n \mid A^n = E\}$ is a semigroup. □

We now turn to part of the construction of the idempotent $E_{(p)}(A)$ in (4.4).

Fix a prime p, and let $e(m)$ be an increasing sequence of integers such that $A^{e(m)}$ is an idempotent modulo p^m in M_N,

$$\left(A^{e(m)}\right)^2 = A^{e(m)} \mod p^m M_N(\mathbb{Z}). \tag{4.5}$$

This sequence exists because of Lemma 4.1, and by thinning out the sequence, and using Lemma 4.1 again, we may also assume

$$\left(B^{e(m)}\right)^2 = B^{e(m)} \mod p^m M_N(\mathbb{Z}). \tag{4.6}$$

But by the uniqueness of the idempotent, it follows that

$$m' > m \Longrightarrow A^{e(m')} = A^{e(m)} \mod p^m, \tag{4.7}$$

and hence, by passing to yet another subsequence,

$$E_{(p)}(A) = \lim_{m\to\infty} A^{e(m)} \tag{4.8}$$

exists in $M_N\left(\mathbb{Z}_{(p)}\right)$, and $E_{(p)}(A)$ is an idempotent matrix. Correspondingly, $E_{(p)}(B)$ is an idempotent matrix. Now, if A and B define isomorphic dimension groups $G(A)$ and $G(B)$, it follows from (1.17) that there exist for each $n \in \mathbb{Z}_+$ integer matrices $K_n, L_n \in M_N(\mathbb{Z})$ and positive integers $m_n$such that

$$B^{m_n} J = K_n A^n, \tag{4.9}$$

$$A^{m_n} = L_n B^n J. \tag{4.10}$$

We may replace the powers m_n by a new sequence (and thus K_n, L_n by new integer matrices) to ensure that A^{m_n}, B^{m_n} have subsequences converging p-adically to the idempotents $E_{(p)}(A)$ and $E_{(p)}(B)$. Since $\mathbb{Z}_{(p)}$ is compact (and metrizable), it follows that there is a subsequence of $n \to \infty$ such that $\lim_n K_n = K$ and $\lim_n L_n = L$ exist in $M_N\left(\mathbb{Z}_{(p)}\right)$, and we get from the relations above that

$$E_{(p)}(B) J = K E_{(p)}(A), \tag{4.11}$$

$$E_{(p)}(A) = L E_{(p)}(B) J. \tag{4.12}$$

Now define the $\mathbb{Z}_{(p)}$-eventual row space $G_{(p)}(A)$ of A as the linear combinations over $\mathbb{Z}_{(p)}$ of the row-vectors of $E_{(p)}(A)$, and similarly for $E_{(p)}(B)$. Then (4.11) and (4.12) together say that

$$G_{(p)}(B) J = G_{(p)}(A). \tag{4.13}$$

Thus (4.13) holds for any prime p. But conversely, by taking p-adic limits as in the proof of Theorem 7 in [BJKR98], if (4.13) holds for all primes p in the set $\operatorname{Prim}(\det(A)) = \operatorname{Prim}(\det(B))$, then we can recover (1.17). Thus

$$G_{(p)}(B) J = G_{(p)}(A) \qquad \text{for all } p \in \operatorname{Prim}(\det(A)) = \operatorname{Prim}(\det(B)) \tag{4.13$'$}$$

is equivalent to (1.17) (the equivalence of (1.17) and (4.13)$'$ is Theorem 7 in [BJKR98]). The details supplied above expand on the arguments from [BJKR98], which were somewhat terse. Let us cast Theorem 7 in [BJKR98] in a somewhat different, but equivalent, form:

Corollary 4.2. *In order that the unordered dimension groups* $\bigcup_n A^{-n}\mathbb{Z}^N$ *and* $\bigcup_n B^{-n}\mathbb{Z}^N$ *associated with a pair of nonsingular matrices* A, B *be isomorphic, it is necessary and sufficient that* $\operatorname{Prim}(\det(A)) = \operatorname{Prim}(\det(B))$, *and that there exists a nonsingular matrix* $J \in \operatorname{GL}(N, \mathbb{Z}[1/\det(A)])$ (*i.e., the matrix entries of* J *are in* $\mathbb{Z}[1/\det(A)]$ *and* $\det(J)$ *is invertible in the ring* $\mathbb{Z}[1/\det(A)]$) *such that*

$$G_{(p)}(B)\,J = G_{(p)}(A) \tag{4.14}$$

for each prime $p \in \operatorname{Prim}(\det(A))$.

What makes this particularly useful for the decidability problem is that any countably generated torsion-free module over the p-adic integers has a trivial structure: such a module is merely a direct sum of replicas of the p-adic numbers or the p-adic integers ([Pru25]; see also [KaMa51]). The total number of direct summands in $G_{(p)}(B)$ and $G_{(p)}(A)$ is bounded by the rank N of A or B. This makes it possible to decide whether or not J exists with the property (4.13) for each p, but the remaining problem is to find a joint J for all p in $\operatorname{Prim}(A)$ and to ensure the positivity property (1.16). Note that in our setting we have $G_{(p)}(A) \subseteq \mathbb{Z}_{(p)}^N$ by construction as p-adic limits of integer vectors, and hence $G_{(p)}(A)$ cannot contain any element which is infinitely divisible by p, and thus $G_{(p)}(A)$ as a $\mathbb{Z}_{(p)}$-module is just a direct sum of at most N copies of $\mathbb{Z}_{(p)}$ (no direct summand $\mathbb{Q}_{(p)}$ can occur). However, be warned, since $\mathbb{Z}_{(p)}$ is not a field, this is not as useful as knowing that a vector space (over a field) has a certain dimension, since the usual operations of change of basis, etc., cannot be performed within the ring $\mathbb{Z}_{(p)}$. In particular, (4.14) says much more than that the p-adic row spaces have the same rank.

Remark 4.3. To see that the p-adic idempotents and row spaces are independent of the chosen subsequences, note more generally that, when an algebraic prime π is given, we may determine which eigenvalues of A are divisible by π. The Newton polygon [Wei98, Section 3-1, pp. 73–78] for the characteristic polynomial helps to tell which eigenvalues can be taken as π-divisible for algebraic primes π. Then diagonalize A, and replace the π-divisible eigenvalues by 0 and other eigenvalues by 1, to get the projection operator $E_{(\pi)}(A)$ onto the eventual π-adic row space. If $\pi = p$ is a rational prime, $E_{(\pi)}(A) = E_{(p)}(A)$ is the projection defined by (4.8). In the case that π is a nonrational algebraic prime, the procedure above gives a working man's definition of $E_{(\pi)}(A)$. Strictly speaking, the idempotents $E_{(\pi)}(A)$, and the eventual ranges $G_{(\pi)}(A)$, were constructed in (4.8) only in the case when the algebraic prime π is in the smaller set of rational primes, i.e., $2, 3, 5, \dots$; but the construction in (4.8) goes over *mutatis mutandis* to the general case, see, e.g., [Wei98, Sections 4-4–4-5]. In view of this, it is perhaps surprising that isomorphism of dimension groups in Corollary 4.2 is decided only by the much smaller set $\operatorname{Prim}(\det(A))$.

In the case when $p \in \operatorname{Prim}(\det(A))$, then we saw that $G_{(p)}(A)$ is derived from the space

$$\sum_{\mu} \{V_\mu(\text{row}) \mid \mu \in \operatorname{spec}(A),\ p \nmid \mu\}, \tag{4.15}$$

where $V_\mu(\text{row})$ is defined analogously as in (1.28) by

$$V_\mu(\text{row}) = \left\{x \in V^{\text{tr}} \mid \exists\, k \in \mathbb{Z}^+ \ni\!-\ x(\mu - A)^k = 0\right\}. \tag{4.16}$$

As noted, this sum space is initially computed in F^N, for a finite-index field extension F. But, since $G_{(p)}(A) \subset \left(\mathbb{Z}_{(p)}\right)^N$ as a $\mathbb{Z}_{(p)}$-module of row vectors, we conclude that the field F in question must in fact be embedded in $\mathbb{Q}_{(p)}$.

When the extension field F in (4.15) is computed for a given $p \in \operatorname{Prim}(\det(A))$, then the existence of this embedding of fields $F \subset \mathbb{Q}_{(p)}$ is a nontrivial consequence of Corollary 4.2. Such an embedding amounts to the conclusion that the equation $f_A(x) = 0$ has its roots μ from (4.15) in $\mathbb{Q}_{(p)}$, where f_A is the characteristic polynomial of A. The roots in question must then in fact be in $\mathbb{Z}_{(p)}$, since f_A is monic. Hence, this solvability of the characteristic equation in $\mathbb{Z}_{(p)}$ is a subtle consequence of Corollary 4.2, since we show that C^*-isomorphism is decided by the $\mathbb{Z}_{(p)}$-modules $G_{(p)}(A)$; and, in particular, that the latter are nonzero as submodules in $\left(\mathbb{Z}_{(p)}\right)^N$. Of course, after knowing existence, there is the practical issue of having algorithms for finding the solutions.

This issue of field embeddings is addressed algorithmically in [BoSh66, Chapter 1, Section 5]. Our Example 12.4 below further illustrates the point: The equation $x^2 = 2$ is solvable in $\mathbb{Z}_{(7)}$, and so we get a natural field embedding of $\mathbb{Q}\left[\sqrt{2}\right]$ into $\mathbb{Q}_{(7)}$, but not into, for example, $\mathbb{Q}_{(5)}$. (The polynomial $x^2 - 2$ is irreducible in $\mathbb{Z}_{(5)}[x]$.)

Similarly, for the complex case, the equation $x^2 + 1 = 0$ is solvable in $\mathbb{Z}_{(5)}$ and in $\mathbb{Z}_{(13)}$, but not in $\mathbb{Z}_{(2)}$ nor in $\mathbb{Z}_{(7)}$. And so we have field embeddings $\mathbb{Q}[i] \hookrightarrow \mathbb{Q}_{(5)}$ and $\mathbb{Q}[i] \hookrightarrow \mathbb{Q}_{(13)}$, but not an analogous embedding of $\mathbb{Q}[i]$ into $\mathbb{Q}_{(2)}$, nor into $\mathbb{Q}_{(7)}$. More generally, if p is odd, then $x^2 + 1$ is irreducible over $\mathbb{Q}_{(p)}$ if and only if $p \equiv 3 \pmod 4$, while for $p \equiv 1 \pmod 4$, $x^2 + 1$ has two distinct roots in $\mathbb{Z}_{(p)}$, by Hensel's theorem; see [Wei98, Section 2-4-7, p. 62]. The solutions in the respective $\mathbb{Z}_{(p)}$'s may be found by the standard p-adic algorithms, e.g., the Newton scheme [BoSh66, Chapter 1, Section 6].

Example 4.4. A very simple example illustrating Corollary 4.2 is the pair

$$A = \begin{pmatrix} 1 & 1 \\ 2 & 0 \end{pmatrix}, \qquad B = \begin{pmatrix} 0 & 1 \\ 2 & 1 \end{pmatrix}.$$

Then the matrix

$$J = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

defines an isomorphism of $G(A)$ onto $G(B)$. Since $2^n \underset{n\to\infty}{\longrightarrow} 0$ in $\mathbb{Z}_{(2)}$, the respective eigenspaces for the eigenvalue 2 do not contribute to the 2-adic row spaces, and only the -1 eigenspaces contribute. A simple computation shows

$$(-2, 1) \cdot \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = (-1, 1),$$

$$G_{(2)}(B) = \mathbb{Z}_{(2)}(-2, 1), \qquad G_{(2)}(A) = \mathbb{Z}_{(2)}(-1, 1) \qquad \text{(using Remark 4.3)},$$

and

$$\operatorname{Prim}(\det(A)) = \operatorname{Prim}(\det(B)) = \{2\},$$

so (4.14) holds.

5. Decidability of C^*-equivalence

In order to digest the steps taken in this central section of the paper, the reader might find it useful to read this section in conjunction with the road map in the following section, Section 6.

In this section we will prove that the problem of finding an integer matrix $J = J(1)$, satisfying any of the equivalent conditions (1.12)–(1.13), (1.16)–(1.17), (1.16)′–(1.17), (1.18), (1.19), (4.13)′ together with positivity, is decidable. In these considerations, positivity and singularity will be dispensed with as in Section 2, i.e., we will henceforth assume in this section that A and B are nonsingular matrices with integer matrix entries, with the property that A, B have positive eigenvalues $\lambda_{(A)}$, $\lambda_{(B)}$ dominating strictly all other eigenvalues in absolute value, and such that the corresponding left eigenvectors $v(A)$ and $v(B)$ are unique up to a scalar multiple, and for a suitable choice of this scalar, a $g \in G(A) = \bigcup_n A^{-n}\mathbb{Z}^N$ is positive if and only if $\langle v(A) \mid g \rangle > 0$ or $g = 0$. We will, as partially explained in Section 3, work in various algebraic extensions R of $\mathbb{Z}$. The idea is roughly that if J satisfies (1.12):

$$J(1)\, G(A) = G(B), \tag{5.1}$$

then $J(1)$ also satisfies

$$J(1)\left(R \otimes_{\mathbb{Z}} G(A)\right) = R \otimes_{\mathbb{Z}} \left(G(B)\right), \tag{5.2}$$

and, conversely, if (5.2) has no solution $J(1) \in M_N(R)$, then (5.1) certainly has no solution, and this can be used to decide absence of C^*-equivalence.

The operator J, as a mapping of the column vectors in $R \otimes_{\mathbb{Z}} G(A)$, must preserve Galois conjugation (see the end of Section 3). We will see in Proposition 5.4 that the conditions (5.1)–(5.2) amount to having a linear mapping which preserves a lattice of subspaces defined by a lattice of basis elements over an extension field, having only specified primes in its determinant, and satisfying congruences. The lattices of subspaces are sums of generalized eigenspaces (see (1.28) for the definition of *generalized eigenspace*). The summands are determined by conditions of divisibility of eigenvalues by algebraic primes and by the Perron–Frobenius eigenvector. In addition we can multiply the matrix $J(1)$ by powers of A, B which can automatically make it divisible by any power of an algebraic prime π at the π-eigenspace. We will show that these conditions are decidable.

By congruences, we mean that a finite set of vectors over a ring R has its image modulo some ideal I to lie in a specified finite set in R/I. In particular, any Boolean or logical combination of congruences is a set of congruences. We can test congruences by testing each element of this set of residue classes.

Over the integers, a matrix which preserves a sequence of rational subspaces in a direct sum decomposition can be conjugated into a block-triangular form, by taking bases over the integers corresponding to the sequence of subspaces [New72]. Every subgroup of a free abelian group is free, and a finitely generated subgroup is a summand if and only if it has no elements which are not divisible by a prime p in it but are divisible in the total group [Kap69]. However, an integer matrix which preserves a sequence of rational subspaces in a direct sum decomposition cannot always be conjugated further to be block-diagonal over the integers without introducing fractions.

In an algebraic number ring, some finite, computable power of any ideal (the order of the class group [Ser79]) will be principal. It basically follows from ideas in [Wei98, Section 5-3] that we can get a finite list of representatives for the class group, and then we need only have a procedure to test whether an ideal is principal. If it were principal then we can bound the norm of some field element giving the equivalence and test all possibilities. A general algorithm is embodied in the free number-theory software PARI; a theoretical treatment of this problem is in [PoZa97, Section 6.5], [Buc86]. A general algorithm for determining the class group is given in an appendix of [KiRo79]. This means that congruences to a modulus which is an ideal, or fractions whose denominators lie in an ideal, can be restated as congruences to a modulus which is an element, or fractions whose denominators divide a power of some element. Thus we need only to consider ideals (m) generated by a single element $m \in \Omega$ in the following lemma, which will be used in the last step of the decision procedure.

Lemma 5.1. *Let Ω be an algebraic number ring with quotient field F, and let m_1, m_2 be relatively prime elements of Ω, i.e., $(m_1)+(m_2)=\Omega$. Let $f \in F$ be relatively prime to m_1 also. Let $\mathrm{CC}\,[m_1, m_2, f]$ be the following set of congruence classes of matrices M:*

$$\begin{aligned}(5.3)\quad \mathrm{CC}\,[m_1, m_2, f] = \{M \pmod{m_1} \mid M \in M_N(\Omega\,[1/m_2]) \text{ and}\\ \text{there exists an } x \in \Omega\,[1/m_2] \text{ such that } 1/x \in \Omega\,[1/m_2] \text{ and } \det(M) = fx\}.\end{aligned}$$

In words, $\mathrm{CC}\,[m_1, m_2, f]$ is the set of modulo-m_1 reductions of matrices M over F whose entries m_{ij} can be expressed as fractions of elements of Ω whose denominators divide a power of m_2 and such that the determinant of M is a product of f and units and powers of primes dividing m_2.

It follows that there is a finite algorithm to list the finite set $\mathrm{CC}\,[m_1, m_2, f]$.

Remark 5.2. The set $\mathrm{CC}\,[m_1, m_2, f]$ is finite since m_2 is invertible modulo m_1. It is a subset of $M_N\,(\Omega/\,(m_1))$, and the quotient ring $\Omega/\,(m_1)$ is finite. That an algorithm determines something means that the algorithm always gives the correct answer in a finite number of steps.

Proof of Lemma 5.1. We first show that to any given modulus such as m_1^k, we can put a matrix modulo m_1^k into diagonal form using row and column operations (elementary matrices, having one non-zero off-main diagonal entry) modulo m_1. Each such operation lifts to a similar operation over $\Omega[1/m_2]$, so it preserves the given set, and moreover, these lifted operations will preserve the norm of the matrix. The reason that this works is that $\Omega[1/m_2]/(m_1) = \Omega/(m_1)$ is a principal ideal domain, even though Ω may not be. This means that every ideal is modulo m_1 generated by some element—for this it suffices to factor m_1 into primes, use the fact that finite extensions of the p-adic integers are principal ideal domains, and then use the Chinese remainder theorem [Wei98, Remark 4-1-5 and Theorem 2-2-10] to assemble primes.

We can determine the group G_{41} generated by row operations modulo m_1; it is a subsemigroup of the finite semigroup $M(N, \Omega/(m_1))$ generated by a given finite list of generators. The criterion for being in $\mathrm{CC}[m_1, m_2, f]$ is that a matrix is in

$G_{41}D_{41}G_{41}$ where

$$\begin{aligned}D_{41} = \{D \pmod{m_1} \mid D \in M(N, \mathbb{Z}_{m_1^N}) \text{ is diagonal,} \\ \det(D) = xf \pmod{m_1^N} \text{ for an } x \in \Omega\,[1/m_2] \text{ such that } 1/x \in \Omega\,[1/m_2]\}.\end{aligned}$$

We can determine (list) the finite set of such reductions by determining a finite list of generators for the group of units of $\Omega[1/m_2]$, that is, units of Ω and combinations of prime factors of m_2, as well as the class group, the prime factors of f, and their images in the class group. Weiss [Wei98, Corollary 3-3-3, Proposition 4-4-8] gives methods for finding an integral basis—we can take some rational basis, compute its discriminant, and then find integral bases locally at primes which divide the discriminant (in effect by finding extensions of the ring of p-adic integers). Weiss [Wei98, Chapters 2, 3, and Section 4-9] further gives p-adic methods for determining what the prime ideals are which lie over given rational primes p. We can factor an element into primes, by factoring its rational norm into primes [Jac75, p. 64], and successively attempting division by the algebraic primes over p. Also from Weiss [Wei98, Chapter 5] we have algorithms for bounding the norms of representatives of the class group, so that to compute the class group, it remains to tell when two given elements generate the same ideal class, which is discussed by Pohst and Zassenhaus [PoZa97, Chapter 6]. These authors [PoZa97, Chapter 5] also give an algorithm for finding generators for the group of units in algebraic number fields.

Necessity of this condition follows by the first paragraph. We now show sufficiency, i.e., that every such diagonal matrix modulo m_1 actually arises from a matrix of $\mathrm{CC}[m_1, m_2, f]$. To do this, we start with a diagonal matrix the product of whose entries modulo m_1^N is some fx. Then we alter it by multiples of m_1 so as to modify the determinant by an arbitrary multiple of m_1^N. To do this, make the entries $(i, i+1)$ for each i equal to m_1 and the entry $(N, 1)$ equal to any $xm_1 \in m_1\Omega[1/m_2]$. This adds the single product xm_1^N to the determinant. □

We next return to the early steps in the decision procedure and describe the algebra of endomorphisms which preserves a collection of subspaces (those in the next definition).

Definition 5.3. Let A, B be matrices with rational matrix entries. Assume that A, B are nonsingular, and that A, B have positive eigenvalues $\lambda_{(A)}$, $\lambda_{(B)}$ which are larger than the absolute value of all other eigenvalues, with corresponding left eigenvectors $v\,(A)$, $v\,(B)$ unique up to scalars. Let K denote the field generated by the eigenvalues of A and B. Assume that A and B act on vector spaces V, W over $\mathbb{Q}$. Let R be a subring of K. Then A and B act in a natural manner on $V \otimes_{\mathbb{Z}} R$ and $W \otimes_{\mathbb{Z}} R$ respectively. Then $\mathrm{DGI}(A, B, R)$ denotes the additive group of R-homomorphisms $J\,(1)$ from $V \otimes R$ to $W \otimes R$ such that

(α) the direct sums $v\,(A)^{\perp}$ and $v\,(B)^{\perp}$ of all nonmaximal generalized eigenspaces are mapped into each other, and, more generally, for each g in the Galois group of K over $\mathbb{Q}$, the Galois conjugate $\left(v\,(A)^{\perp}\right)^g$ is mapped into $\left(v\,(B)^{\perp}\right)^g$,

(β) for each algebraic prime π of K which divides an eigenvalue, $J\,(1)$ preserves the span $E\,(\pi)$ of the generalized eigenspaces whose eigenvalues are divisible by π.

We shall use the abbreviation DGI, for "dimension group isomorphisms", although "dimension group pre-isomorphisms" would be a more accurate description.

If $\pi = p$ is an ordinary prime, then $E(\pi) \otimes \mathbb{Z}_{(p)}$ is the orthogonal complement of the $\mathbb{Z}_{(p)}$-eventual row space $G_{(p)}(A)$ of A defined in (4.12)–(4.13), which is spanned by generalized row eigenvectors for eigenvalues not divisible by p.

Note that $\mathrm{DGI}(A, B, R)$ really depends on A, B and not merely on V, W, because the generalized eigenspaces and eigenvalues of A and B occur in these conditions. Then our criterion for a dimension group isomorphism says that there is such a map $J(1)$ defined over $\mathbb{Z}$ with the following properties for all algebraic primes π dividing $\det(A)$ and thus $\det(B)$. (We identify $J(1)$ with the map it defines on various sub- and quotient-modules.)

(i) $J(1)$ is nonzero modulo the non-Perron–Frobenius generalized eigenspaces (which can be ensured by congruences relatively prime to π),
(ii) on the quotient $V/E(\pi)$ the determinant of $J(1)$ is relatively prime to π,
(iii) the determinant of $J(1)$ is divisible only by the primes π.

Here (i), (ii) are congruence conditions and (iii) is a determinant condition; these will be transformed a little so that they become the basic criteria whose satisfiability we must decide. By linear algebra, as outlined in the next paragraph, we find a nonsingular map J_0 over the rational numbers satisfying the first two conditions (α)–(β), if it exists, from V to W, and then a general hypothetical map must differ from J_0 by a map J_a in $\mathrm{DGI}(A, A, \mathbb{Q})$: $J(1) = J_0 J_a$. Replace J_0 by some $c_0 J_0$, $c_0 \in \mathbb{Q}$, so that $J_0^{-1} \in M_N(\mathbb{Z})$, where $M_N(R)$ is the algebra of all $N \times N$ matrices over the ring R. Then $J_a \in M_N(\mathbb{Z})$. Write $J_0 = J_c/N_c$, $J_c \in M_N(\mathbb{Z})$, $N_c \in \mathbb{Z}$. Then (i), (ii), (iii) translate into congruence conditions and norm conditions on J_a:

($\mathrm{i_a}$) $J_c J_a$ on the chosen maximal eigenvector $v(A)$ of A is nonzero modulo p_a (a fixed prime relatively prime to $\det(A)$, $\det(J_c)$, N_c);
($\mathrm{ii_a}$) $J_c J_a$ on the quotient $V/E(\pi)$ has determinant a multiple of N_c^N by a invertible number modulo π;
($\mathrm{iii_a}$) the determinant of J_a is $N_c^N / \det(J_c)$ times a number dividing some power of $\det(A)\det(B)$;
($\mathrm{iv_a}$)

$$J_c J_a \equiv 0 \pmod{N_c}. \tag{5.4}$$

The vector space $\mathrm{DGI}(A, A, \mathbb{Q})$ is in fact also an algebra, which we next describe. Let K now denote the field generated by the eigenvalues of A. The next proposition is based on general principles of Galois theory, see, e.g., [Rot98] and [Jac75], as well as standard facts about linear resolutions, see [New72], [Ser77], [Ser98]. First, we can find a basis for the set of linear mappings between two vector spaces V, W which map a finite list of subspaces X_i into another list Y_i. This can be done by writing these inclusion conditions as linear equations in the entries of a matrix. Then write out the determinant of a general matrix in this subspace in terms of variables; if this determinant is not identically zero as a polynomial, then we can find a nonsingular mapping. The next proposition also extends a more primitive variant which appeared earlier in [BJO99, Corollary 9.5]. To understand the statement of the proposition, recall the following standard terminology: If $K \supset \mathbb{Q}$ is a number field, the Galois group $\Gamma = \mathrm{Gal}(K/\mathbb{Q})$ is the group of automorphisms g of K which fix $\mathbb{Q}$ pointwise, i.e., $x^g = x$ for $g \in \Gamma$ and $x \in \mathbb{Q}$. But we shall also consider Γ as a group of transformations of column vectors K^N. If $x = (x_i)_{i=1}^N \in K^N$, we set $x^g = ((x_i)^g)_{i=1}^N$.

The submodules V_i of the vector space $K \otimes \mathbb{Z}^N$ on which A acts, in the following proposition, are all direct sums of generalized eigenspaces of A (see (1.27)–(1.28)), and they are defined as follows: Recall that, for each algebraic prime π, $E(\pi)$ is the linear span of the generalized eigenspaces V_μ where the eigenvalue μ has π as a factor. Thus the Galois action permutes the spaces $E(\pi)$ among themselves. Also throw in $v(A)^\perp$ and its Galois conjugates $\left(v(A)^\perp\right)^g$ in addition to the $E(\pi)$'s, recalling that $v(A)^\perp$ is also a sum of generalized eigenspaces. Note that this implies that Galois conjugation by g will send the generalized eigenspace V_μ for any eigenvalue μ to the generalized eigenspace V_{μ^g} for μ^g (since it will send, for example, generating eigenvectors of one to those of the other, if we make the first coordinate 1, and will send K-linear combinations to possibly different K-linear combinations). So the Galois conjugates of $v(A)^\perp$ will still be sums of generalized eigenspaces. Thus each finite intersection

$$E(\pi_1) \cap E(\pi_2) \cap \dots \cap E(\pi_n) \cap \left(v(A)^\perp\right)^{g_1} \cap \left(v(A)^\perp\right)^{g_2} \cap \dots \cap \left(v(A)^\perp\right)^{g_k}, \qquad g_1, g_2, \dots, g_k \in \Gamma = \mathrm{Gal}(K/\mathbb{Q}),$$

is a direct sum of generalized eigenspaces (if nonzero). The Galois group of K over $\mathbb{Q}$ must map each such finite intersection into another one. By Definition 5.3, all these finite intersections are preserved by $\mathrm{DGI}(A, A, K)$. Now, choose a linear ordering I_i, $i = 1, \dots, l$, of these intersections (the ordering is not unique), such that

(1) if $I_i \supseteq I_j$ then $j \leq i$,
(2) if I_i is a Galois conjugate of I_j and $i < j$, then for all k with $i \leq k \leq j$, I_k is also a Galois conjugate of I_j.

Define $V_j = \bigoplus_{i=j}^{l} I_i$. This gives a decreasing filtration. Since I_i are invariant subspaces of $\mathrm{DGI}(A, A, K)$, all V_i are also invariant subspaces. It is not true that $\mathrm{DGI}(A, A, K)$ is precisely the algebra fixing all V_i, but Proposition 5.4 next gives a partial converse. Since the construction of the filtration above is rather involved, we have fleshed it out in a simple example (Example 5.6 below) in order to highlight the idea.

Proposition 5.4. *There is a filtration V_i, $i = 0, \dots, l$, of the vector space on which A acts in which $\mathrm{DGI}(A, A, K)$ has a block-triangular structure. The ideal $\mathcal{J} = \{M \in \mathrm{DGI}(A, A, K) \mid MV_i \subset V_{i+1},\ i = 0, \dots, l-1\}$ is a nilpotent ideal and $\mathrm{DGI}(A, A, K)/\mathcal{J}$ has a natural embedding by the block structure into $\bigoplus_i \mathrm{GL}(V_i/V_{i+1})$. This embedding is an isomorphism. There is a subfiltration $V_{s(i)}$ defined over $\mathbb{Q}$ such that $V_{s(i)}/V_{s(i+1)}$ is a direct sum of Galois conjugates of $V_{s(i+1)-1}/V_{s(i+1)}$. These structures can be finitely computed.*

Proof. We find the eigenvalues of A, diagonalize A over K, factoring ideals into primes, using standard algorithms, e.g., [PoZa97]. Define I_i and V_i as in the paragraph before the proposition. The effect of Galois action and the families of intersections of these spaces can be considered by taking Galois-invariant bases B_π for $E(\pi)$. We have ordered the intersections I_j with bases B_j by inclusion, and have put Galois conjugates next to each other. Then the subspace generated by all bases succeeding any given basis is preserved, and we have a block-triangular structure corresponding to it, and a larger block-triangular structure, whose blocks are the sets of Galois-conjugate blocks of those from the former structure. The latter will be defined over $\mathbb{Q}$ as required. Since the elements of $\mathcal{J}$ strictly increase filtration, any l-fold product of elements of $\mathcal{J}$ is zero, where l is the filtration length, i.e., the elements of $\mathcal{J}$ are the matrices in the algebra which are zero on the main-diagonal blocks, and so the quotient maps isomorphically into the sum of the general linear groups on V_j/V_{j+1} with basis $B_{0j} = B_j \setminus \bigcup_{k>j} B_k$. Each I_j, by induction, and thus each V_j is spanned by the union of the B_i's contained in it. But we note that the general linear group on the span of B_{0j} will preserve all subspaces $E(\pi)$, and their images will span each of the required summands, so together they will span the sum. Finally, the larger filtration mentioned above gives the $s(i)$'s. □

It follows that all Galois-invariant linear maps on $V_{s(j)}/V_{s(j+1)}$ will also lift to $\mathrm{DGI}(A, A, \mathbb{Q})$.

Proposition 5.5. *Suppose a vector space V over $\mathbb{Q}$ is a direct sum over an extension field $K \supset \mathbb{Q}$ of Galois-conjugate subspaces V_i (with corresponding bases), transitively permuted by the Galois group of K. Then the algebra generated by automorphisms of V over $\mathbb{Q}$ which preserve each space V_i is isomorphic to the general linear group of V_1 over the minimal field K_1 required to define V_1, which corresponds to the subgroup N of the Galois group that sends V_1 to itself.*

Proof. If V_1 can be defined over a subfield of K, then the Galois group of that field must fix V_1; conversely if the Galois group fixes V_1, it will also fix the complementary sum of generalized eigenspaces, hence it will fix a projection operator to the subspace whose kernel is the complementary sum of generalized eigenspaces, and from the columns of a matrix for this operator, the subspace can be defined.

Given an endomorphism of V_1 over K which arises from a mapping over $\mathbb{Q}$, the endomorphisms of all other V_i are uniquely determined as its Galois conjugates. This means we have a one-to-one linear mapping from endomorphisms of V over $\mathbb{Q}$ fixing V_1 (and these by Galois conjugacy fix every V_i), into the general linear group of V_1 over K. In fact the image lies in the general linear group over K_1 since over it, we can define a projection operator to V_1. This mapping is also an epimorphism, since, given any K_1-linear mapping h of V_1 to itself, there are Galois conjugates defined on the other V_i (the Galois operator is unique up to the subgroup fixing V_1, which also fixes h). We can take the sum of h and its Galois conjugates on the other V_i, and the sum will be a Galois-invariant mapping of V, and therefore defined over $\mathbb{Q}$. □

Example 5.6. (Illustrating the construction from Proposition 5.4 of a covariant filtration.) Consider some matrix A with three eigenvalues p, q, pq with respective generalized eigenspaces E_1, E_2, E_3, so that the two sum spaces $E_1 \oplus E_3$ and $E_2 \oplus E_3$ are preserved under the Galois action, as is their intersection E_3. Then the algebra of endomorphisms has a block-triangular structure with three blocks and the main-diagonal blocks are isomorphic to the respective endomorphism algebras $\mathrm{End}(E_1)$, $\mathrm{End}(E_2)$, $\mathrm{End}(E_3)$. Suppose now that p and q are Galois conjugates so that the product pq is Galois-invariant. The larger block structure will then correspond to the two spaces $E_1 \oplus E_2$ and E_3. The group of endomorphisms of $E_1 \oplus E_2$ over the rational numbers will be isomorphic to the automorphisms of E_1 over a quadratic extension field corresponding to the Galois conjugation which interchanges p and q.

We now describe how the elements in $\mathrm{DGI}(A, A, \mathbb{Q})$ may be put into block-triangular form.

As indicated in the paragraph before Proposition 5.4, the V_j's arise by taking direct sums of intersections of the $E(\pi)$'s and $\left(v(A)^{\perp}\right)^{g}$'s, ordered in such a way as to refine the partial order by inclusion of subspaces, and such that Galois conjugates are adjacent. Now add all V_j's which are smaller in the order, to each given element, to make this a decreasing sequence of subspaces. Then all V_j's are invariant subspaces of $\mathrm{DGI}(A, A, K)$. Choose a base of algebraic integer vectors for each generalized eigenspace, so that the Galois conjugate of a base is chosen as a base for the Galois conjugate subspace. Choose also a second basis for the sum of all Galois conjugates of each generalized eigenspace, which exists over the rational integers. Then each V_j is a sum of generalized eigenspaces, so it is spanned by the union of bases which are in it; likewise each $V_{s(i)}$ is spanned over $\mathbb{Q}$ by the union of the second basis elements which are in it. Make the elements of the second basis, in order, the columns of a matrix J_f. Then conjugation by J_f will put the matrices in $\mathrm{DGI}(A, A, \mathbb{Q})$ into block triangular form, because all columns corresponding to each subspace $V_{s(i)}$, which has the form, all basis vectors v_i, $i \geq n_0$, and will span an invariant subspace. In this basis, Galois conjugation is expressed by permutation of basis elements. Then substitution of $J_a = J_f J_g \det(J_f)^{-1} J_f^{-1}$ applied to $(\mathrm{i_a})$, $(\mathrm{ii_a})$, $(\mathrm{iii_a})$, $(\mathrm{iv_a})$ gives the corresponding formulas $(\mathrm{i_g})$, $(\mathrm{ii_g})$, $(\mathrm{iii_g})$, $(\mathrm{iv_g})$.

$(\mathrm{i_g})$ $J_f J_g \det(J_f) J_f^{-1}$ on a chosen maximal eigenvector of A is nonzero modulo p_a (which is a fixed prime relatively prime to $\det(A)$, $\det(J_c)$, N_c, $\det(J_f)$).

$(\mathrm{ii_g})$ $J_c J_f J_g \det(J_f) J_f^{-1} = J_c J_a \det(J_f)^2$ on the quotient $V/E(\pi)$ has determinant a multiple of $\det(J_f)^{2N} N_c^N$ by a rational integer which is invertible modulo π.

$(\mathrm{iii_g})$ $\det(J_g) = \det(J_f)^N \det(J_a)$ is $\det(J_f)^N N_c^N / \det(J_c)$ times a number dividing some power of $\det(A)\det(B)$.

$(\mathrm{iv_g})$

$$J_f J_g \det(J_f) J_f^{-1} \equiv 0 \pmod{\det(J_f)^2}, \tag{5.5}$$

$$J_c J_f J_g \det(J_f) J_f^{-1} \equiv 0 \pmod{N_c det(J_f)^2} \tag{5.6}$$

The first of these says that J_a is an integer matrix and the second is the same as (5.4) multiplied by $\det(J_f)^2$. (Any further multiples by constant matrices could be treated in similar fashion; we are multiplying matrices by these quantities, so when we take determinants we multiply by Nth powers).

We now prove two general propositions about congruences which will be needed.

Recall some aspects of the theory of finite-dimensional algebras $\mathcal{A}$ with unit over a field. The Jacobson radical is the intersection of all maximal proper ideals, equivalently the maximal nilpotent ideal, equivalently in characteristic 0, the kernel $\{x \in \mathcal{A} \mid \mathrm{Trace}(xy) = 0,\ \forall\, y \in \mathcal{A}\}$, where algebra elements are represented as matrices acting on a basis for the algebra [Jac75, Ch. I.14, p. 62]. Modulo the Jacobson radical, the algebra is semisimple, which means it has no nilpotent ideals, and then that every element a is regular in the sense there exists x such that $axa = a$. A semisimple algebra is isomorphic to a direct sum of simple algebras [vdW91]; this decomposition is unique, and corresponds to the set of central idempotents of the algebra. Simple algebras will be given as matrix algebras over algebraic number rings. However, simple finite-dimensional algebras must always be full matrix algebras over division rings.

We will apply the next proposition to integer matrices in $J_f^{-1}\,\mathrm{DGI}(A, A, \mathbb{Q}) J_f$ and the congruences ($\mathrm{i_g}$), ($\mathrm{ii_g}$), ($\mathrm{iv_g}$), and the determinant condition ($\mathrm{iii_g}$).

Note that we can write any Boolean combination of congruences on a single matrix variable x to various moduli in the form

$$\exists\, s \in S \ni x \equiv s \pmod{m} \tag{5.7}$$

for a finite computable set S, by [Wei98]. In the application of Proposition 5.7, m can be taken as, say, the product of the $2N$th power of all denominators and determinants for A, B, M_c, M_f, p_a.

The terminology in the following proposition, that we can solve a finite system of congruences, means that there is an algorithm to determine whether solutions exist, and to find some solution if it exists. The determinant restrictions are those stated in the proof.

Proposition 5.7. *Let $\mathcal{A}$ be a finite-dimensional algebra of matrices over a commutative ring R in block-triangular form, and let J be its Jacobson radical consisting of matrices which have zero main-diagonal blocks. If we can solve any finite system of additive congruences on $\mathcal{A}/J$ subject to any restrictions on the determinant, then we can solve any finite system of additive congruences on $\mathcal{A}$ subject to any restrictions on the determinant. More generally we can restate the congruences on $\mathcal{A}$ as congruences on $\mathcal{A}/J$ and use the same determinant conditions.*

Proof. Note that for our matrix representation the norm conditions on $\mathcal{A}$ will give norm conditions on $\mathcal{A}/J$, since the latter gives the main-diagonal blocks in a block-triangular representation, and the product of their determinants is the determinant in $\mathcal{A}$. The condition that the determinant is a fixed algebraic integer f times products from a finite list of primes and units will translate into a finite list of similar conditions at each main diagonal block, based on the prime factorizations of f. Additively, write an element which is to have determinant involving certain primes, and satisfy congruences, as $x + j$ where j is in the Jacobson radical. The congruences will say, for some $j \in J$, a Boolean combination of congruences $x+j \equiv c \pmod{m}$ hold. If we take all possibilities j_0 for $j \pmod{m}$, this will be a Boolean combination of congruences $x \equiv c - j_0 \pmod{m}$. □

Congruences on an element of an algebraic number ring Ω modulo m will not be changed if we pass to an extension field (but require the element to belong in the original ring), and it will suffice to take congruences modulo the prime power factors of m in the new ring, that is, if Ω_1 is the algebraic number ring of a finite extension of the quotient field of Ω, and if $x, m \in \Omega$, then x is divisible by m in Ω if and only if x is divisible by m in Ω_1.

We make one further transformation of our congruences and determinant conditions. Since it is of the same nature as the previous changes except that we must use Proposition 5.5 and Proposition 5.7 in a way which is difficult to predict, we will not state the formulas explicitly but describe the changes. Using Proposition 5.7, we pass to congruences on the indecomposable blocks of the matrix representations. We use Proposition 5.5 and a further conjugation to pass to congruences over an algebraic number field on particular generalized eigenspaces. This will result in congruences ($\mathrm{i_h}$), ($\mathrm{ii_h}$), ($\mathrm{iv_h}$), and a determinant condition ($\mathrm{iii_h}$). The conditions (ii), and so on, will bound the powers of all primes occurring in the determinant of $J(1)$, J_a, J_g at that generalized eigenspace, except for those which divide the eigenvalue.

One way to determine the congruences is to find a basis for the space of matrices satisfying ($\mathrm{i_g}$)–($\mathrm{iv_g}$), compute their images in the sum of main diagonal blocks, and then give a congruence specifying the span of these images as a finite-index subgroup of a direct sum of rings of the form $M_{N_i}(\Omega_i[1/\lambda_i])$, where the λ_i are eigenvalues and Ω_i the algebraic number rings of the fields in Proposition 5.5.

Proposition 5.8. *Given the congruences* ($\mathrm{i_h}$), ($\mathrm{ii_h}$), ($\mathrm{iv_h}$), *we may construct equivalent congruences of the same type in which the moduli for each generalized eigenspace are relatively prime to the corresponding eigenvalue* π. *Moreover it suffices to find matrices satisfying these conditions with matrix entries in* $\Omega[1/\pi]$. *To do this, split the congruences into ordered tuples of congruences on the respective indecomposable blocks, between each block and a corresponding constant matrix, and replace each modulus with its quotient by all powers of primes dividing the corresponding eigenvalue.*

Proof. We can eliminate the other prime factors of moduli and the denominators by multiplying by a power of the defining matrix A large enough to cancel off the denominators. That is, if we have a solution mapping J_c at a particular generalized eigenspace which satisfies congruences for all primes except those which divide the eigenvalue λ, then $A^n J_a$ will produce a solution at all the other primes, which is congruent to zero modulo any set power of the primes in λ, and therefore exists over Ω. And if any solution does exist, multiplication by a large power of A must produce one which is congruent to zero modulo high powers of the primes in λ; hence it is one that can be found in this way. The last statement follows by invertibility of the matrix A restricted to any eigenspace, at all primes not dividing the eigenvalue, so that there will be arbitrarily large powers of A congruent to the identity. □

We are now ready to state and prove our main theorem. The proof is built up from the previous results, and it is further spelled out in the next section.

As noted in the Introduction, instead of saying "stationary stable AF-algebras" in the following theorem, we might of course say "dimension groups defined by direct limits using constant primitive integer matrices as in (1.1)".

Theorem 5.9. *There is an algorithm to decide isomorphism of stationary stable AF-algebras arising from primitive integer matrices.*

Proof. This result is a consequence of the preliminary discussion and the propositions above. First reduce the problem to the case of nonsingular matrices by the method in Section 2. This reduces the problem to one of finding a matrix $J(1)$ which preserves certain subspaces, has certain primes in its determinants, and satisfies congruences, going from A to B. We find such a matrix J_0 over the rational numbers; the proposed solution must differ from it by multiplying with a matrix $J_a \in \mathrm{DGI}(A, A, \mathbb{Q}) \cap M_N(\mathbb{Z})$ meeting corresponding conditions (we multiply by a constant N_c to arrange that J_a have integer entries). We find the Jacobson radical of $\mathrm{DGI}(A, A, \mathbb{Q})$ and the simple components of the quotient by it, and restate the congruences in terms of those simple components. They are determined in terms of certain combinations of generalized eigenspaces, as general linear groups over algebraic number fields. Again we conjugate, and obtain a new finite set of congruences on a tuple of matrices over algebraic number rings (no longer necessarily fields, because they are images of integer matrices) of the same general nature as the originals, ($\mathrm{i_h}$), ($\mathrm{ii_h}$), ($\mathrm{iv_h}$), and a determinant condition ($\mathrm{iii_h}$). We use Proposition 5.8 to ensure that the congruences involve moduli relatively prime to the eigenvalues and can allow these eigenvalues as denominators. By Lemma 5.1, we can solve them. □

6. The explicit algorithm

In this section we write out the algorithm hinted at in the proof of Theorem 5.9 in more detail. Given two square integer primitive matrices A, B, the algorithm can be used to decide whether the associated (ordered) dimension groups $G(A)$, $G(B)$ are isomorphic or not.

The algorithm has seven steps, numbered I–VII.

Algorithm.

I. Reduce to the nonsingular case as in Lemma 2.1 and its proof:
   (a) Find the kernel of A^N, B^N over $\mathbb{Q}$.
   (b) Find a free basis for the integer vectors in these subspaces.
   (c) Find the images of A, B on those vectors, giving associated nonsingular matrices which henceforth replace A, B. The rank of the two nonsingular matrices must have the same value N, otherwise the algorithm stops.

II. Determine the eigenspace structure of A, B (a general reference for steps II and III is [Jac75, Chapter 1, Sections 1–7]):
   (a) Determine the Perron–Frobenius eigenvalue.
   (b) Determine all eigenvalues and corresponding generalized eigenspaces.
   (c) Determine the field K generated by the eigenvalues and the action of the Galois group on them.
   (d) Factor the eigenvalues into powers of algebraic primes, noting the norms of primes and the action of the Galois group on them. A necessary condition for isomorphism of dimension groups is that the algebraic primes dividing the determinants of A, B must be the same. Stop if not.

III. Determine $\mathrm{DGI}(A, B, K)$ and $\mathrm{DGI}(A, B, \mathbb{Q})$:
   (a) From step II, write out, for each algebraic prime π, the sum $E(\pi)$ of generalized eigenspaces such that π divides the corresponding eigenvalue. Also write out $v(A)^{\perp}$, the sum of the non-Perron–Frobenius generalized eigenspaces, and its Galois conjugates. Do this for both A, B. Call the results $E(\pi)(A)$, $E(\pi)(B)$, $\left(v(A)^{\perp}\right)^{g}$, $\left(v(B)^{\perp}\right)^{g}$.
   (b) Write out the linear equations on a matrix J_{01} over K, ensuring that J_{01} maps each $E(\pi)(A)$ onto $E(\pi)(B)$ and each $\left(v(A)^{\perp}\right)^{g}$ onto $\left(v(B)^{\perp}\right)^{g}$ when going from A to B.
   (c) Find a $\mathbb{Q}$-basis for K which is acted on by the Galois group, and expand J_{01} as a matrix J_{02} using this basis to define a basis for K^N over the field $\mathbb{Q}$ (that is, the K-linear transformation J_{01} is a $\mathbb{Q}$-linear transformation J_{02}). Find the linear equations for Galois invariance (hence definability) over $\mathbb{Q}$ of J_{02}.

(d) By linear algebra, find a basis for the space of all matrices J_{02}. Write the polynomial for a generic matrix in it, and write out its determinant. By algebra of polynomials over K, find whether this polynomial is identically zero, and if it is not identically zero, find a matrix J_0 in it. If it is identically zero, there is no dimension group isomorphism, and the algorithm stops.

IV. Write out congruence conditions on a hypothetical matrix giving an isomorphism $J(1)$ and associated matrices:

(a) $J(1)$ is nonzero modulo the Perron–Frobenius eigenspace; write this in terms of congruences relatively prime to the determinants of A, B. Also write out the congruences that on $V/E(\pi)$ the determinant is relatively prime to π and the condition that its determinant is divisible only by primes in $\det(A)$. This is (i), (ii), (iii) of the text after Definition 5.3.

(b) Write $J(1) = J_0 J_a$ where $J_a \in \mathrm{DGI}(A, A, \mathbb{Q})$ and restate (i), (ii), (iii) as conditions on the hypothetical J_a. This gives ($\mathrm{i_a}$), ($\mathrm{ii_a}$), ($\mathrm{iii_a}$), ($\mathrm{iv_a}$) of the text.

V. Compute the filtration V_I and the associated filtration of algebras:

(a) This filtration is obtained as follows. Take all intersections of the $E(\pi)$ and the Galois conjugates of V_0, which will be various sums of generalized eigenspaces. Order them so that the numbers of sets being intersected increases and that Galois conjugates are adjacent, and add all previous spaces into the next ones so that the sequence of sets increases. Take bases for these spaces using Galois permuted bases for the generalized eigenspaces. (See the paragraph before Proposition 5.4.)

(b) Compute the filtration on the known algebra $\mathrm{DGI}(A, A, K)$ which arises from this, the ideal J of maps which send each $V_i \to V_{i+1}$. Compute the isomorphism $\mathrm{DGI}(A, A, K) \to \sum_i \mathrm{GL}(V_i/V_{i+1})$. (This is Proposition 5.4).

(c) Compute the isomorphism from the Galois invariant elements of $\mathrm{DGI}(A, A, K)/J$ into a direct sum of general linear groups G_s over subfields of K. (This is Proposition 5.5).

VI. Further restate the congruences, as after Example 5.6:

(a) Restate the congruence and norm conditions on J_a in terms of the block triangular form on $\mathrm{DGI}(A, A, \mathbb{Q})$ which arises from step V. The map is a conjugation by some matrix J_f and we have conditions ($\mathrm{i_g}$), ($\mathrm{ii_g}$), ($\mathrm{iii_g}$), ($\mathrm{iv_g}$) on $J_g = \det(J_f) J_f^{-1} J_a J_f$.

(b) Restate the congruences and norm conditions in terms of equivalent conditions on the image element of J_g in G_s, which we call ($\mathrm{i_h}$), ($\mathrm{ii_h}$), ($\mathrm{iii_h}$), ($\mathrm{iv_h}$).

(c) Restate the congruences so that we have only congruences on each generalized eigenspace to moduli relatively prime to the corresponding eigenvalue (Proposition 5.8). This involves multiplying by some power of A and considering the resulting congruences.

VII. Solve the congruences, that is determine whether any solution exists, and if so, find a solution (Lemma 5.1). We do this by finding all matrices $N \times N$ modulo moduli m_1 over an algebraic number ring Ω whose entries have denominators dividing m_2 and whose determinant is a fixed number f relatively prime to m_1 times units in $\Omega[1/m_2]$. This is a finite set and we list it, with representatives:

(a) We determine the basic theory of Ω: integral basis, multiplication, class group, units, primes dividing m_1, m_2, f.
(b) Determine the group G_{41} of products of elementary matrices modulo m_1; we can compute it as a subset of a finite semigroup (all matrices over $\Omega/(m_1)$) having given generators.
(c) Determine the possible determinants of matrices in this set each of which is the reduction of a product of units in $\Omega[1/m_2]$ (a finitely generated group) times products of primes dividing f (a finite set) which is the identity in the class group.
(d) Determine the possible diagonal forms F_{41} modulo m_1: list diagonal elements modulo m_1^N whose product is a possible determinant. (These conditions are unchanged if we pass to the smaller modulus used in the proof).
(e) The required list is $G_{41}F_{41}G_{41}$.

7. The case $\lambda = |\det(A)|$

Theorem 5.9 and Section 6 give a finite algorithm (but in general a long one) to decide whether two square, nonsingular, integer primitive matrices A, B are C^*-equivalent or not. In special cases, like those considered in [BJO99], this algorithm can be substantially simplified. One nice feature of the algorithm is that it uses only "elementary" algebraic results, and avoids using the deep results on decidability from [GrSe80a, GrSe80b]. Nevertheless, the implementation of the algorithm for general pairs A, B may of course be complicated. Let us pick up and generalize one special case from [BJO99]. In Theorem 17.18 and Corollary 17.21 there, it was proved that if A, B had a special form, and $\lambda_{(A)} = |\det(A)|$ and $\lambda_{(B)} = |\det(B)|$, then the ideal generated by $\langle v(A) \,|\, w(A)\rangle$ in $\mathbb{Z}[1/\det(A)]$ is a complete invariant, if the left and right Perron–Frobenius eigenvectors are taken to have integer components, and $\gcd(v(A)) = 1$, $\gcd(w(A)) = 1$, where gcd denotes the greatest common divisor of the components. We now prove that this is also true for more general matrices A, B.

In stating this more general result, there is a technical complication. In picking extension fields F and an associated ring R of algebraic integers, it is not automatically true that the ideals in R are principal. But by a result in [Wei98] or [Ser79], there is always a finite extension E of F in which the associated ideals are automatically principal. We refer to this in the statement of the proposition. To further simplify the terminology in the statement of the proposition we denote the above-mentioned respective Perron–Frobenius column vectors w, w', i.e., $Aw = \lambda w$ and $Bw' = \lambda' w'$, and similarly v, v' for the two respective Perron–Frobenius row vectors.

Proposition 7.1. *Choose a finite extension E of the algebraic number field F of the eigenvalues of primitive nonsingular integer matrices A, B in which all ideals of F become principal and consider primes in it.*

(i) *An isomorphism J on ordered dimension groups from the dimension group of A to that of B sends the row Perron–Frobenius eigenvector v' (normalized so all entries are algebraic integers with* $\gcd 1$) *of B to a multiple c times the row Perron–Frobenius eigenvector v of A.*

(ii) *The two Perron–Frobenius eigenvalues generate the same algebraic number field and involve the same primes of that field.*
(iii) *Assume that for each non-Perron–Frobenius eigenvalue μ of A or B, the Perron–Frobenius eigenvalue λ is divisible by some algebraic prime not dividing μ. Then the Perron–Frobenius column eigenvector w is mapped to a multiple ξ times the other Perron–Frobenius eigenvector w'.*
(iv) *If λ satisfies the hypothesis in* (iii), *then the latter coefficient ξ factorizes into the primes dividing λ.*
(v) *If λ satisfies the hypothesis in* (iii), *then the former coefficient c factorizes into primes dividing λ. The inner products of left and right Perron–Frobenius eigenvectors are equal modulo normalization: $v'Jw' = cvw' = (c/\xi)\,vJw$. Therefore the inner product of the normalized Perron–Frobenius eigenvectors is an invariant up to units in the algebraic number ring generated by $1/\lambda$.*

Proof. The first assertion is by [BJKR98, Theorem 6], and the second is by [BJKR98, Theorem 10].

The third assertion follows because the space of vectors in the dimension group $G \otimes E$ such that some fixed multiple is arbitrarily divisible by a given algebraic prime is sent to the corresponding subspace of the other dimension group, and this set is the sum of the generalized eigenspaces for all eigenvalues divisible by the prime. If these spaces are intersected over all primes dividing the Perron–Frobenius eigenvalue, we get, by our hypothesis, only the Perron–Frobenius eigenspace.

The fourth assertion follows because the eigenspace of w will consist precisely of those vectors in the dimension group which are divisible by arbitrary powers of primes occurring only in λ, so it must be preserved by any isomorphism of dimension groups. In addition, vectors in this 1-dimensional space which are not divisible by primes other than those in λ will be unique up to multiplication by units and primes dividing λ, so they will be preserved by any isomorphism, up to such multiplication.

Next note that the fourth statement and the first part of the fifth statement are equivalent whenever we have an isomorphism from the dimension group to itself induced by an integer matrix. The reason is that since row and column Perron–Frobenius eigenvectors are preserved, this integer matrix in a basis corresponding to generalized eigenvectors becomes block diagonal, and the block for the Perron–Frobenius eigenvectors must be the same element for the row eigenvectors as for the column eigenvectors, and by (iv) it involves only primes dividing λ.

Now consider integer matrices R and S inducing mappings each way between two different column dimension groups, with Perron–Frobenius eigenvectors v and v' normalized over the algebraic number ring. We have $v \to c_1 v'$ and $v' \to c_2 v$, where c_1 and c_2 are algebraic integers since R and S are integer matrices. But $c_1 c_2 = c$ arises from a map of the dimension group to itself, so it divides a power of λ, hence so do c_1 and c_2. ∎

The following is a partial converse to Proposition 7.1.

Corollary 7.2. *Suppose A, B are nonsingular primitive integer matrices such that their Perron–Frobenius eigenvalues are integers and that the inner products as above are equal, i.e., after normalization, that $\langle v(A) \,|\, w(A) \rangle = \langle v(B) \,|\, w(B) \rangle$, that the primes dividing the Perron–Frobenius eigenvalues are equal, and that the dimensions of the matrices are at least* 3*. Suppose that the Perron–Frobenius eigenvalues* *are the determinants of A, B up to sign. Then there exists an isomorphism between the ordered dimension groups of A and B.*

Proof. By Lemma 17.19 of [BJO99], there is a unimodular matrix J sending the Perron-Frobenius row eigenvector of A to the Perron-Frobenius row eigenvector of B and the Perron-Frobenius column eigenvector of A to the Perron-Frobenius column eigenvector of B (and we can choose signs for positivity). By [BJKR98, Theorem 6] this gives a positive mapping on dimension groups. Since the row eigenvectors are perpendicular to the sum $V(A) = v(A)^{\perp}$ of all non-Perron-Frobenius generalized eigenspaces, $JV(A) = V(B)$, and also $v(B)J \subseteq \mathbb{Q}v(A)$ as noted in Section 1. Write any vector v as a direct sum according to (1.20), $v = x + y$. This splitting can introduce certain fixed primes p in the denominator.

Note that the matrix A is unimodular and integer restricted to the integer vectors in $V(A)$ (and similarly for the matrix B), because each determinant is the product of its determinant on this space and its determinant on the Perron–Frobenius eigenspace, and because it is an integer matrix preserving this subspace. Multiplication by A is multiplication by λ on x (see Figure 1), and the same is true for B.

$$A \sim \begin{array}{c} \begin{array}{cc} \qquad V(A) \qquad\qquad & \qquad \mathbb{C}w(A) \end{array} \\ \left(\begin{array}{ccc|c} * & \cdots & * & 0 \\ \vdots & \begin{array}{c} A|_{V(A)} \\ \text{with} \\ \left|\det\left(A|_{V(A)}\right)\right| = 1 \end{array} & \vdots & \vdots \\ * & \cdots & * & 0 \\ \hline 0 & \cdots & 0 & \begin{array}{c} \lambda_{(A)} \\ = \left|\det A\right| \end{array} \end{array}\right) \end{array} \begin{array}{l} V(A) \\ \\ \mathbb{C}w(A) \end{array}$$

FIGURE 1. The case $|\det A| = \lambda_{(A)}$: Decomposition relative to (1.20) and unimodular restriction.

For v to be in the dimension group means for all sufficiently large n, $A^n v$ has integer entries. Any prime p which does not divide λ will not occur in the denominator of the expression $B^m JA^{-n}(x + y)$.

Consider those primes p which divide λ. We claim that they cannot occur in denominators of y. Restricted to vectors y, the matrix A is unimodular, so modulo any powers of those primes it lies in a finite group, $\mathrm{GL}(N, \mathbb{Z}_{p^s})$. Thus we can choose arbitrarily large n so that A^n is congruent to the identity. But then in $A^n(x + y)$, the denominators in x have vanished, being multiplied by λ^n and those in y remain. So $x + y$ is not in the dimension group, a contradiction.

Therefore in

$$\begin{aligned} B^m JA^{-n}(x + y) &= B^m JA^{-n}x + B^m JA^{-n}y \\ &= J\lambda'^m \lambda^{-n} x + B^m JA^{-n}y \end{aligned} \tag{7.1}$$

both terms are integer for sufficiently large m (with a symmetrical argument the other way) which verifies the conditions in Section 1 for isomorphism of ordered dimension groups. □

8. The case of no infinitesimal elements and the case of rational eigenvalues

In this section we will consider the C^*-equivalence problem in two extreme cases. To describe these two cases, let us recall some facts from [Eff81], [BJO99]. We define a functional τ_A on $G(A)$ by the formula

$$\tau_A(g) = \langle v(A) \mid g \rangle, \qquad g \in G(A), \tag{8.1}$$

where $v(A)$ is a left Perron–Frobenius eigenvector for A. This functional τ_A is called "the" trace since it defines a trace on the corresponding C^*-algebra. It follows from the eigenvalue equation that $v(A)$ can be taken to have components in the field $\mathbb{Q}[\lambda] = \mathbb{Q}[1/\lambda]$, where λ is the Perron–Frobenius eigenvalue. But multiplying $v(A)$ by a positive integer, we may assume that the components of $v(A)$ are contained in the ring $\mathbb{Z}[1/\lambda]$. It then follows from (1.8), and $v(A) A^{-n} = \lambda^{-n} v(A)$, that

$$\tau_A(G(A)) \subset \mathbb{Z}[1/\lambda]. \tag{8.2}$$

Furthermore, $\tau_A(G(A))$ is invariant under multiplication by elements of $\mathbb{Z}$ and by $1/\lambda$, so it is a $\mathbb{Z}[1/\lambda]$-module. In particular, $\tau_A(G(A))$ is an ideal in the ring $\mathbb{Z}[1/\lambda]$. We need only verify that $\frac{1}{\lambda}\tau_A(g)$ is in $\operatorname{ran}(\tau_A)$ for all $g \in G(A)$, where $\operatorname{ran}(\tau_A)$ denotes the range of the trace functional τ_A, i.e., the subgroup $\tau_A(G(A))$ from (8.2). Pick $g \in G(A)$, and set $g = A^{-n}m$, $n \in \mathbb{Z}_+$, $m \in \mathbb{Z}^N$. Then $\frac{1}{\lambda}\tau_A(g) = \left\langle v(A) A^{-1} \,\middle|\, g \right\rangle = \left\langle v(A) \,\middle|\, A^{-1} g \right\rangle = \tau_A\left(A^{-(n+1)}m\right) \in \operatorname{ran}(\tau_A)$ as claimed. This is a very special feature of the constant-incidence-matrix situation which is not shared by the range of a trace on a general dimension group of general AF-algebras. This range is not even closed under multiplication in the general case when the incidence matrix is not assumed constant. We have the natural short exact sequence of groups

$$0 \longrightarrow \ker(\tau_A) \hookrightarrow G(A) \xrightarrow{\tau_A} \tau_A(G(A)) \longrightarrow 0 \tag{8.3}$$

and the order isomorphism

$$G(A) / \ker(\tau_A) \underset{\approx}{\xrightarrow{\tau_A}} \operatorname{ran}(\tau_A) \subset \mathbb{Z}\left[1/\lambda_{(A)}\right], \tag{8.4}$$

where $\operatorname{ran}(\tau_A)$ inherits the natural order from $\mathbb{Z}[1/\lambda]$. Note that for the particular matrices we considered in [BJO99], we had

$$\operatorname{ran}(\tau_A) = \mathbb{Z}[1/\lambda] \tag{8.5}$$

(see [BJO99, (5.21)–(5.22)]), but be warned that this is not a general feature. This will be discussed further in Remarks 9.5 and 9.7. Chapter 5 in [BMT87] also has a nice treatment of $\operatorname{ran}(\tau_A)$ in the general case. Let us already at this point state and prove the remarkable fact that *any* subset I of $\mathbb{Q}[\lambda]$ which is an ideal over $\mathbb{Z}[1/\lambda]$ occurs as the image of the trace for a suitable primitive nonsingular matrix A (this is a version of [BMT87, Corollary 5.15] which is a consequence of results of Handelman, see [Han81] and [Han87]):

Proposition 8.1. *Let λ be a real algebraic integer larger than the absolute value of any of its conjugates, and let $I \subset \mathbb{Q}[\lambda]$ be an ideal over $\mathbb{Z}[1/\lambda]$. Then I can occur as the image of the trace for some matrix whose Perron–Frobenius eigenvalue is a power of λ (the size of the matrix will be the degree $\mathbb{Q}[\lambda]/\mathbb{Q}$).*

Proof. Let $I_1 = I \cap \mathbb{Z}[\lambda]$; it will be a $\mathbb{Z}[\lambda]$-ideal which spans I over $\mathbb{Z}[1/\lambda]$.

Now define an integer matrix M which expresses the action of λ on I_2, that is, form an additive basis w_i for I_1, let $\lambda w_i = \sum_j m_{ij} w_j$, $m_{ij} \in \mathbb{Z}$. This matrix will have an eigenvalue λ, and we claim that at the corresponding eigenspace, the image of the trace is isomorphic to I. This is because the action of M on $\mathbb{Z}^N$ has been forced to be that of λ on I_1, and because the trace reflects this module structure, by means of the short (nearly exact) sequence.

Finally we claim that we can conjugate M over $\mathrm{GL}(N, \mathbb{Z})$ to a matrix whose powers are eventually positive; then those powers will be nonnegative matrices whose image of trace is the same. To get eventual positivity, given that λ is the largest eigenvalue (the largest of its Galois conjugates), it is necessary and sufficient that its row and column eigenvectors for this eigenvalue be positive, by a limit argument somewhat like that in Proposition 1.1. Let v, w be row and column eigenvectors at the eigenvalue λ, with signs chosen so that their inner product is positive. Multiply each by a large integer, and then take relatively prime integers approximating its components. Such a pair of vectors can be mapped over $\mathrm{GL}(N, \mathbb{Z})$ to any vectors whose entries are relatively prime integers having the same inner product, by [BJO99, Lemma 17.19], in particular, to ones which are positive, if $N > 2$. If $N = 2$ we use the same result and get a congruence condition, but that is compatible with positivity. $\square$

Remark 8.2. The quotient of the ring $\mathbb{Z}[1/\lambda]$ by any of these ideals will be finite. The ideal can be lifted to an ideal inside the rank-N additive group $\mathbb{Z}[\lambda]$, and the quotient of two rank-N free abelian groups is finite—its order is given by the determinant of the map expressing the inclusion.

Let us return to the two special cases of C^*-equivalence we shall discuss in this section. These are the following.

(i) The kernel $\ker(\tau_A)$ is 0, i.e., $G(A)$ has no infinitesimal elements, i.e., the characteristic polynomial of A is irreducible over $\mathbb{Z}$ (equivalent: over $\mathbb{Q}$).
(ii) All the eigenvalues of A are rational (thus integer), each of them is relatively prime to the rest, and none is equal to ± 1.

In Sections 9 and 12 we will apply this to many examples. See, for example, Example 9.9 for an application in the situation (ii) above.

Theorem 8.3. *Two primitive $N \times N$ matrices A, B over $\mathbb{Z}_+$ with irreducible characteristic polynomials are C^*-equivalent if and only if the following three conditions all hold:*

(i) *the roots of their characteristic polynomials generate the same field,*
(ii) *their Perron–Frobenius eigenvalues are divisible by the same algebraic primes, and*
(iii) *their dimension groups, as modules over $\mathbb{Z}[1/\lambda]$ (or a full-rank subring), are isomorphic. These modules are isomorphic to the fractional ideals given by the image of the trace τ.*

Moreover, these three conditions are equivalent to the one condition:

(iv) *the two ordered additive subgroups in $\mathbb{Z}[1/\lambda]$ defined by the ranges of the respective traces are isomorphic.*

If in addition the characteristic polynomials of A, B are equal, then C^*-equivalence (isomorphism of ordered dimension groups) is the same as shift equivalence.

Note that taking powers of the matrix will preserve the $\mathbb{Z}[1/\lambda]$-module mentioned in (iii), *i.e., the ideal in $\mathbb{Z}[1/\lambda]$, and not replace it by its powers.*

Remark 8.4. To say that the dimension groups $G(A)$ and $G(B)$ as modules over $\mathbb{Z}[1/\lambda]$ are isomorphic means that there is an isomorphism $\varphi\colon G(A) \to G(B)$ of abelian groups such that

$$\varphi(\omega g) = \omega\varphi(g) \tag{8.6}$$

for all $g \in G(A)$, $\omega \in \mathbb{Z}[1/\lambda]$. This is not the same as saying that $G(A)$ is isomorphic to $G(B)$ as ideals in $\mathbb{Z}[1/\lambda]$. The latter concept means that there is an automorphism φ of the ring $\mathbb{Z}[1/\lambda]$ such that $\varphi(G(A)) = G(B)$. When we talk about equivalence of ideals it is the *first* concept we are thinking about, i.e., there is an element of the quotient field $\mathbb{Q}[1/\lambda] = \mathbb{Q}[\lambda]$ mapping the one ideal into the other by multiplication.

Proof of Theorem 8.3. The first three statements are a reformulation of [BJKR98, Proposition 10], except for the relationship with the trace, which we next show. The definition (8.1), properties (1.8), (1.10), and

$$t_A \circ A^{-1} = \lambda^{-1}\tau_A$$

imply that the image of the trace is a module over $\mathbb{Z}[1/\lambda]$ and a subset of $\mathbb{Z}[1/\lambda]$. Using the standard basis for $\mathbb{Z}^N$, it is generated by $\langle v \mid e_i = v_i\rangle$ as a module over $\mathbb{Z}[1/\lambda]$ since $A^{-n}e_i$, $n \in \mathbb{Z}_+$ generate the dimension group. The trace mapping is an epimorphism if we pass to rational coefficients (that is, tensor dimension groups with $\mathbb{Q}$), just because its image is nonzero (consider v as a Perron–Frobenius column eigenvector) and closed under field operations in $\mathbb{Q}[1/\lambda]$. Its kernel is zero since the dimension group with rational coefficients is also a 1-dimensional vector space over $\mathbb{Q}[1/\lambda]$ (for instance, by [BMT87, Chapter 5]). Thus the trace mapping is an isomorphism to its image as asserted in the second part of (iii).

A theorem of Handelman (stated as Theorem 5.2 in [BMT87]) in fact allows us to replace the condition in Theorem 8.3 above that A and B be nonnegative with the condition that instead they are *integral eventual positive* (IEP), i.e., that they are in $M_N(\mathbb{Z})$ and have respective powers with strictly positive entries.

Next we show that dimension group isomorphism in our sense implies shift equivalence if the irreducible characteristic polynomials of A, B are equal. The only difference with the isomorphisms used in [BMT87, Theorem 2.8] is that there the actions of A, B are the same, that is, the matrices themselves represent the field element acting on this module. But the field element A, B represent are roots of the same irreducible characteristic polynomials, and are the unique Perron–Frobenius roots of these polynomials so they must be the same field element.

Equivalence to (iv): (iv) is, properly understood, a rephrasing of (iii), given the isomorphism in the first paragraph of the proof. We will clarify the kind of module structure which is involved. Assuming (iv), the images of the traces generate the fields $\mathbb{Q}[\lambda_{(A)}] = \mathbb{Q}[\lambda_{(B)}]$, but the rings $\mathbb{Z}[\lambda_{(A)}]$ and $\mathbb{Z}[\lambda_{(B)}]$ may be different, in which case we work with the full-rank subring $\mathbb{Z}[\lambda_{(A)}] \cap \mathbb{Z}[\lambda_{(B)}]$. Condition (i) is immediate, and condition (ii) follows since algebraic primes dividing λ are those primes which can divide elements of the dimension groups to arbitrary powers.

Conversely, suppose we are given (i), (ii), (iii). The equality of fields asserted in [BJKR98, Proposition 10] is taken in the sense of "equality of $\mathbb{Q}[\lambda_{(A)}]$ and $\mathbb{Q}[\lambda_{(B)}]$ as subfields of the real numbers", which gives embeddings of $\mathbb{Z}[\lambda_{(A)}]$ and $\mathbb{Z}[\lambda_{(B)}]$ into the real numbers. Thus it also embeds the modules which can be considered as subsets of $\mathbb{Q}[\lambda_{(B)}]$. The isomorphism of modules as additive groups acted on multiplicatively (i.e., the action $y \mapsto xy$) by subrings of $\mathbb{Q}[\lambda_{(A)}]$ having full rank (in this case N) means there is some element of the quotient field mapping one to the other: if the isomorphism of (iii) maps some element y to z (considered as images in the real numbers) then the ratio y/z is independent of the choice of y by definition of the isomorphism in (iii), and we multiply by this ratio to get the isomorphism in (iv). □

Note that this applies in particular to Example 9.8 below.

Theorem 8.5. *Let A and B be matrices over $\mathbb{Z}_+$, all of whose eigenvalues are rational, and each of which is divisible by some prime not dividing the other eigenvalues. Assume further that A and B have the same characteristic polynomial. Let E_a and E_b be their matrices of column eigenvectors normalized to be integer vectors having greatest common divisor 1. Let D be a diagonal matrix whose entries involve only powers of primes in the respective eigenvalues, let D_s be a diagonal matrix consisting of precisely the diagonal eigenvalues. Then the following are equivalent:*

(i) *A and B are C^*-equivalent;*
(ii) *A and B are shift equivalent, as follows: for some choice of signs in E_a, E_b, and some choice of D, and for all sufficiently large n, $E_a D D_s^n E_b^{-1}$ and $E_b D^{-1} D_s^n E_a^{-1}$ are integer matrices.*

Proof. Consider an isomorphism of dimension groups. The eigenvectors generate the 1-dimensional spaces of vectors such that some multiples of those vectors are in the dimension group and are divisible by arbitrary powers of the respective eigenvalues. Hence any dimension group isomorphism must preserve those subspaces. Moreover, we claim that a dimension group isomorphism must send normalized eigenvectors to normalized eigenvectors of the image. The rational multiples of a normalized eigenvector v with rational eigenvalue η which lie in the dimension group are the elements of $M_v = \{(n/m)v \mid n \in \mathbb{Z},\ \exists\, k \in \mathbb{Z}_+, m|\eta^k\}$: a vector $w \in M_v$ lies in the dimension group $G(A)$, since w is a multiple of an integer vector by negative powers of A, B. And if $w = (n/m)v \in G(A)$ then there is a $k \in \mathbb{Z}$ such that $A^k v = \eta^k v \in \mathbb{Z}^N$, so that $m|\eta^k$ in lowest terms, $w \in M_v$. It follows that dimension group isomorphism implies the existence of an isomorphism of $\mathbb{Q}^N$ which sends each eigenvector to a multiple of the other eigenvector by a number which divides a power of η. Such a mapping must preserve the action of multiplication by A, given that the characteristic polynomials are equal, because this multiplies each eigenvector by its eigenvalue, and the eigenvalues are the same. So the mapping will be a shift equivalence. Let D be the diagonal matrix whose main diagonal entries are the multiples just mentioned. Then the isomorphism J of dimension groups will be, specifically, $E_b(E_a D)^{-1}$ if it exists. For if we multiply J and its inverse on the left by a large enough power of A or B, respectively, as in (1.17), we see that the resulting matrix products must be integer matrices. Moreover, these multiples are the matrices stated in the theorem. □

9. The transpose map and C^*-symmetry

In this section we will study the behavior of the dimension group $\left(G(A), G(A)_+\right)$ under the transpose map $A \to A^{\mathrm{tr}}$. In particular, we say that A is C^*-symmetric if A is C^*-equivalent to A^{tr}, i.e., $G(A)$ and $G(A^{\mathrm{tr}})$ are isomorphic as ordered groups. We give several examples showing that A may be C^*-symmetric, (9.3), Remark 9.5, or not, Example 9.6 (2×2 matrices with rational eigenvalues), Example 9.8 (2×2 matrices with irrational eigenvalues) and Example 9.9. An interesting feature with these particular examples is that when A is a 2×2 matrix, then C^*-symmetry is equivalent to shift-symmetry (i.e., A and A^{tr} are shift equivalent). For 2×2 matrices, symmetry seems to be more common than non-symmetry. Our first example, while very simple, illustrates both C^*-symmetry and a nontrivial Ext-element. It has $\lambda = \lambda_{(A)} = 2$. The Ext-group represents another contrast between the two cases, λ rational (and hence integral), and the characteristic polynomial irreducible. In the first case, we generally have $\ker(\tau_A) \neq 0$, and as we note in Remark 9.5, $\operatorname{ran}(\tau_A) = \mathbb{Z}[1/\lambda]$. Hence this extra extension structure for $G(A)$ arises only in the reducible case: The corresponding short exact sequence

$$0 \longrightarrow \ker(\tau_A) \longrightarrow G(A) \xrightarrow{\tau_A} \mathbb{Z}[1/\lambda] \longrightarrow 0 \tag{9.1}$$

may be non-split, which means that $G(A)$ is then not the direct sum of the two groups $\ker(\tau_A)$ and $\mathbb{Z}[1/\lambda]$.

Recall that for groups R and S, $\operatorname{Ext}(R, S)$ is again a group. Elements in $\operatorname{Ext}(R, S)$ are equivalence classes of short exact sequences

$$0 \longrightarrow S \longrightarrow E \xrightarrow{\psi} R \longrightarrow 0, \tag{9.2}$$

see [CaEi56], [BJO99, p. 62], and there are natural operations

$$E \longmapsto -E$$

and

$$E, E' \longmapsto E + E'$$

on $\operatorname{Ext}(R, S)$ which turn it into a group. We say that (9.2) splits if there is some $\varphi \in \operatorname{Hom}(R, E)$ such that $\psi \circ \varphi = \mathrm{id}_R$. Then (9.2) splits if and only if it represents the zero element in $\operatorname{Ext}(R, S)$. For example,

$$\operatorname{Ext}(\mathbb{Z}_2, \mathbb{Z}) \cong \mathbb{Z}_2,$$

where the non-split Ext-element is represented by

$$0 \longrightarrow 2\mathbb{Z} \longrightarrow \mathbb{Z} \xrightarrow{\mathrm{proj}} \mathbb{Z}_2 \longrightarrow 0$$

and the zero element is represented by

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Z} \oplus \mathbb{Z}_2 \xrightarrow{0 \oplus \mathrm{id}} \mathbb{Z}_2 \longrightarrow 0.$$

The next example illustrates how nontrivial Ext-elements are part of the invariant structure for the dimension groups.

Example 9.1. The dimension group defined by A may be order isomorphic to that defined by its transpose $B = A^{\mathrm{tr}}$. Hence an AF-C^*-algebra built on such a matrix A (i.e., from the corresponding stationary Bratteli diagram) has a nontrivial period-two symmetry corresponding to $A \mapsto A^{\mathrm{tr}}$. An example here is

$$A = \begin{pmatrix} 1 & 1 \\ 2 & 0 \end{pmatrix}, \qquad A^{\mathrm{tr}} = \begin{pmatrix} 1 & 2 \\ 1 & 0 \end{pmatrix}. \tag{9.3}$$

In this case A and A^{tr} have eigenvalues 2 and -1, and both of the dimension groups G and G^{tr} are in $\operatorname{Ext}(\mathbb{Z}[1/2], \mathbb{Z})$. It can be checked (by use of [BJO99, Corollary

11.28]) that this Ext-element is not zero. Here $\ker(\tau) = \mathbb{Z}$, $\operatorname{ran}(\tau) = \mathbb{Z}[1/2]$, and the corresponding short exact sequence

$$0 \longrightarrow \mathbb{Z} \longrightarrow G(A) \xrightarrow{\tau} \mathbb{Z}[1/2] \longrightarrow 0 \tag{9.4}$$

does not split, i.e., it is not the zero element in Ext. Equivalently, $G(A)$ is not $\mathbb{Z} \oplus \mathbb{Z}[1/2]$ as a group. If it were, we would get $\tau(w)^{-1} \in \mathbb{Z}[1/2]$ by [BJO99, Corollary 11.28]. But we computed $\tau(w) = 3$, and $1/3$ is not in $\mathbb{Z}[1/2]$. Since $\lambda_{(A)} = 2 = |\det A|$, it is tempting to apply Theorem 7.2. In fact the inner-product invariants are $\langle v \,|\, w\rangle = \begin{pmatrix} 2 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = 3$, and $\langle v' \,|\, w'\rangle = \begin{pmatrix} 1 & 1 \end{pmatrix} \begin{pmatrix} 2 \\ 1 \end{pmatrix} = 3$. But since the dimension is 2 (< 3), Theorem 7.2 does not apply directly, and instead we will verify directly that A and A^{tr} are C^*-equivalent. Define matrices J, K by

$$J = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \qquad K = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}. \tag{9.5}$$

One verifies that

$$A = KJ, \qquad A^{\mathrm{tr}} = JK. \tag{9.6}$$

Thus A and A^{tr} are elementary shift equivalent, and it follows that they are shift equivalent and C^*-equivalent (see the discussion in [BJKR98]).

However, we will see in Examples 9.9 and 12.4 that this is not a general feature of the transpose map.

We may analyze the C^*-symmetry question by dimension-group analysis: If we show that the ordered group $G(A)$ is order isomorphic to $G(A^{\mathrm{tr}})$, then A is C^*-equivalent to A^{tr}, i.e., A is C^*-symmetric. Clearly then the two groups $G(A)$ and $\operatorname{ran}(\tau_A)$ are order isomorphic whenever $\ker(\tau_A) = 0$, and we have the result:

Proposition 9.2. *Let $A \in M_N(\mathbb{Z})$ be nonsingular and primitive, and suppose its characteristic polynomial $p_{(A)}(x)$ is irreducible, and $\operatorname{ran}(\tau_A) = \operatorname{ran}(\tau_{A^{\mathrm{tr}}})$: then A is C^*-equivalent to A^{tr}. Note in particular that this holds if:*

(i) $N = 2$,
(ii) *the Perron–Frobenius eigenvalue $\lambda_{(A)}$ is irrational, and*
(iii) $\operatorname{ran}(\tau_A) = \operatorname{ran}(\tau_{A^{\mathrm{tr}}})$.

Proof. This follows directly from Theorem 8.3. □

Remark 9.3. We saw that by scaling out denominators in the entries v_i of the left (row) Perron–Frobenius eigenvector $v(A) = (v_1, \dots, v_N)$ we can arrange that $v_i \in \mathbb{Z}[1/\lambda]$ for all i. But then a further scaling with a power of λ we can get each v_i in the subring $\mathbb{Z}[\lambda] \subset \mathbb{Z}[1/\lambda]$. Suppose that the characteristic polynomial of A is irreducible. Note that, as a group, $\mathbb{Z}[\lambda]$ is then a copy of the lattice $\mathbb{Z}^N$ so the entries v_i may therefore be viewed as vectors in $\mathbb{Z}^N$. Then pick $v(A)$ such that $\gcd(v_i) = 1$ for each i. In this case the matrix V with the v_i's as rows is in $M_N(\mathbb{Z})$ and is nonsingular. If we could define greatest common divisors in the ring $\mathbb{Z}[\lambda]$ then we could divide v by this greatest common divisor and obtain some new v defined over $\mathbb{Z}[\lambda]$ which has g.c.d. 1. Then the image of its trace would contain the span of its coordinates v_i over $\mathbb{Z}[\lambda]$, that is, the entire ring $\mathbb{Z}[\lambda]$. Moreover the image of the trace will be contained in this ring, so they are equal. In general, however, this ring will not be a principal ideal domain, so that the class of the ideal generated by the trace becomes an obstruction. In fact, the subgroup in $\mathbb{Z}[\lambda]$ which is generated by the v_i's is also an ideal in $\mathbb{Z}[\lambda]$. Indeed, for $m \in \mathbb{Z}^N$, $\sum_i m_i v_i = \tau(m) = \langle v \mid m \rangle$, so $\lambda \sum_i m_i v_i = \langle vA \mid m \rangle = \langle v \mid A^{\mathrm{tr}} m \rangle$, and $A^{\mathrm{tr}} m \in \mathbb{Z}^N$. As a consequence, we get that the special incidence matrices A which we considered in [BJO99] satisfy the condition $\operatorname{ran}(\tau_A) = \mathbb{Z}\left[1/\lambda_{(A)}\right]$. However, this fails for the matrix A from Example 9.8, and others. The group $\tau\left(\mathbb{Z}^N\right)$ is contained in $\tau(G) = \operatorname{ran}(\tau_A)$ and the following proposition indicates their relationship.

Proposition 9.4. *Assume that the Perron–Frobenius row eigenvector v is chosen to lie in $\mathbb{Z}^N[\lambda]$. Then the map induced by the inclusion $\mathbb{Z}[\lambda]/\tau\left(\mathbb{Z}^N\right) \to \mathbb{Z}[1/\lambda]/\tau(G)$ is an epimorphism with kernel precisely*

$$\left\{x \in \mathbb{Z}[\lambda]/\tau\left(\mathbb{Z}^N\right) \mid \exists m \in \mathbb{Z},\ \lambda^m x = 0\right\}.$$

Proof. Assuming, as we will show, that the image consists of torsion elements relatively prime to λ, the inclusion gives a natural mapping. If we multiply any element in $\mathbb{Z}[1/\lambda]$ by a power of power of λ, we can get an element of $\mathbb{Z}[\lambda]$, so this mapping is an epimorphism. We also claim that if we multiply any element of $\tau(G)$, say $vA^{-n}x$, $x \in \mathbb{Z}^N$ by a power of λ, we will get an element of $\tau\left(\mathbb{Z}^N\right)$. This is because $vA^{-n}x = v\lambda^{-n}x$ using the left two factors.

Note that since $\tau(G)$ and $\mathbb{Z}[1/\lambda]$ are both torsion-free and λ-divisible, their quotient has no λ-torsion. Hence every element annihilated by a power of λ lies in the kernel. (We will show that the image consists of torsion elements relatively prime to λ.)

Let y be in the kernel of this mapping. Then $y \in \tau(G)$, so that for some $n \in \mathbb{Z}_+$, $\lambda^n y \in \tau\left(\mathbb{Z}^N\right)$ and is zero in the original group. This identifies the quotient. The left hand group, the quotient of a free abelian group by a full-rank subgroup, is finite, so some fixed n works for the whole kernel. ☐

Remark 9.5 (Rational λ)**.** Even if $N = 2$, the dimension group $G(A)$ is not yet completely understood [BJO99] (perhaps far from it; see, however, [Han87]). If $\lambda = \lambda_{(A)}$ is rational, and therefore an integer, we can have nonisomorphic $G(A_1)$ and $G(A_2)$ even when A_1 and A_2 have the same characteristic polynomial and thus the same Perron–Frobenius eigenvalue λ, as different extensions, $i = 1, 2$,

$$0 \longrightarrow \mathbb{Z}[1/\mu] \hookrightarrow G(A_i) \xrightarrow{\tau} \mathbb{Z}[1/\lambda] \longrightarrow 0, \tag{9.7}$$

i.e., as different elements of the group $\operatorname{Ext}(\mathbb{Z}[1/\lambda], \mathbb{Z}[1/\mu])$. Here μ is the other root of the characteristic polynomial, so μ is a nonzero integer with $|\mu| < \lambda$. See (8.3) and (8.4). This may even happen when A_2 is the transpose of the matrix A_1, by Example 9.6 below. Since here λ is rational one may arrange that $\tau_A(G(A)) = \mathbb{Z}[1/\lambda]$ by choosing v with $\gcd(v) = 1$, and $\ker(\tau_A)$ is a rank-1 nonzero group isomorphic to $\mathbb{Z}[1/\mu]$; see also below. There are specimens of 2×2 primitive matrices A, even with integral Perron–Frobenius eigenvalue such that $\lambda_{(A)} < |\det A|$, and yet the two groups $G(A)$ and $G(A^{\mathrm{tr}})$ are order isomorphic. For example, $A = \left(\begin{smallmatrix} 1 & 5 \\ 3 & 3 \end{smallmatrix}\right)$ has that property. To see this, we may use (1.16)–(1.17). Since $J = \left(\begin{smallmatrix} 1 & 2 \\ 2 & 3 \end{smallmatrix}\right)$ satisfies $JA = A^{\mathrm{tr}} J$, the two conditions hold, and hence the matrix A is C^*-symmetric. So for this particular pair A, A^{tr}, the respective groups $G(A)$ and $G(A^{\mathrm{tr}})$ from the middle term in the diagram (9.7) will then in fact represent the same zero element of $\operatorname{Ext}(\mathbb{Z}[1/6], \mathbb{Z}[1/2])$. For this particular A,

$$G(A) \cong \mathbb{Z}[1/2] \oplus \mathbb{Z}[1/6] \qquad (\ker(\tau) \cong \mathbb{Z}[1/2]) \tag{9.8}$$

as direct sum of abelian groups. For this, note that the integral column eigenvectors for A are $\left(\begin{smallmatrix}1\\1\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}5\\-3\end{smallmatrix}\right)$. Since $\det\left(\begin{smallmatrix}1 & 5\\1 & -3\end{smallmatrix}\right) = -8 = -2^3$ and the eigenvalues of A are $6 = 2\cdot 3$ and -2, we have $\mathbb{Z}\left[1/2\right]^2 \subset G(A)$. Thus $G(A) = \bigcup_{n=0}^{\infty} A^{-n}(\mathbb{Z}\left[1/2\right]^2)$, and (9.8) follows. Specifically, the representation (9.8) may be derived from (1.20), (8.1), and the two identities

$$\ker(\tau_A) = V(A) \cap G(A) = \mathbb{Z}\left[1/2\right]\begin{pmatrix}5\\-3\end{pmatrix} \tag{9.9}$$

and

$$G(A) \cap \mathbb{C}w(A) = \mathbb{Z}\left[1/6\right] w(A), \tag{9.10}$$

where $w(A) = \left(\begin{smallmatrix}1\\1\end{smallmatrix}\right)$. The present computation of $G(A)$ is simplified by the fact that the orthogonal complement of the trace vector $v(A) = \left(\begin{smallmatrix}3, & 5\end{smallmatrix}\right)$ is spanned by the nonmaximal column eigenvector. Here $\lambda_{(A)} = 6$, and so $\mathbb{Z}\left[\lambda_{(A)}\right] = \mathbb{Z}$. That $\tau(G(A)) = \mathbb{Z}\left[1/6\right]$ in this case follows from Remark 9.3 and the general observation that with our choice of $v(A)$, we will have $\tau(G(A)) = \mathbb{Z}\left[1/\lambda_{(A)}\right]$ provided the ideal in $\mathbb{Z}\left[\lambda_{(A)}\right]$ generated by the $v_i(A)$ entries is principal. Ideals in $\mathbb{Z}$ are principal, of course. Here in this case the Ext-element corresponding to $G(A)$ is trivial. (Looking at prime factors in $\det A$, one could also get a $G(A)$ which is non-split. For example, taking $A = \left(\begin{smallmatrix}1 & 6\\2 & 2\end{smallmatrix}\right)$, we get the spectrum $\{5, -2\}$ and that the corresponding dimension group $G(A)$ is here represented by a nonzero element of $\operatorname{Ext}(\mathbb{Z}\left[1/5\right], \mathbb{Z}\left[1/2\right])$. The analysis here is analogous to that presented above: We get $\ker(\tau_A) \cong \mathbb{Z}\left[1/2\right]$, $\operatorname{ran}(\tau_A) \cong \mathbb{Z}\left[1/5\right]$, and the corresponding short exact sequence

$$0 \longrightarrow \mathbb{Z}\left[1/2\right] \longrightarrow G(A) \longrightarrow \mathbb{Z}\left[1/5\right] \longrightarrow 0 \tag{9.11}$$

is now non-split. The example $A = \left(\begin{smallmatrix}1 & 6\\2 & 2\end{smallmatrix}\right)$ is C^*-symmetric, as A and A^{tr} are in fact shift equivalent: Take $R = \left(\begin{smallmatrix}-1 & 2\\2 & -2\end{smallmatrix}\right)$ and $S = \left(\begin{smallmatrix}7 & 4\\4 & 3\end{smallmatrix}\right)$. Then $RS = A^{\mathrm{tr}}$ and $SR = A$. It follows from [BJO99] that $G(A)$, when represented in the Ext-group, is generally not the zero element.)

Example 9.6. Here we will exhibit a primitive nonsingular 2×2 matrix A with rational eigenvalues such that A is not C^*-equivalent to A^{tr} (and thus is not shift equivalent to A^{tr}). The respective dimension groups $G(A)$ and $G(A^{\mathrm{tr}})$ are not even isomorphic as groups, let alone order isomorphic, and hence this A in (9.12) is "more" nonsymmetric than the corresponding specimen (9.15) in Example 9.8. The example is

$$A = \begin{pmatrix}65 & 7\\24 & 67\end{pmatrix}. \tag{9.12}$$

Putting

$$E_A = \begin{pmatrix}-7 & 1\\12 & 2\end{pmatrix}, \qquad E_B = \begin{pmatrix}-2 & 12\\1 & 7\end{pmatrix}, \qquad D = \begin{pmatrix}53 & 0\\0 & 79\end{pmatrix}, \tag{9.13}$$

we have

$$A = E_A D E_A^{-1}, \qquad B = A^{\mathrm{tr}} = E_B D E_B^{-1}. \tag{9.14}$$

The eigenvalues of A and B are 53 and 79, which are both prime and congruent to $-1 \mod 13$. Using Theorem 8.5 it follows that if A and B were C^*-equivalent there would exist some diagonal matrix $D_0 = \left(\begin{smallmatrix}x & 0\\0 & y\end{smallmatrix}\right)$ where x, y are congruent to $\pm 1 \mod 13$ such that $E_A D_0 E_B^{-1}$ would have integral entries. But the $(1,1)$ entry of this matrix is $(49x+y)/26$. If this is an integer, and $x=\varepsilon_1+n_1\cdot 13$, $y=\varepsilon_2+n_2\cdot 13$, where n_1, n_2 are integers and $\varepsilon_i=\pm 1$, then $\frac{1}{13}(49x+y)=\frac{1}{13}((4\cdot 13-3)x+y)=-\varepsilon_1\frac{3}{13}+\varepsilon_2\frac{1}{13} \mod 1$, but this can never be an integer. Thus A is not C^*-symmetric.

Remark 9.7 (Irrational λ)**.** The assumption in Proposition 9.2 that the range of the respective traces τ_A and $\tau_{A^{\mathrm{tr}}}$ be the same (viewed as subgroups of $\mathbb{Z}\left[1/\lambda_{(A)}\right]$) cannot be omitted. It is true in general that $\operatorname{ran}(\tau_A)$ is an ideal in $\mathbb{Z}\left[1/\lambda_{(A)}\right]$, but the ideal may be proper, and it may be different from one to the other. An example showing this to be the case can be found in [BMT87, p. 104], [PaTu82, pp. 79–83]. The example is a matrix A such that A and its transpose $B=A^{\mathrm{tr}}$ are not shift equivalent. We will give another example of this, and then apply Theorem 8.3 to show that they are not C^*-equivalent either:

Example 9.8. The example is $A=\left(\begin{smallmatrix}19&5\\4&1\end{smallmatrix}\right)$. Here $\lambda=10+\sqrt{101}$, so the characteristic polynomial is irreducible and therefore $\ker(\tau_A)=0$. Since $\det A=-1$, the unordered dimension groups $G(A)$ and $G(A^{\mathrm{tr}})$ are both $\mathbb{Z}^2$. However, we will show that they are not order isomorphic. We have

$$A=\begin{pmatrix}19&5\\4&1\end{pmatrix},\qquad B=A^{\mathrm{tr}}=\begin{pmatrix}19&4\\5&1\end{pmatrix}. \tag{9.15}$$

We prove that the two ideals $\operatorname{ran}(\tau_A)$ and $\operatorname{ran}(\tau_{A^{\mathrm{tr}}})$ are nonisomorphic. The eigenvalues are $10\pm\sqrt{101}$. Let $\omega=(1+\sqrt{101})/2$ so that $1,\omega$ form a $\mathbb{Z}$-basis for the algebraic integers in $\mathbb{Q}(\sqrt{101})$. (The fact that all algebraic integers in a quadratic field have this form is [Wei98, Theorem 6-1-1, p. 234]. One can check that 1, ω are algebraic integers, then that the trace must be an algebraic integer, and see what happens when we subtract some $a+b\omega$ to simplify, in terms of the norm being an algebraic integer.) The respective (column) eigenvectors for A, A^{tr} are

$$\begin{pmatrix}4+\omega\\2\end{pmatrix},\ \begin{pmatrix}5-\omega\\2\end{pmatrix}\quad\text{and}\quad\begin{pmatrix}2\\-5+\omega\end{pmatrix},\ \begin{pmatrix}-2\\4+\omega\end{pmatrix}. \tag{9.16}$$

By transposing and interchanging the two, we get as Perron–Frobenius row eigenvectors for A, A^{tr}

$$\begin{pmatrix}2,&\omega-5\end{pmatrix},\qquad\begin{pmatrix}\omega+4,&2\end{pmatrix}. \tag{9.17}$$

Let I_1, I_2 denote the ideals they generate. We note that $\omega-5=\left(-9+\sqrt{101}\right)/2$ and that the norm of this number is $(81-101)/4=-5$. Hence, over the algebraic number ring, which is $\mathbb{Z}[\omega]$ and properly contains $\mathbb{Z}[1/\lambda]$, both ideals are the entire ring $(1)=\mathbb{Z}[\omega]$, since the two have isomorphic spans over the algebraic number ring. Thus, we need to see whether some element in the quotient field will multiply one ideal to the other, as additive groups, or modules over $\mathbb{Z}[1/\lambda]=\mathbb{Z}[\lambda]=\{a+b\sqrt{101}\mid a,b\in\mathbb{Z}\}$.

Note that the two generators listed in (9.17) will actually generate each ideal over $\mathbb{Z}$ additively, not just as modules over $\mathbb{Z}[\lambda]$, since multiplication by $\sqrt{101}=2\omega-1$ sends

$$\begin{pmatrix}1,&\omega\end{pmatrix}\longrightarrow\begin{pmatrix}2\omega-1,&2(\omega+25)-\omega\end{pmatrix}=\begin{pmatrix}2\omega-1,&\omega+50\end{pmatrix}, \tag{9.18}$$

$$\begin{pmatrix}2,&\omega-5\end{pmatrix}\longrightarrow\begin{pmatrix}4\omega-2,&(\omega+50)-5(2\omega-1)\end{pmatrix}=\begin{pmatrix}4\omega-2,&55-9\omega\end{pmatrix}, \tag{9.19}$$

$$\begin{pmatrix}4+\omega,&2\end{pmatrix}\longrightarrow\begin{pmatrix}(\omega+50)+4(2\omega-1),&4\omega-2\end{pmatrix}=\begin{pmatrix}9\omega+46,&4\omega-2\end{pmatrix}, \tag{9.20}$$

which are still in the same additive subgroups.

The additive spans of the two pairs of generators in (9.17) are, respectively

$$2\mathbb{Z} + (\omega - 5)\,\mathbb{Z} = \{a + b\omega \mid a, b \in \mathbb{Z} \text{ such that } a - b \equiv 0 \pmod 2\}\,, \tag{9.21}$$

$$2\mathbb{Z} + (\omega + 4)\,\mathbb{Z} = \{a + b\omega \mid a, b \in \mathbb{Z} \text{ such that } a - b \equiv 1 \pmod 2\}\,. \tag{9.22}$$

These are preserved by multiplication by $\sqrt{101} = 2\omega - 1 \equiv 1 \pmod 2$, so that each span over $\mathbb{Z}$ is a $\mathbb{Z}\,[\lambda]$-module.

We will now complete the proof. If the ideals were isomorphic under multiplication by some $f \in \mathbb{Q}[\lambda]$, then f cannot involve primes of the algebraic number ring, since both ideals span the complete algebraic number ring as modules over it. Therefore f is a unit. Thus f is up to a sign a power of $\lambda = 9 + 2\omega \equiv 1 \pmod 2$. Hence multiplication by f preserves the congruence conditions defining the two additive spans, and thus it preserves each ideal separately. So it is impossible for a unit to send one ideal to the other.

Example 9.9. The following is an example of integer matrices A, B which have isomorphic dimension groups (unordered) but such that the corresponding transposed matrices A^{tr}, B^{tr} do not have isomorphic dimension groups. Informally, for matrices over $\mathbb{Z}$ with eigenvalues 1, p, q, the isomorphism type of the dimension group is determined by the way the p-divisible and q-divisible integer vectors lie, as subspaces, within all integer vectors.

$$\begin{pmatrix} 1 & 0 & 0 \\ x & p & 0 \\ y & 0 & q \end{pmatrix}$$

The p, q-divisible spaces split off as spanned by $(0, 1, 0)$, $(0, 0, 1)$, hence the column dimension groups are the same no matter what x, y are. We can use the diagonal as a comparison. The row dimension groups depend on how the p and q eigenvectors lie in their sum. Row eigenvectors are in the row kernels of

$$\begin{pmatrix} 1-p & 0 & 0 \\ x & 0 & 0 \\ y & 0 & q-p \end{pmatrix}, \qquad \begin{pmatrix} 1-q & 0 & 0 \\ x & p-q & 0 \\ y & 0 & 0 \end{pmatrix}.$$

These vectors are spanned by $(x, p-1, 0)$ and $(y, 0, q-1)$, respectively. If m divides $p-1$, $q-1$ and $x-y$ but not x, y then we have sum vectors which are divisible. This will give non-isomorphism of row dimension groups.

More formally, the column dimension groups consist of all vectors of the form $(a, b/p^n, c/q^n)$ (we may consider the form of the inverse and its columns). Any isomorphism on row dimension groups will be an integer matrix which preserves the row and column divisible eigenspaces. Take the case $p = 3$, $q = 5$, $x = y = 1$ as compared with $x = y = 0$. Then the row vectors $(0, 1, 0)$, $(0, 0, 1)$ for the diagonal case must be mapped to multiples by powers of 3, 5, -1 of vectors $(1, 2, 0)$, $(1, 0, 4)$, and the total determinant of the matrix must be odd. This should be a 2-adic isomorphism, but it cannot be since $(0, 1, 0) - (0, 0, 1)$ is not divisible by 2, whereas $(1, 2, 0) - (1, 0, 4)$ is divisible by 2, and the same is true if they are replaced by any of their odd multiples.

Remark 9.10. It follows from Theorem 3.1 of Boyle and Handelman [BoHa93] that there are nonnegative integer matrices that are shift equivalent to the pair in Example 9.9 and hence have the same dimension groups. We will now construct an example where the ordered dimension groups are isomorphic for two matrices, but for the transpose matrices, the ordered dimension groups are not isomorphic.

We modify Example 9.9 a little bit so as to get an example of two nonnegative integer matrices having identical ordered column dimension groups but nonisomorphic row dimension groups. We start with the same matrices as before except we take 3 and 7 as the two main diagonal primes. Then we add a large odd prime eigenvalue 101 which will enable a conjugate to be positive. This gives matrices A, B:

$$A = \begin{pmatrix} 101 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 3 & 0 \\ 0 & 1 & 0 & 7 \end{pmatrix}, \qquad B = \begin{pmatrix} 101 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 3 & 0 \\ 0 & 1 & 0 & 7 \end{pmatrix}.$$

We multiply these matrices by 5 and then conjugate by the matrix C:

$$C = \begin{pmatrix} 2 & -1 & 0 & 0 \\ 1 & 1 & -1 & 0 \\ 1 & 0 & 2 & -1 \\ 1 & 0 & -1 & 1 \end{pmatrix},$$

whose determinant is 5 and which approximately moves the row and column eigenvectors to $(1,1,1,1)$ to get nonnegative matrices

$$\begin{pmatrix} 205 & 200 & 200 & 200 \\ 104 & 109 & 94 & 94 \\ 110 & 110 & 105 & 70 \\ 86 & 86 & 106 & 141 \end{pmatrix}, \qquad \begin{pmatrix} 205 & 200 & 200 & 200 \\ 103 & 108 & 93 & 93 \\ 111 & 111 & 106 & 71 \\ 86 & 86 & 106 & 141 \end{pmatrix}.$$

These have identical dimension groups: the original unordered dimension groups are the same, by the above, just adding the eigenspace for the eigenvalue 101 in both cases. The order structure is determined by the Perron–Frobenius row eigenvalue, which is $(1,0,0,0)\,C^{-1}$ in both cases.

But for the transposes, row dimension groups, we have the direct sum of the 101 eigenspace with $\mathbb{Z}[1/5]$ times the previous examples. Making the prime 5 invertible will not affect the above argument that the row dimension groups are not isomorphic because this was a 2-adic nonisomorphism, given that the row eigenspaces for $5 \cdot 3$ and $5 \cdot 7$ eigenvalues must be preserved by an isomorphism. These are the spaces of vectors in the dimension group divisible by arbitrarily high powers of 3 and 7.

10. The quotient $G/\mathbb{Z}^N$ is an invariant

Recall that $G = G(A) = \bigcup_{n=0}^{\infty} A^{-n}\mathbb{Z}^N$. In this section we will consider the quotient group $G/\mathbb{Z}^N$. Here $\mathbb{Z}^N$ can be replaced with any free abelian subgroup L of G such that

$$G(A) = \bigcup_{n=0}^{\infty} A^{-n}L \tag{10.1}$$

and

$$AL \subset L. \tag{10.2}$$

We used the quotient group in [BJO99], but at the time we did not know if it was an invariant, and what the isomorphism classes were (in the category of abelian torsion groups). These issues are now resolved in the next proposition, which implies that the quotient is indeed an isomorphism invariant, i.e., that a given C^*-isomorphism implies that the corresponding two quotients are isomorphic groups.

Abelian torsion groups are classified in general by the so-called Ulm invariant [Kap69, pp. 26–27], [KaMa51, and references given there]. The Ulm invariant in general is a sequence of natural numbers suitably indexed by ordinals. These numbers are calculated as dimensions of certain vector spaces over the field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. First, any given torsion group decomposes over its p-subgroups, and the Ulm dimensions are then calculated for each ordinal, when p is fixed. In the present application, the Ulm invariant is, as we show, very simple and concrete.

Example 10.1. *The quotient group $G/\mathbb{Z}^N$ for the special case of Section* 7. It is easy to understand concretely the torsion group quotient for the special case of Section 7 when it is assumed that $|\det A| = \lambda_{(A)}$. Of course then $\lambda_{(A)}$ is an integer, and we may therefore form $\mathbb{Z}\left[1/\lambda_{(A)}\right]$ the usual way as an inductive limit $\bigcup_{n=1}^{\infty} \mathbb{Z}_{\lambda_{(A)}^n}$ as described in (4.3) with natural embeddings $\mathbb{Z}_{\lambda_{(A)}^n} \hookrightarrow \mathbb{Z}_{\lambda_{(A)}^{n+1}}$, and it follows from the discussion in Section 4 and Section 7 (Figure 1) that there is then a natural isomorphism between the two groups $G(A)/\mathbb{Z}^N$ and $\mathbb{Z}\left[1/\lambda_{(A)}\right]/\mathbb{Z}$. Hence, in this very special case, $\operatorname{Prim}\left(\lambda_{(A)}\right)$ is a complete invariant for the corresponding torsion group quotient. See also [BJO99] for more details. It is the case of dimension groups $G(A)$ more general than that of Section 7 which requires a nontrivial localization. The next two propositions deal with the general case, and the appropriate localizations.

One method of localizing at a prime p is to take the tensor product of an abelian group with $\mathbb{Z}\left[1/2, 1/3, \dots, \widehat{1/p}, \dots\right]$, inverting all primes except p; another is to tensor with the p-adic integers. Both agree for all torsion groups; the latter localization factors through the former. These tensor products are exact functors of abelian groups A which are subgroups of $\mathbb{Q}^N$, that is, they preserve exact sequences; this follows from [CaEi56, Proposition 7.2, p. 138], since the group $D(A)$ is a direct sum of copies of $\mathbb{R}/\mathbb{Z}$ which has no nontrivial continuous homomorphisms into the totally disconnected p-adics. Thus $\operatorname{Tor}^1(A, C)$ is zero. Unless otherwise specified we will mean the former, smaller tensor product when we localize.

Proposition 10.2. *Assume that A is a nonsingular $N \times N$ integer matrix and $G = \bigcup_n A^{-n}\mathbb{Z}^N$ the associated dimension group. Suppose L is any rank-N lattice in G such that $\bigcup_n A^{-n}L = G$. Then G/L is isomorphic to the product over primes dividing* $\det A$ *of a certain number $n(p)$ copies of $\mathbb{Z}_{p^\infty}$. The number $n(p)$ is the largest j such that if we write the characteristic polynomial of A as $x^N + c_1 x^{N-1} + \dots + c_{N-1}x + c_N$, p does not divide c_j. In addition G is dual to the eventual row space in the sense*

$$G \otimes \mathbb{Z}\left[1/2, \dots, \widehat{1/p}, \dots\right] = \left\{ v \in \mathbb{Q}^N \mid \langle w \,|\, v \rangle \in \mathbb{Z}_{(p)} \;\forall\, w \in G_{(p)}(A) \right\}. \tag{10.3}$$

Proof. G written as $\bigcup_{n=0}^{\infty} A^{-n}\left(\mathbb{Z}^N\right)$ will have as denominators only primes dividing $\det A$. If L includes $\mathbb{Z}^N$ then we have a torsion group whose torsion involves only primes in $\det A$.

We first argue that locally at each prime p in it, G consists of those vectors dual to the eventual p-adic row space $G_{(p)}(A)$ of A (see (4.12)–(4.13)). That is, (10.3) holds. The dimension group is the group of vectors x such that for some n,

$A^n x \in \mathbb{Z}^N$. This is the group of vectors such that $\exists\, n \in \mathbb{Z}_+$ such that for $\forall\, w \in \mathbb{Z}^N$, we have $wA^n x \in \mathbb{Z}$. This is the group of rational vectors whose products with the row space of A^n is integer. This construction also goes through if we localize at any prime. To say that a vector has p-integer product with the row space of A^n for some n then implies that it has p-integer product with the idempotent p-adic limit $E_{(p)}(A)$ of powers of A, defined in (4.8) and mentioned in Theorem 7 of [BJKR98]. Conversely suppose it has p-integer product with the idempotent p-adic limit, then by p-adic continuity, it must have p-integer product with some finite power. This gives the claim.

Now to show that the quotient group at the prime p is p-divisible, take a p-adic dual basis to $G_{(p)}(A)$, which, like any p-adic torsion-free module, must be a free module (the p-adic integers are a principal ideal domain, and argue as with the ordinary integers). Approximate these vectors p-adically by rational vectors b_i using a p-adic approximation theorem such as [Wei98, 1-2-3, p. 8], choosing these rational vectors so that they give a p-adic basis. Take the free abelian group L_1 generated by b_i. As soon as we have a lattice L including L_1 and $\mathbb{Z}^N$, the p-adic dimension group consists of a sum of copies of the p-adic integers corresponding to L_1 and a sum of copies of the p-adic field corresponding to the remaining vectors (in the null space of $E_{(p)}(A)$—we can take additional basis vectors for it). When we divide by L, we are dividing out by all the L_1 part p-adically, and by something isomorphic inside a p-adic field in the rest, and the result will be p-divisible.

In fact, for any lattice L such that $\bigcup_n A^{-n}L$ is the dimension group, the quotient will be isomorphic to this, since multiplication by A^{-1} gives an isomorphism of pairs $(\bigcup_n A^{-n}L, L) \to \left(\bigcup_n A^{-n}L, A^{-1}L\right)$, and eventually this lattice must be large enough.

Now consider the p-adic rank, in relation to the characteristic polynomial. By Newton's method [Wei98, 3-1-1, p. 74], if the characteristic polynomial has the given form, we can factor it over the p-adics as a product of two polynomials, one of which is x^{N-j} modulo p, and the other of which has invertible constant term over the p-adics. We can put the matrix into corresponding block form. The former part will be p-adically nilpotent, and the null space will be its row space. ☐

Corollary 10.3. *Let A, B be matrices as in Proposition* 10.2. *For any choice of lattices L, L' in their dimension groups satisfying the hypotheses in Proposition* 10.2, $G(A) \cong G(B) \Rightarrow G(A)/L \cong G(B)/L'$.

Remark 10.4. As noted, our groups $G(A)$ are contained in $\mathbb{R}^N$ (even in $\mathbb{Q}^N$) where N is the rank of $G(A)$. But it is clear that general lattices L in $\mathbb{R}^N$ are given by a choice of basis in $\mathbb{R}^N$ as a vector space. Writing the vectors in a basis, equivalently the generators for L, as column vectors, we note that the lattices L may be viewed as, or identified with, nonsingular real matrices. Making this identification, and fixing the rank N, we further note that the containment $L \subset L'$, for two given lattices, holds if and only if there is some $C \in M_N(\mathbb{Z})$ such that we have the following matrix factorization:

$$L = L'C. \tag{10.4}$$

There is a similar version of this for row spaces (or lattices defined from row vectors), as well as a p-adic variation, *mutatis mutandis;* and we have already seen an instance of the latter in (4.11)–(4.13).

Remark 10.5. We now show, using (10.4), that the conditions on L from Proposition 10.2 are all integrality conditions. There are three in all, and we proceed to spell them out. If A is given as usual, and if $G(A)$ is the corresponding group, i.e., $\bigcup_{n=0}^{\infty} A^{-n}(\mathbb{Z}^N)$, then a lattice L is a subgroup, i.e., $L \subset G(A)$, if and only if there is a natural number n such that

$$A^n L \in M_N(\mathbb{Z}). \tag{10.5}$$

Some given lattice L will satisfy the invariance property $A(L) \subset L$ if and only if the conjugate matrix $L^{-1}AL$ satisfies

$$L^{-1}AL \in M_N(\mathbb{Z}). \tag{10.6}$$

The further condition on L that it is generating, i.e., that $\bigcup_{n=0}^{\infty} A^{-n}(L) = G(A)$, holds if and only if for some natural number n we have

$$L^{-1}A^n \in M_N(\mathbb{Z}). \tag{10.7}$$

The three conditions should also be compared with (1.17) from Section 1.

Now Proposition 10.2 applies when $G(A)$ is given and some lattice satisfies all three conditions (10.5)–(10.7), and we get as a corollary that if two lattices L and L' both satisfy the conditions, then the two torsion groups $G(A)/L$ and $G(A)/L'$ are isomorphic groups.

In the study of dimension groups, it is convenient to explicitly compute certain extensions. Let $\mathbb{Z}_{p^\infty}$ denote the union of $\mathbb{Z}_{p^n}$ under inclusion, a divisible p-torsion group whose order p subgroup has rank 1. By standard theory [CaEi56], the extension group $\mathrm{Ext}(\mathbb{Z}_{p^\infty}, \mathbb{Z})$ can be computed using the exact sequence

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0 \tag{10.8}$$

as the cokernel of the map $\mathrm{Hom}(\mathbb{Z}_{p^\infty}, \mathbb{Q}) \to \mathrm{Hom}(\mathbb{Z}_{p^\infty}, \mathbb{Q}/\mathbb{Z})$; the former group is zero and the latter group is $\mathrm{Hom}(\mathbb{Z}_{p^\infty}, \mathbb{Z}_{p^\infty})$. Every p-adic integer gives a mapping in this group; we check this mapping is one-to-one and onto, so that the Ext group is the p-adic integers. (To check "onto", note that we get every mapping $\mathbb{Z}_{p^n} \to \mathbb{Z}_{p^n}$ and take limits.) In general, we are dealing with a direct sum of copies of these Ext groups.

Next we look at the problem of isomorphism of dimension groups in a somewhat different way, by showing that dimension groups can easily be computed as extensions. In some cases this leads to a quick decision about whether two dimension groups are isomorphic. However in the most general case, the problem of deciding isomorphism given this extension structure seems to still require the methods of Section 5. In view of Remark 10.4 we need only state the result for the case when the lattice L is $\mathbb{Z}^N$.

Corollary 10.6. *As in Proposition* 10.2, *consider an unordered dimension group as an extension of* $\mathbb{Z}^N$ *by a divisible torsion group* $G/\mathbb{Z}^N$ *whose structure, computed as in Proposition* 10.2, *is a direct sum over* i *of* n_i *copies of* $\mathbb{Z}_{p(i)^\infty} = \mathbb{Z}[1/p(i)]/\mathbb{Z}$. *The extension class in* $\mathrm{Ext}^1(G/\mathbb{Z}^N, \mathbb{Z}^N)$ *is an element of* $\bigoplus_i \bigoplus_{j=1}^{n_i} \mathbb{Z}_{p(i)}$. *We write* *this as an* $N \times \sum_i n_i$ *matrix whose entries are* $p(i)$*-adic integers:*

$$\begin{array}{c|c|c|c|}
 & n_1 & n_2 & \\
\hline
N & \mathbb{Z}_{(p(1))} & \mathbb{Z}_{(p(2))} & \cdots \\
\hline
\end{array},$$

where $p(i)$ *runs over all elements in* $\operatorname{Prim}(\det(A))$. *Its columns consist precisely of a basis for the null-space of the matrices* $E(A)$ *taken at each prime* $p(i)$. *Two such matrices* M_1, M_2 *represent isomorphic unordered dimension groups if and only if there is a matrix* $C \in \mathrm{GL}(N, \mathbb{Z}[1/\det(A)])$ *and an invertible direct sum of* $p(i)$*-adic integer matrices* D *such that* $CM_1D = M_2$.

Proof. The given structure (that is, M_1 up to its equivalence with any CM_1D) is an isomorphism invariant because the p-adic row spaces $G_{(p)}(A)$ defined in (4.12)–(4.13) are invariants. Corollary 4.2 shows that a rational matrix over $\mathbb{Z}[1/\det(A)]$ giving an isomorphism on dimension groups must give an isomorphism on the p-adic row spaces, hence the dual p-adic null spaces of $E_{(p)}(A)$. In fact Corollary 4.2 gives, as necessary and sufficient conditions for unordered dimension group isomorphism, in effect, the existence of C and D: the p-adic symmetries just mean we are considering the row spaces up to isomorphism, and the $\mathrm{GL}(N, \mathbb{Z}[1/\det A])$ symmetry means that we have a rational map which is an isomorphism at all primes other than the ones considered here.

The extension class of any extension of $\mathbb{Z}^N$ by a group $G/\mathbb{Z}^N$ may be computed by extending the map $\mathbb{Z}^N \subset \mathbb{Q}^N$ to a mapping $G \to \mathbb{Q}^N$, and letting this give a map in $\operatorname{Hom}(G/\mathbb{Z}^N, (\mathbb{Q}/\mathbb{Z})^N) \cong \operatorname{Ext}^1(G/\mathbb{Z}^N, \mathbb{Z}^N)$. This is the remark of Cartan–Eilenberg [CaEi56, p. 292]. To identify this class it suffices to look at the p-torsion subgroup of $G/\mathbb{Z}^N$ for each prime p since the group is the direct sum of its p-torsion subgroups. To identify this class, take the tensor product of G with the p-adic integers, getting a localized extension of $\mathbb{Z}_{(p)}^N$ by the p-torsion subgroup of $G/\mathbb{Z}^N$, which is $G \otimes \mathbb{Z}_{(p)}^N$. But if we write all p-adic vectors as the direct sum $K \oplus R$ of the p-adic null space of R_A and a complementary space R, by Proposition 10.2,

$$G \otimes \mathbb{Z}_{(p)}^N = (K \otimes \mathbb{Q}_{(p)}) \oplus (R \otimes \mathbb{Z}_{(p)}). \tag{10.9}$$

Thus the extension class is represented taking

$$(K \otimes \mathbb{Q}_{(p)}) \oplus (R \otimes \mathbb{Z}_{(p)}) \to (K + R) \otimes \mathbb{Q}_{(p)} \tag{10.10}$$

and collapsing by $\mathbb{Z}_{(p)}^N$ to give the inclusion

$$(K \otimes \mathbb{Q}_{(p)})/(K \otimes \mathbb{Z}_{(p)}) \to (K + R) \otimes (\mathbb{Q}_{(p)}/\mathbb{Z}_{(p)}) = (\mathbb{Q}_{(p)}/\mathbb{Z}_{(p)})^N. \tag{10.11}$$

This map is induced by the map

$$(K \otimes \mathbb{Q}_{(p)}) \to (K + R) \otimes \mathbb{Q}_{(p)} = \mathbb{Z}^N \otimes \mathbb{Q}_{(p)} \tag{10.12}$$

which can be taken to send the ith unit vector on the left to the ith vector in a basis for K on the right. This means taking basis vectors for the null space of E_A as forming the columns of the matrix giving the extension. □

In Example 12.3 we will give an example where the groups G/L are the same, but the extensions are different.

11. Remarks on the singular case

Except for Sections 2 and 6 and Theorem 5.9 of this paper, we have considered AF-algebras defined by nonsingular primitive matrices $A, B, \ldots$. Let us comment that the class of dimension groups arising from primitive matrices does change if one dispenses with the nonsingularity assumption. George Elliott has given an example of a dimension group which in his terminology is not ultrasimplicial. For example, the group arising from the stationary diagram associated with the matrix

$$\begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 2 \\ 2 & 1 & 0 \end{pmatrix}$$

cannot arise from a diagram associated with a nonsingular matrix [Ell79]. Elliott actually proves the following: If G is the dimension group defined by the matrix via Bratteli diagrams, then it is not possible to span a given finite set of positive elements of G by another finite set of positive linearly independent (over $\mathbb{Z}$) elements, where the span uses only positive coefficients. But it is not hard to see that this is equivalent to the impossibility of writing the group as a direct limit with injective maps, that is, with nonsingular matrices. In the case at stake, Elliott gives the following three positive elements of G which cannot be spanned in the above manner: $(1,0)$, $(1,-1)$, $(1,1)$. In this case G is isomorphic to the direct product of $\mathbb{Z}[1/3]$ and $\mathbb{Z}$, with order defined by the condition that the positive elements are those elements which have strictly positive first coordinate—the one from $\mathbb{Z}[1/3]$. The matrix is primitive.

Since C^*-equivalence is weaker than shift equivalence, the matrix above is also an example of a matrix which is primitive, but not shift equivalent to a primitive nonsingular matrix. Other such examples may be found in [BoHa91].

We do not expect that the analogue of our Theorem 11.3 is true in the context of shift equivalence. (For example, it looks like the example [BoHa91, Appendix 3, p. 310] can be modified as follows (multiply approximately by 10). There is no 4×4 nonnegative matrix whose spectrum is $\{14, 10i, -10i, 3\}$. However, we can readily construct an integer 4×4 matrix with this spectrum (block diagonal), with the eigenvector at 14 being $(1,0,0,0)$. Then we take a unimodular matrix mapping the vector $(1,0,0,0)$ to $(1,1,1,1)$. Then some power of this conjugated matrix is nonnegative, giving us the situation of Theorem 11.3. Moreover it should follow from [BoHa93, Theorem 3.1] that this matrix over $\mathbb{Z}$ is shift equivalent to a primitive nonnegative matrix of larger dimension.) For our weaker C^*-equivalence we have the added flexibility of replacing matrices by powers of themselves.

We will prove in Theorem 11.3 below that in some special circumstances, the condition of nonsingularity of the matrix A can be removed, and A merely assumed to be primitive, without changing the class of C^*-algebras. In the general case when A is not assumed invertible, we may introduce the eventual range of A,

$$\mathcal{W}(A) := \bigcap_{i=0}^{\infty} A^i \mathbb{Q}^N = A^N \mathbb{Q}^N . \tag{11.1}$$

Note that A is bijective as a map $\mathcal{W}(A) \to \mathcal{W}(A)$. We may now introduce an additive group $G(A)$ by

$$G(A) := \left\{ g \in \mathcal{W}(A) \mid A^k g \in \mathbb{Z}^N \text{ for some } k \in \mathbb{Z}_+ \right\} , \tag{11.2}$$

and one notes that this group $G(A)$ identifies with the inductive limit of the sequence (1.6), i.e. $G(A)$ is the dimension group when it is equipped with the obvious order. (This version of $G(A)$ was used, but not defined, already in Section 2 above.) Let us give some details. An element of the inductive limit (1.6) can be represented by a sequence $\{g_m, g_{m+1}, \dots\}$ in $\mathbb{Z}^N$ with $Ag_n = g_{n+1}$ for $n = m, m+1, \dots$. Two such sequences represent the same element if they coincide from a certain step n onward. Given such a sequence, there is a unique sequence $\{h_1, h_2, \dots\}$ in $\mathcal{W}(A)$ such that $Ah_n = h_{n+1}$ for $n = 1, 2, \dots$ and such that $h_n = g_n$ for all large n. Then h_1 is the element of $G(A) \subset \mathcal{W}(A)$ representing the dimension group element in (11.2), so this shows the equivalence between the two definitions (11.2) and (1.6) of $G(A)$. The definition (11.2) is the definition used in [BMT87, p. 49]. If A is nonsingular and, as in (11.2), $A^k g = m \in \mathbb{Z}^N$, then $g = A^{-k}m$ is a typical element of the (1.8)–(1.10) version of $G(A)$, and *vice versa.* If A is primitive, we still have the Perron–Frobenius data, and the order can be defined as before, *mutatis mutandis.*

Lemma 11.1. *Given a vector $u \in \mathbb{R}^r$ there exist r vectors $w_i \in \mathbb{Z}^r$ such that the convex cone generated by the w_i contains an open neighborhood of u, and the determinant of the matrix the w_i form is ± 1.*

Proof. The standard unit vectors do this for any vector in the subsemigroup of strictly positive integer vectors. We claim transforms of these by integer row and column operations, permutations, and reversals of sign, take any vector to the interior of this subsemigroup—then just reverse those operations on the standard basis vectors. In fact, we get all coordinates nonzero by certain linear combinations, then reverse their signs. ◻

Remark 11.2. It is not in general possible to get a determinant-1 system of matrices which approximate multiples by some positive constant C of a given set of nonnegative vectors w_i in Lemma 11.1. This is easiest to see when the vectors w_i are chosen diagonally dominant. But Lemma 11.1 can probably be strengthened a little.

Theorem 11.3. *Let A be an integer primitive matrix. Suppose that when the vector u in Lemma 11.1 is the Perron-Frobenius eigenvector of A, the vectors $w_i \in \mathbb{Z}^r$ can be chosen to be positive in terms of the order structure of the dimension group of A. Then the ordered dimension group arising from the primitive integer matrix A is order isomorphic to one arising from a nonsingular primitive integer matrix B.*

Proof. Let the dimension of A be d and the rank of all sufficiently large powers A^s be r. By Lemma 11.1, we find a set of r vectors w_i in the eventual row space R, that is, the row space of A^N, or some specific higher power, a rank-r subspace of $\mathbb{Z}^d$ such that the cone over $\mathbb{Q}_+$ generated by this set includes a neighborhood of the maximum eigenvector v within R. This is sufficient to establish that all sufficiently large powers of A have their rows expressed as (unique) nonnegative linear combinations of w_i, since all rows of A^s divided by their lengths converge to fixed multiples of v and hence are eventually in the convex cone; but to be in the convex cone means that we have these convex combinations.

However, we also need that it can be chosen that these convex combinations are eventually integer. For that, it suffices that the determinant of the w_i expressed as combinations of a basis for the integral vectors in the eventual row space, i.e.,

$R \cap \mathbb{Z}^d$, a rank-r free abelian group, is 1 or -1. This follows from the lemma and the extra assumption.

Now let B be the matrix of A^s expressed as acting on the vectors w_i, which will be nonnegative, and positive. Then B is shift equivalent to A^s over the integers (maybe with negative entries), just by the inclusion mapping given by the vectors w_i. By a theorem of Parry and Williams [PaWi77] (reproved in our 1979 paper [KiRo79]), any shift equivalence over $\mathbb{Z}$ of primitive matrices can be realized by a shift equivalence over $\mathbb{Z}_+$. This shift equivalence will induce an isomorphism of ordered dimension groups. □

12. Strong local isomorphism

Definition 12.1. We will say that two dimension groups G, G' are strongly locally isomorphic at the prime p if and only if there is an isomorphism $G \otimes \mathbb{Z}_{(p)} \to G' \otimes \mathbb{Z}_{(p)}$ induced by a matrix of integers. (The first paragraph of the proof below shows that this is equivalent to requiring that the isomorphism be induced by a matrix of rational numbers.) (Recall that G and G' are locally isomorphic at prime p if there merely is an isomorphism $G \otimes \mathbb{Z}_{(p)} \to G' \otimes \mathbb{Z}_{(p)}$.)

In the next theorem we show that strong local isomorphism is described a condition similar to that in Corollary 10.6 if we just take the submatrix corresponding to the prime in question. This condition is rather strong and can be decided by a simpler algorithm than the general algorithm in Section 5. When we speak of realizing some p-adic construct over an algebraic number field K, we mean in terms of an inclusion $K \subset \mathbb{Z}_{(p)}$ corresponding to a non-archimedean completion of K. Note in connection with the following theorem that if the ranks of the p-adic eventual row spaces of A and B are different, local isomorphism cannot hold. Also note that the equivalent conditions imply that the smallest fields over which the eventual p-adic row spaces can be realized are the same for A and B.

Theorem 12.2. *Given two nonnegative matrices A, B, form a matrix whose rows are a basis for the p-adic eventual row spaces of A, B whose ranks are n_p. Their dimension groups are strongly locally isomorphic at the prime p if and only if the corresponding two matrices A, B for each p admit some matrices $C \in \mathrm{GL}(n, \mathbb{Q})$, $D \in \mathrm{GL}(n_p, \mathbb{Z}_{(p)})$ such that $AC = DB$. This condition is decidable.*

Proof. The proof of Corollary 4.2, or alternatively, the proof of Proposition 10.2, shows that having a rational mapping which induces isomorphism of p-adic dimension groups is equivalent to having a rational mapping which induces an isomorphism of p-adic eventual row spaces. To make such a mapping integer, multiply by all denominators relatively prime to p. At p we must have integrality on the eventual row space $G_{(p)}(A)$ which is a summand of the space of all p-adic integer vectors. The use of a projection $E_{(p)}(A)$ to this subspace enables us to get a map equal to the given integer mapping defined over some algebraic number field, p-adic integer, and equal to the rational mapping on the eventual row space. The irrational part of this map will also consist of algebraic integers, since $\mathbb{Z}$ will be an additive summand of the algebraic number ring, and can be discarded, since it must be zero on the summand. This gives a matrix of integers inducing the p-adic isomorphism, and thus the local isomorphism is strong.

A rational mapping inducing an isomorphism of p-adic row spaces is equivalent to having a matrix C (giving the rational mapping) and a matrix D such that

$DAC = B$ (where D expresses the image of the row basis vectors of A as linear combinations of a basis for B); it must be p-adic integer and invertible since we can also map backwards by the isomorphism of row spaces.

Next we show this criterion is decidable. The field generated by all eigenvalues of A or B will be sufficient to realize the p-adic eventual row spaces: we take this field and some prime π giving an embedding in an extension of $\mathbb{Z}_{(p)}$. Then the p-adic eventual row space is spanned by the generalized eigenspaces for eigenvalues which are relatively prime to π, since multiplication by powers of A will not send them to zero, but will annihilate all other generalized eigenspaces, modulo any power of π. Some linear combinations of basis vectors for these generalized eigenspaces must give a p-adic basis.

The required p-adic matrix D then must lie in this field K, since C, A, B do. Being p-adic integer means that its denominators are relatively prime to p. It can then be expanded as a larger matrix over $\mathbb{Z}_{ip} = \mathbb{Z}[1/2, 1/3, \dots, \widehat{1/p}, \dots]$, using a basis for the p-adic integers of K over $\mathbb{Z}_{ip}$. Given the matrix D, the condition that a corresponding C exists over $\mathbb{Q}$ can be stated by linear equations in D. Existence of rational C means that all columns of BD are rational combinations of the columns of A. For the expanded matrices over $\mathbb{Z}_{ip}$, that means that we have any linear column combinations of the columns of A yielding the desired columns of BD^{-1}. In turn that means that the columns of BD^{-1} have zero inner product with all vectors which have zero inner product with the columns of A, which is a linear condition.

We can now determine a p-adic basis for this linear space of matrices D, write the determinant of D as a polynomial in the coefficients of a general linear combination of basis elements, and determine whether or not it is possible for the determinant to be nonzero modulo p by testing each congruence class of entries modulo p. $\square$

Example 12.3. Let

$$A = \begin{pmatrix} 4 & 1 \\ 1 & 2 \end{pmatrix}, \qquad B = \begin{pmatrix} 7 & 0 \\ 0 & 1 \end{pmatrix}. \tag{12.1}$$

The respective characteristic polynomials are $x^2 - 6x + 7$ and $x^2 - 8x + 7$, with determinant 7, and we consider the local dimension groups at 7. Since 7 does not divide 8, only one root of the former polynomial is divisible by 7. Thus only the identity element of the $\mathbb{Z}_2$ Galois group fixes the eigenvalue not divisible by 7. This implies that the 7-adic row space is irrational, and the minimal fields over which eventual row spaces are defined are respectively $\mathbb{Q}\left[\sqrt{2}\right]$, $\mathbb{Q}$, so the dimension groups are not locally isomorphic. Note that, even so, the two quotient groups $G(A)/\mathbb{Z}^2$ and $G(B)/\mathbb{Z}^2$ are isomorphic. This follows from Proposition 10.2: Recall, to verify this we need only compute the respective Ulm numbers from the characteristic polynomials, and there is only the prime $p = 7$ to check. So the 7-reduced rank is 1 for each of the two quotient torsion groups calculated from A and B.

Example 12.4. Our next example illustrates C^*-symmetry, as well as the calculation of the p-adic eventual row spaces. Consider

$$A = \begin{pmatrix} 3 & 1 \\ 2 & 3 \end{pmatrix} \tag{12.2}$$

and its transpose $B = A^{\mathrm{tr}}$; for this particular choice of the pair A, B, the minimal fields over which eventual row spaces are defined are isomorphic. We can arbitrarily choose which root of the characteristic polynomial $x^2 - 6x + 7$, the same as for A in Example 12.3, is divisible by 7 (representing the unique p-adic root which is divisible by 7), say $3 - \rho$ where ρ is a square root of 2 in $\mathbb{Z}_{(7)}$ (see next paragraph). The eventual row eigenspaces are spanned by the other row eigenvectors, which are $(1, \rho)$ for B and $(\rho, 1)$ for A. A mapping of eigenspaces must map one to a multiple c times the other. If it commutes with the Galois action, then it must do the same for their conjugates, so that it has the form

$$\begin{pmatrix} 0 & c \\ c & 0 \end{pmatrix}. \tag{12.3}$$

The determinant restricted to the eventual 7-adic row space is c, so the congruences are $c \equiv 0 \pmod 7$, which are solvable. The dimension groups of this matrix and its transpose are locally isomorphic at the prime 7. Since 7 is the only prime involved, this implies global isomorphism of the unordered dimension groups.

Here we think of the field $\mathbb{Q}\left[\sqrt{2}\right]$ as embedded in the field of 7-adics $\mathbb{Q}_{(7)}$ via $1 \mapsto 1$ and $\sqrt{2} \mapsto \rho$, where $\rho \in \mathbb{Z}_{(7)} \subset \mathbb{Q}_{(7)}$. The polynomial $x^2 - 2$ may be considered in $\mathbb{Z}_{(7)}[x]$, and it is reducible there. To find the two roots $\pm\rho$ in $\mathbb{Z}_{(7)}$, calculate the terms $t_0, t_1, \dots \in \{0, 1, 2, \dots, 6\}$ in $\rho = t_0 + t_1 \cdot 7 + t_2 \cdot 7^2 + \dots \in \mathbb{Z}_{(7)}$ recursively, starting with $t_0 = 3$ or $t_0 = 4$ (see, e.g., [BoSh66, p. 18]). They can be found with Maple or the PARI program. The results are $\rho = 3 + 1 \cdot 7 + 2 \cdot 7^2 + 6 \cdot 7^3 + 1 \cdot 7^4 + 2 \cdot 7^5 + \cdots$ and $-\rho = 4 + 5 \cdot 7 + 4 \cdot 7^2 + 0 \cdot 7^3 + 5 \cdot 7^4 + 4 \cdot 7^5 + \cdots$. Since the root $3 - \rho$ of $x^2 - 6x + 7$ is divisible by 7, the 7-adic eventual row spaces in $\left(\mathbb{Z}_{(7)}\right)^2$ are the respective $\mathbb{Z}_{(7)}$-modules

$$G_{(7)}(A) = \mathbb{Z}_{(7)}(\rho, 1)$$

and

$$G_{(7)}(B) = \mathbb{Z}_{(7)}(1, \rho),$$

by Remark 4.3, i.e., they are generated over $\mathbb{Z}_{(7)}$ by the respective row eigenvectors corresponding to the second eigenvalue $3 + \rho$, the one not divisible by 7.

Note also in this case that A and A^{tr} are conjugate by the unimodular matrix $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$; and hence it even follows directly as in Example 9.1 that A and A^{tr} are (elementary) shift equivalent.

Note finally that if one denotes the A matrices in (12.1) and (12.2) by A_1, A_2, respectively, and one defines

$$J = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \tag{12.4}$$

then $A_2 J = J A_1$, and thus if $K = A_1 J^{-1}$ we have the system

$$A_2 = JK, \qquad A_1 = KJ. \tag{12.5}$$

But K does not have positive matrix entries, so this does not imply elementary shift equivalence. However, if we redefine

$$K = A_1^2 J^{-1} = \begin{pmatrix} 11 & 6 \\ 1 & 3 \end{pmatrix}, \tag{12.6}$$

then we have the pair of shift relations for the squares,

$$A_1^2 = KJ, \qquad A_2^2 = JK, \tag{12.7}$$

which is the assertion that A_1^2 and A_2^2 are elementary shift equivalent. In particular, A_1 and A_2 are C^*-equivalent. This latter conclusion and the one in Example 9.1 also follow the next general observation:

Observation 12.5. If A, B are nonsingular primitive $N \times N$ matrices and there exists a unimodular matrix J in $M_N(\mathbb{Z})$ such that

$$v(B)J = \mu v(A) \tag{12.8}$$

for a positive number μ, and

$$BJ = JA, \tag{12.9}$$

then A and B are C^*-equivalent.

Proof. Since J is unimodular, we have

$$\begin{cases} B^n J A^{-n} = J A^n A^{-n} = J \in M_N(\mathbb{Z}), \\ A^n J^{-1} B^{-n} = A^n A^{-n} J^{-1} = J^{-1} \in M_N(\mathbb{Z}), \end{cases} \tag{12.10}$$

and the observation follows from (1.16)–(1.17). (The condition (12.8) may be replaced by the strictly stronger requirement that J and J^{-1} have only nonnegative matrix entries.) $\square$

Remark 12.6. In fact we have the "partial" implication (12.9) $\Rightarrow$ (12.8), but (12.8) for some real scalar μ, while the positivity restriction on μ is not a consequence of (12.9) alone. We further stress that (12.9)–(12.8) are more restrictive than C^*-equivalence, even more restrictive than shift equivalence: take, for example, $A = \left(\begin{smallmatrix} 2 & 1 \\ 4 & 4 \end{smallmatrix}\right)$ and $B = \left(\begin{smallmatrix} 2 & 2 \\ 2 & 4 \end{smallmatrix}\right)$, which are shift equivalent by [Bak83], but do not satisfy (12.9).

To summarize, the two examples have four matrices in all, and the first one in Example 12.3 is C^*-equivalent to the two in Example 12.4, but $\left(\begin{smallmatrix} 7 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ from Example 12.3 is not C^*-equivalent to the other three. The first one, $\left(\begin{smallmatrix} 4 & 1 \\ 1 & 2 \end{smallmatrix}\right)$ in Example 12.3, is symmetric, and A from Example 12.4 is C^*-symmetric in that it is C^*-equivalent to its own transpose.

Remark 12.7. Note that the two matrices A_1, A_2 in (12.1), (12.2) considered above are elementary shift equivalent over $\mathbb{Z}$ since they are conjugate over $\mathbb{Z}$. But while A_1^2, A_2^2 are elementary shift equivalent over $\mathbb{Z}_+$, A_1 and A_2 are not! (These types of 2×2 examples have been considered earlier by Kirby Baker [Bak83, Bak87].) This is seen as follows: Suppose $A_1 = CD$ where C, D are nonnegative integer 2×2 matrices. Then C expresses the rows of A_1 as nonnegative integer combinations of the rows of D. The entries 1 in the rows of A_1 can only come from entries 1 in the rows of D. Moreover these 1's can only be in the same row. Furthermore, in the linear combinations these 1's can only be multiplied by 1's. So the product CD looks like, up to symmetry,

$$\begin{pmatrix} 1 \cdot c_{12} & d_{11} \cdot 1 \\ c_{21} \cdot 1 & 1 \cdot d_{22} \end{pmatrix} = \begin{pmatrix} 4 & 1 \\ 1 & 2 \end{pmatrix}. \tag{12.11}$$

But if we write out the equations, there are no solutions unless one of C, D is a permutation matrix, and thus DC cannot be equal to A_2.

13. Concluding remarks

In the paper we addressed the interplay between the local and the global versions of the isomorphism problem. There are different, but related, decidability results in the literature. Ax and Kochen [AxKo65a, AxKo65b, AxKo66] and Grunewald and Segal [GrSe82] address decidability in a p-adic setting.

Acknowledgements. The co-authors are very grateful to Brian Treadway for his excellent work in typesetting, and in coordinating the many pieces of manuscript, and sequences of revisions, which arrived by fax and e-mail. We also thank Daniele Mundici and David Stewart for helpful conversations and references on computation and algorithms. We are especially indebted to Vincenzo Marra for pointing out a serious mistake in the preprint version of Theorem 11.3, and reminding us about the reference [Ell79]. The referee of the paper sent a very extensive report making many constructive suggestions both for improving the exposition and for making the reduction to nonsingular matrices explicit. P.E.T.J. benefited by a Norwegian-funded visit to the University of Oslo in the winter 1998–99 and in the summer 2000 where part of the work was done, and he is grateful for the support and hospitality.

Richtiges Auffassen einer Sache und Mißverstehen der gleichen Sache schließen einander nicht vollständig aus.

—Franz Kafka, *Der Prozeß*

References

[AxKo65a] J. Ax and S. Kochen, *Diophantine problems over local fields, I*, Amer. J. Math. **87** (1965), 605–630.

[AxKo65b] J. Ax and S. Kochen, *Diophantine problems over local fields, II: A complete set of axioms for p-adic number theory*, Amer. J. Math. **87** (1965), 631–648.

[AxKo66] J. Ax and S. Kochen, *Diophantine problems over local fields, III: Decidable fields*, Ann. of Math. (2) **83** (1966), 437–456.

[Bak83] K.A. Baker, *Strong shift equivalence of* 2×2 *matrices of nonnegative integers*, Ergodic Theory Dynamical Systems **3** (1983), 501–508.

[Bak87] K.A. Baker, *Strong shift equivalence and shear adjacency of nonnegative square integer matrices*, Linear Algebra Appl. **93** (1987), 131–147.

[BJKR98] O. Bratteli, P.E.T. Jorgensen, K.H. Kim, and F. Roush, *Non-stationarity of isomorphism between AF algebras defined by stationary Bratteli diagrams*, Ergodic Theory Dynam. Systems, to appear.

[BJO99] O. Bratteli, P.E.T. Jorgensen, and V. Ostrovs'kyĭ, *Representation theory and numerical AF-invariants: The representations and centralizers of certain states on* $\mathcal{O}_d$, submitted to Mem. Amer. Math. Soc.

[Bla86] B. Blackadar, *K-theory for Operator Algebras*, MSRI Publication Series, vol. 5, Springer-Verlag, New York–Heidelberg–Berlin–Tokyo, 1986.

[BMT87] M. Boyle, B. Marcus, and P. Trow, *Resolving maps and the dimension group for shifts of finite type*, Mem. Amer. Math. Soc. **70** (1987), no. 377.

[BoHa91] M. Boyle and D. Handelman, *The spectra of nonnegative matrices via symbolic dynamics*, Ann. of Math. (2) **133** (1991), 249–316.

[BoHa93] M. Boyle and D. Handelman, *Algebraic shift equivalence and primitive matrices*, Trans. Amer. Math. Soc. **336** (1993), 121–149.

[BoSh66] Z.I. Borevich and I.R. Shafarevich, *Number Theory*, Pure and Applied Mathematics, vol. 20, Academic Press, New York–London, 1966, translated from the Russian Теория Чисел, Moscow, 1964, by N. Greenleaf.

[Bra72] O. Bratteli, *Inductive limits of finite dimensional* C^**-algebras*, Trans. Amer. Math. Soc. **171** (1972), 195–234.

[Buc86] J. Buchmann, *Generalized Continued Fractions and Number Theoretic Computations*, Berichte der Mathematisch-Statistischen Sektion in der Forschungsgesellschaft Joanneum, vol. 269, Forschungszentrum Graz Mathematisch-Statistische Sektion, Graz, 1986, Paper from the sixteenth Styrian mathematical symposium held in Stift Rein/Graz, September 21–26, 1986.

[CaEi56] H.P. Cartan and S. Eilenberg, *Homological Algebra*, Princeton University Press, Princeton, New Jersey, 1956.

[CuKr80] J. Cuntz and W. Krieger, *Topological Markov chains with dicyclic dimension groups*, J. Reine Angew. Math. **320** (1980), 44–51.

[DHS99] F. Durand, B. Host, and S. Skau, *Substitutional dynamical systems, Bratteli diagrams, and dimension groups*, Ergodic Theory Dynam. Systems **19** (1999), 953–993.

[DMR76] M. Davis, Yu. Matijasevič, and J. Robinson, *Hilbert's tenth problem: Diophantine equations: positive aspects of a negative solution*, Mathematical Developments Arising from Hilbert Problems (De Kalb, Ill., 1974) (F.E. Browder, ed.), Proceedings of Symposia in Pure Mathematics, vol. 28, American Mathematical Society, Providence, 1976, pp. 323–378.

[Eff81] E.G. Effros, *Dimensions and C^*-algebras*, CBMS Regional Conf. Ser. in Math., vol. 46, Conference Board of the Mathematical Sciences, Washington, 1981.

[Ell76] G.A. Elliott, *On the classification of inductive limits of sequences of semisimple finite-dimensional algebras*, J. Algebra **38** (1976), 29–44.

[Ell79] G.A. Elliott, *On totally ordered groups, and K_0*, Ring theory (Waterloo, 1978) (D. Handelman and J. Lawrence, eds.), Lecture Notes in Math., vol. 734, Springer, Berlin, 1979, pp. 1–49.

[GrSe80a] F. Grunewald and D. Segal, *Some general algorithms, I: Arithmetic groups*, Ann. of Math. (2) **112** (1980), 531–583.

[GrSe80b] F. Grunewald and D. Segal, *Some general algorithms, II: Nilpotent groups*, Ann. of Math. (2) **112** (1980), 585–617.

[GrSe82] F. Grunewald and D. Segal, *Résolution effective de quelques problèmes diophantiens sur les groupes algébriques linéaires*, C. R. Acad. Sci. Paris Ser. I Math. **295** (1982), 479–481.

[Han81] D. Handelman, *Positive matrices and dimension groups affiliated to C^*-algebras and topological Markov chains*, J. Operator Theory **6** (1981), 55–74.

[Han87] D. Handelman, *Eventually positive matrices with rational eigenvectors*, Ergodic Theory Dynamical Systems **7** (1987), 193–196.

[Her69] Hans Hermes, *Enumerability, Decidability, Computability: An Introduction to the Theory of Recursive Functions*, Springer-Verlag, New York, 1969, Translated from the German by G. T. Hermann and O. Plassmann. Second revised edition. Die Grundlehren der mathematischen Wissenschaften, Band 127.

[Her78] Hans Hermes, *Aufzählbarkeit, Entscheidbarkeit, Berechenbarkeit: Einführung in die Theorie der rekursiven Funktionen*, third ed., Springer-Verlag, Berlin, 1978.

[HiSi00] M. Hindry and J.H. Silverman, *Diophantine Geometry: An Introduction*, Graduate Texts in Mathematics, vol. 201, Springer-Verlag, New York, 2000.

[Jac75] N. Jacobson, *Lectures in Abstract Algebra, Vol. III: Theory of fields and Galois theory*, Graduate Texts in Mathematics, vol. 32, Springer-Verlag, New York–Heidelberg, 1975, second corrected printing.

[Jac97] J. Jacklitch, *Homeomorphisms of* 1*-dimensional hyperbolic attractors*, thesis preprint, 1997.

[KaMa51] I. Kaplansky and G.W. Mackey, *A generalization of Ulm's theorem*, Summa Brasil. Math. 2 (1951), 195–202.

[Kap69] I. Kaplansky, *Infinite Abelian Groups*, revised ed., The University of Michigan Press, Ann Arbor, 1969.

[KiRo79] K.H. Kim and F.W. Roush, *Some results on decidability of shift equivalence*, J. Combin. Inform. System Sci. **4** (1979), 123–146.

[KiRo88] K.H. Kim and F.W. Roush, *Decidability of shift equivalence*, Dynamical Systems (College Park, MD, 1986–87) (J.C. Alexander, ed.), Lecture Notes in Mathematics, vol. 1342, Springer-Verlag, Berlin-New York, 1988, pp. 374–424.

[Kit98] B.P. Kitchens, *Symbolic Dynamics: One-sided, Two-sided and Countable State Markov Shifts*, Universitext, Springer-Verlag, Berlin, 1998.

[Knu81] Donald E. Knuth, *The art of computer programming: Vol. 2: Seminumerical algorithms*, 2nd ed., Addison-Wesley Publishing Co., Reading, Mass., 1981.

[Kob84] N. Koblitz, *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, 2nd ed., Graduate Texts in Mathematics, vol. 58, Springer-Verlag, New York, 1984.

[MuPa98] D. Mundici and G. Panti, *The equivalence problem for Bratteli diagrams*, preprint, 1998.

[New72] M. Newman, *Integral Matrices*, Pure and Applied Mathematics, vol. 45, Academic Press, New York–London, 1972.

[PaTa95] Jacob Palis and Floris Takens, *Hyperbolicity and sensitive chaotic dynamics at homoclinic bifurcations*, Cambridge Studies in Advanced Mathematics, vol. 35, Cambridge University Press, 1993.

[PaTu82] W. Parry and S. Tuncel, *Classification Problems in Ergodic Theory*, London Mathematical Society Lecture Note Series, vol. 67, Statistics: Textbooks and Monographs, no. 41, Cambridge University Press, Cambridge–New York, 1982.

[PaWi77] W. Parry and R.F. Williams, *Block coding and a zeta function for finite Markov chains*, Proc. London Math. Soc. (3) **35** (1977), 483–495.

[PoZa97] M. Pohst and H. Zassenhaus, *Algorithmic Algebraic Number Theory*, Encyclopedia of Mathematics and its Applications, vol. 30, Cambridge University Press, Cambridge, 1997, revised reprint of the 1989 original.

[Pru25] H. Prüfer, *Theorie der Abelschen Gruppen II*, Math. Z. **22** (1925), 222–249.

[Rad99] Charles Radin, *Miles of tiles*, American Mathematical Society, Providence, RI, 1999.

[Rot98] J.J. Rotman, *Galois Theory*, second ed., Universitext, Springer-Verlag, New York, 1998.

[Ser77] J.-P. Serre, *Linear Representations of Finite Groups*, Graduate Texts in Mathematics, vol. 42, Springer-Verlag, New York–Heidelberg, 1977.

[Ser79] J.-P. Serre, *Local Fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York–Berlin, 1979.

[Ser98] J.-P. Serre, *Abelian l-adic Representations and Elliptic Curves*, Research Notes in Mathematics, vol. 7, A K Peters, Ltd., Wellesley, MA, 1998, revised reprint of the 1968 original (W.A. Benjamin, Inc.).

[SwVo00] R. Swanson and H. Volkmer, *Invariants of weak equivalence in primitive matrices*, Ergodic Theory Dynam. Systems **20** (2000), 611–626.

[vdW91] B. L. van der Waerden, *Algebra, Vol. II*, Springer-Verlag, New York, 1991, Based in part on lectures by E. Artin and E. Noether, Translated from the fifth German edition by John R. Schulenberger.

[Wag99] J.B. Wagoner, *Strong shift equivalence theory and the shift equivalence problem*, Bull. Amer. Math. Soc. (N.S.) **36** (1999), 271–296.

[Wei98] E. Weiss, *Algebraic Number Theory*, Dover, Mineola, NY, 1998.

(O. Bratteli) Department of Mathematics, University of Oslo, PB 1053 – Blindern, N-0316 Oslo, Norway

E-mail address: bratteli@math.uio.no

(P.E. T. Jorgensen) Department of Mathematics, The University of Iowa, 14 MacLean Hall, Iowa City, IA 52242-1419, U.S.A.

E-mail address: jorgen@math.uiowa.edu

(K.H. Kim and F. Roush) Mathematics Research Group, Alabama State University, Montgomery AL 36101–0271, U.S.A.

E-mail address: kkim@asunet.alasu.edu, froush@asunet.alasu.edu