

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[§]

[†]*Department of Mathematics, University of Oslo, PB 1053—Blindern,
N-0316 Oslo, Norway
(e-mail: bratteli@math.uio.no)*

[‡]*Department of Mathematics, The University of Iowa, 14 MacLean Hall, Iowa City,
IA 52242-1419, USA
(e-mail: jorgen@math.uiowa.edu)*

[§]*Mathematics Research Group, Alabama State University,
Montgomery AL 36101-0271, USA
(e-mail: {kkim,froush}@asunet.alasu.edu)*

(Received 21 March 2001 and accepted in revised form 17 July 2001)

Abstract. The notion of isomorphism on 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. A 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. Special cases of this problem will be considered in a forthcoming paper.

0. Introduction

In [BJKR98] we studied an isomorphism of the stable AF-algebras associated with constant square primitive non-singular 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 non-singularity is removed. Special cases of the problem will be considered in [BJKR99b] from the viewpoint of numerical invariants. This is a sequel and will also appear in *Ergod. Th. & Dynamic. Sys.* The decision procedure is spelled out explicitly in §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 an 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 later).

The significance of this result goes well beyond the theory of AF-algebras, since the result may be viewed as a decision procedure for isomorphisms 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 non-trivial 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, 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 non-singular 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 §6.

By decidability of a class of problems, we will mean here 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 is zero or one here according to whether 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, although 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, try not 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, 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. In particular, [PoZa97, Wei98, 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 slightly more detail and discussion than is customary in a paper which does not cut across boundaries between fields.

In a subsequent paper, [BJKR99b], we will use the general algorithm given in §6 of this paper to derive special methods and invariants which are useful in deciding isomorphism in special cases. Other special cases, motivation, and much background material are contained in [BJO99].

1. Equivalent isomorphism conditions

Recall from [BJKR98] that two matrices A, B with non-negative 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 non-negative integer matrix entries such that the diagram (1.1) below commutes.

$$\begin{array}{ccc}
 & & \bullet \\
 & \searrow J(1) & \\
 \bullet & & \bullet \\
 \downarrow A^{n_1} & \swarrow K(1) & \downarrow B^{m_1} \\
 \bullet & & \bullet \\
 & \searrow J(2) & \\
 \bullet & & \bullet \\
 \downarrow A^{n_2} & \swarrow K(2) & \downarrow B^{m_2} \\
 \bullet & & \bullet \\
 & \searrow J(3) & \\
 \bullet & & \bullet \\
 \downarrow A^{n_3} & \swarrow K(3) & \downarrow B^{m_3} \\
 \bullet & & \bullet \\
 & \searrow J(4) & \\
 \vdots & & \vdots
 \end{array} \tag{1.1}$$

The diagram expresses the following two identities:

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

for $k = 1, 2, \dots$. This corresponds to an isomorphism of the associated stable AF-algebras [BJKR98, Bra72], and it corresponds to an 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 non-singular, but this extra condition can be dispensed with by a remedy described in §2. So assume that A and B are non-singular, 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 [BJKR99b, §5] 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 non-singular. This does not contradict the results in §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 non-zero integer, let $\text{Prim}(n)$ denote the set of prime factors of n . Then (1.2) implies

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

and thus (1.3) implies

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

Thus a necessary and sufficient condition for C^* -equivalence of two primitive, non-singular $(N \times N)$ matrices A , B with non-negative integer matrix entries is the existence of a (necessarily non-singular) matrix $J(1)$ with non-negative 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, BMT87] for details). Let $G(A)$ be the inductive limit of the sequence

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

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

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

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

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

and equip $G_n(A)$ with the order

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

(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 non-negative integers, and correspondingly,

G^+ means the non-zero positive elements of G and $G_+ = G^+ \cup \{0\}$.) Then $G_0 \subseteq G_1 \subseteq G_2 \subseteq \dots$ and we define

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

with the order defined by

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

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

$$J(1)G(A) = G(B) \quad (1.12)$$

and

$$J(1)G^+(A) = G^+(B); \quad (1.13)$$

see [BJO99, Proposition 11.7]. The one-to-one 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 $\theta: G(A) \rightarrow G(B)$, 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 $\mathbb{Q}[\lambda_{(A)}]$. Define $V(A)$ as the orthogonal complement of $v(A)$, i.e. $V(A) = \{x \in \mathbb{Q}[\lambda_{(A)}]^N \mid \langle v(A) \mid x \rangle = 0\} = v(A)^\perp$. 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 non-maximal generalized eigenvectors of A ; see (1.28). Thus

$$v(A)A = \lambda_{(A)}v(A), \quad Aw(A) = \lambda_{(A)}w(A), \quad \text{and} \\ \langle v(A) \mid V(A) \rangle = \{0\}, \quad \langle v(A) \mid w(A) \rangle \in \mathbb{Q}[\lambda_{(A)}] \cap (0, \infty). \quad (1.14)$$

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

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

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 $\langle v(A) \mid w(A) \rangle$ from (1.14) plays an important role in the discussion of the isomorphism problem in [BJKR99b, §1] and in [BJO99].

Let us mention an alternative form of the isomorphism criterion (1.12) and (1.13), formulated in [BJO99, Proposition 11.7]. Two primitive non-singular $(N \times N)$ matrices A, B with positive integer matrix entries are C^* -equivalent if and only if there is a non-singular $(N \times N)$ matrix $J = J(1)$ in $M_N(\mathbb{Z})$ satisfying the two conditions

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

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

$$B^m J A^{-n} \text{ and } A^m J^{-1} B^{-n} \text{ both have integer matrix entries; } \quad (1.17)$$

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 ensure 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

$$J \text{ has positive matrix entries.} \quad (1.16)'$$

(But again, a given J may satisfy (1.16) and (1.17) without having positive or integer matrix entries.) The combined two conditions (1.16) and (1.17) are equivalent to the two conditions (1.16)' and (1.17), and to (1.12) and (1.13). For this one uses Perron–Frobenius theory (see, e.g., [New72]): asymptotically when $m \rightarrow \infty$, 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) and (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 non-singular $(N \times N)$ matrix $J = J(1)$ in $M_N(\mathbb{Z})$ such that

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

$$B^m J A^{-n} \text{ and } A^m J^{-1} B^{-n} \text{ both have positive integer matrix entries.} \quad (1.18)$$

Thus the single condition (1.18) is equivalent to each of the three pairs of conditions (1.12) and (1.13); (1.16)' and (1.17); and (1.16) and (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 non-singular primitive $(N \times N)$ matrices with positive integer matrix entries, and assume that there is a non-singular 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*

for all positive integers n , the matrices

$$B^{kn+l} J A^{-n} \text{ and } A^{kn+l} J^{-1} B^{-n} \text{ both have positive integer matrix entries.} \quad (1.19)$$

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

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

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. Taking logarithms, we want

$$m \log \lambda_1 + \log C - n \log \lambda_2 > m \log \lambda_3 + \log(C_1 N^2) + n \log \lambda_4 \quad (1.21)$$

which can be rearranged equivalently as

$$m(\log \lambda_1 - \log \lambda_3) > -\log C + \log(C_1 N^2) + n(\log \lambda_2 + \log \lambda_4). \quad (1.22)$$

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

$$\frac{\log \lambda_2 + \log \lambda_4}{\log \lambda_1 - \log \lambda_3} \quad (1.23)$$

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 §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 $B^m JA^{-n}$. 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 non-negative 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 the diagonalization process, we will have algebraic integers. $\square$

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, §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

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

where

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

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

$$(x^2 - 13)(x^2 - 17)(x^2 - 221) \equiv 0 \pmod{p^k} \quad (1.25)$$

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

$$(x^2 - 13)(x^2 - 17)(x^2 - 221) = 0 \quad (1.26)$$

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 an 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 §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 $\bigcup_m A^{-m}(\mathbb{Z}^N)$ 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

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

where V_λ is the *generalized eigenspace*

$$V_\lambda = \{x \in V \mid \exists k \in \mathbb{Z}^+ \text{ s.t. } (\lambda - A)^k x = 0\}. \quad (1.28)$$

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

2. Reduction to non-singular 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 non-singular, and with a different definition of positivity in $G(A)$ and $G(B)$. The discussion of the general case when A is not assumed non-singular is resumed in [BJKR99b, §5].

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 non-singular 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 non-singular. 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

$$C = R^{-1}AR: \mathbb{Z}^M \longrightarrow \mathbb{Z}^M$$

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 non-zero 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 non-singular. $\square$

This mapping $A \mapsto C$ preserves unordered dimension groups. The lemma also shows that every unordered dimension group of an integer matrix (see [BJKR99b, equation (5.2)]) is the unordered dimension group of a non-singular 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 the 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 non-singular 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 $\langle vR \mid g' \rangle > 0$. In this way we consider the ordered dimension groups of a singular matrix as the unordered dimension group of a non-singular 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 non-singular matrix as we continue with the decision procedure in §5.

We will not need Theorems 6 and 7 from [BJKR98] directly in §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 [BJKR98] 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 $M^{(-1)}$ 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 $MM^{(-1)} = M^{(-1)}M$ 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 non-singular matrices. In effect, it is the ordinary inverse restricted to the non-zero generalized eigenspaces. Let D be the determinant of M restricted to the non-zero generalized eigenspaces, the product of its non-zero eigenvalues. Then the Drazin inverse has denominators which divide D^N . Use $M^{(-n)}$ 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 non-negative matrix $J(1)$ such that for all $d \in \mathbb{Z}_+$ there is a $c \in \mathbb{Z}_+$ such that*

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

and

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

are non-negative integer matrices.

Proof. Form the matrices $J(i), K(i)$, using the formulae (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 non-singular case, provided that we use the Drazin inverse. $\square$

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 intertwining 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

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

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

$$D_B = JD_A, \quad \tilde{D}_B = J\tilde{D}_A, \quad (3.2)$$

and hence

$$J\mathbb{R}D_A = \mathbb{R}D_B. \quad (3.3)$$

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

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

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 non-zero and gives non-trivial information about J . We would also like to exploit this idea 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

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

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

$$\mathbb{Z}[\lambda] \subset \mathbb{O}[\lambda] \subset \mathbb{Q}[\lambda]. \quad (3.6)$$

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 $\mathbb{O}[\lambda_{(A)}] = \mathbb{O}[\lambda_{(B)}]$. One other choice we shall use is

$$\Omega = \mathbb{O}[\lambda_1, \dots, \lambda_N, \mu_1, \dots, \mu_N], \quad (3.7)$$

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 :

$$\det(\lambda \mathbb{1} - A) = 0, \quad \det(\mu \mathbb{1} - B) = 0. \quad (3.8)$$

Our decision procedure will involve even other rings and fields. For example, in §4, 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, Ch. 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 less than one taken on by φ .

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

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

and

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

show that we may have non-unique 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 §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 §4 for definitions.) These field extensions may be identified by use of a Newton approximation scheme; see, e.g., [BoSh66, Ch. 1, §5] and [Wei98, Ch. 5]. For example, the field $\mathbb{Q}(\sqrt{-5})$ of (3.9) and (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, §1-2].

To make it clear when our primes refer to those in the standard set-up $\mathbb{Z} \subset \mathbb{Q}$, 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 $(x_i) \rightarrow (x_i^g)$, 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) and (1.17)), ((1.16)' and (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 $n \rightarrow \infty$. 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 $n \rightarrow \infty$. Since $n \rightarrow A^n \mathbb{Z}^N$ is decreasing, and

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

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

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

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

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

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) and (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

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

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 $(A^{kn_0})^2 = A^{kn_0}$ 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. $\square$

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 ,

$$(A^{e(m)})^2 = A^{e(m)} \bmod p^m M_N(\mathbb{Z}). \quad (4.5)$$

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

$$(B^{e(m)})^2 = B^{e(m)} \bmod p^m M_N(\mathbb{Z}). \quad (4.6)$$

But by the uniqueness of the idempotent, it follows that

$$m' > m \implies A^{e(m')} = A^{e(m)} \bmod p^m, \quad (4.7)$$

and hence, by passing to yet another subsequence,

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

exists in $M_N(\mathbb{Z}_{(p)})$, 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

$$B^{m_n} J = K_n A^n, \quad (4.9)$$

$$A^{m_n} = L_n B^n J. \quad (4.10)$$

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 $n \rightarrow \infty$ such that $\lim_n K_n = K$ and $\lim_n L_n = L$ exist in $M_N(\mathbb{Z}_{(p)})$, and we get from the relations above that

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

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

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

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

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 $\text{Prim}(\det(A)) = \text{Prim}(\det(B))$, then we can recover (1.17). Thus

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

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 non-singular matrices A, B be isomorphic, it is necessary and sufficient that $\text{Prim}(\det(A)) = \text{Prim}(\det(B))$, and that there exists a non-singular matrix $J \in \text{GL}(N, \mathbb{Z}[1/\det(A)])$ (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*

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

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

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 $\text{Prim}(A)$ 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, §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 non-rational 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, §§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 $\text{Prim}(\det(A))$.

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

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

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

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

As noted, this sum space is initially computed in F^N , for a finite-index field extension F . However, since $G_{(p)}(A) \subset (\mathbb{Z}_{(p)})^N$ 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 $p \in \text{Prim}(\det(A))$, then the existence of this embedding of fields $F \subset \mathbb{Q}_{(p)}$ is a non-trivial 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 non-zero as submodules in $(\mathbb{Z}_{(p)})^N$. 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, Ch. 1, §5]. The example in [BJKR99b, Example 6.4] further illustrates the point: the equation $x^2 = 2$ is solvable in $\mathbb{Z}_{(7)}$, and so we get a natural field embedding of $\mathbb{Q}[\sqrt{2}]$ 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, §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, Ch. 1, §6].

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

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

Then the matrix

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

defines an isomorphism of $G(A)$ onto $G(B)$. Since $2^n \rightarrow_{n \rightarrow \infty} 0$ 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

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

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

and

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

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, §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) and (1.13), (1.16) and (1.17), (1.16)' and (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 §2, i.e. we will henceforth assume in this section that A and B are non-singular 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 $\langle v(A) | g \rangle > 0$ or $g = 0$. We will, as partially explained in §3, work in various algebraic extensions R of $\mathbb{Z}$. The idea is roughly that if J satisfies (1.12):

$$J(1)G(A) = G(B), \quad (5.1)$$

then $J(1)$ also satisfies

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

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 §3). We will see in Proposition 5.4 that the conditions (5.1) and (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, §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 can be found in [PoZa97, §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 $\text{CC}[m_1, m_2, f]$ be the following set of congruence classes of matrices M :*

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

In words, $\text{CC}[m_1, m_2, f]$ 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 $\text{CC}[m_1, m_2, f]$.

Remark 5.2. The set $\text{CC}[m_1, m_2, f]$ 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 $\text{CC}[m_1, m_2, f]$ is that a matrix is in $G_{41}D_{41}G_{41}$

where

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

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, Ch. 2, 3, and §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, Ch. 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, Ch. 6]. These authors [PoZa97, Ch. 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 $\text{CC}[m_1, m_2, f]$. 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. $\square$

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 non-singular, 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 $\text{DGI}(A, B, R)$ 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 non-maximal 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 $(v(A)^\perp)^g$ is mapped into $(v(B)^\perp)^g$;
- (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) and (4.13), which is spanned by generalized row eigenvectors for eigenvalues not divisible by p .

Note that $\text{DGI}(A, B, R)$ 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 non-zero 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 feasibility we must decide. By linear algebra, as outlined in the next paragraph, we find a non-singular map J_0 over the rational numbers satisfying the first two conditions (α) and (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 $\text{DGI}(A, A, \mathbb{Q})$: $J(1) = J_0 J_a$. 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) and (iii) translate into congruence conditions and norm conditions on J_a :

- (i_a) $J_c J_a$ on the chosen maximal eigenvector $v(A)$ of A is non-zero modulo p_a (a fixed prime relatively prime to $\det(A)$, $\det(J_c)$, N_c);
- (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 ;
- (iii_a) the determinant of J_a is $N_c^N / \det(J_c)$ times a number dividing some power of $\det(A) \det(B)$;
- (iv_a)

$$J_c J_a \equiv 0 \pmod{N_c}. \quad (5.4)$$

The vector space $\text{DGI}(A, A, \mathbb{Q})$ 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, 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 non-singular 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 $\Gamma = \text{Gal}(K/\mathbb{Q})$ is the group of automorphisms g of K which fix $\mathbb{Q}$ pointwise, i.e. $x^g = x$ for $g \in \Gamma$ and $x \in \mathbb{Q}$. However, 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) and (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 $(v(A)^\perp)^g$ 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, e.g., 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

$$E(\pi_1) \cap E(\pi_2) \cap \cdots \cap E(\pi_n) \cap (v(A)^\perp)^{g_1} \cap (v(A)^\perp)^{g_2} \cap \cdots \cap (v(A)^\perp)^{g_k},$$

$$g_1, g_2, \dots, g_k \in \Gamma = \text{Gal}(K/\mathbb{Q}),$$

is a direct sum of generalized eigenspaces (if non-zero). 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 $\text{DGI}(A, A, K)$. 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 $\text{DGI}(A, A, K)$, all V_i are also invariant subspaces. It is not true that $\text{DGI}(A, A, K)$ 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 $\text{DGI}(A, A, K)$ has a block-triangular structure. The ideal $\mathcal{J} = \{M \in \text{DGI}(A, A, K) \mid MV_i \subset V_{i+1}, i = 0, \dots, l-1\}$ is a nilpotent ideal and $\text{DGI}(A, A, K)/\mathcal{J}$ has a natural embedding by the block structure into $\bigoplus_i \text{GL}(V_i/V_{i+1})$. 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. $\square$

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

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 $\mathbb{Q}$. $\square$

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 $\text{End}(E_1), \text{End}(E_2), \text{End}(E_3)$. 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 $\text{DGI}(A, A, \mathbb{Q})$ 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 $(v(A)^\perp)^g$'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 $\text{DGI}(A, A, K)$. 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 . Next, conjugation by J_f will put the matrices in $\text{DGI}(A, A, \mathbb{Q})$ 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 (i_a) , (ii_a) , (iii_a) , (iv_a) gives the corresponding formulae (i_g) , (ii_g) , (iii_g) , (iv_g) .

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

(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 .

(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 $\det(A) \det(B)$.

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

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

The first of these says that J_a is an integer matrix and the second is the same as (5) 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 N th 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 zero the kernel $\{x \in \mathcal{A} \mid \text{Trace}(xy) = 0, \forall y \in \mathcal{A}\}$, 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 that 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 $J_f^{-1} \text{DGI}(A, A, \mathbb{Q}) J_f$ and the congruences (i_g) , (ii_g) , (iv_g) , and the determinant condition (iii_g) .

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

$$\exists s \in S \ni x \equiv s \pmod{m} \quad (5.7)$$

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 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 A/J subject to any restrictions on the determinant, then we can solve any finite system of additive congruences on A subject to any restrictions on the determinant. More generally we can restate the congruences on A as congruences on A/J and use the same determinant conditions.*

Proof. Note that for our matrix representation the norm conditions on A will give norm conditions on 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 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 $x \equiv c - j_0 \pmod{m}$. $\square$

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 Propositions 5.5 and 5.7 in a way which is difficult to predict, we will not state the formulae 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 (i_h) , (ii_h) , (iv_h) , and a determinant condition (iii_h) . The conditions (ii) , and so on, will bound the powers of all primes occurring in the

determinants 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 $(i_g)-(iv_g)$, 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 (i_h) , (ii_h) , (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 . 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. $\square$

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 non-singular matrices by the method in §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 $J_a \in \text{DGI}(A, A, \mathbb{Q}) \cap M_N(\mathbb{Z})$ meeting corresponding conditions (we multiply by a constant N_c to arrange that J_a has integer entries). We find the Jacobson radical of $\text{DGI}(A, A, \mathbb{Q})$ 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, (i_h) , (ii_h) , (iv_h) , and a determinant condition (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. $\square$

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 non-singular 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 non-singular matrices which henceforth replace A, B . The rank of the two non-singular matrices must have the same value N , otherwise the algorithm stops.
- II. Determine the eigenspace structure of A, B (a general reference for steps 6 and 6 is [Jac75, Ch. 1, §§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 $\text{DGI}(A, B, K)$ and $\text{DGI}(A, B, \mathbb{Q})$.
 - (a) From step 6, 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 $E(\pi)(A), E(\pi)(B), (v(A)^\perp)^g, (v(B)^\perp)^g$.
 - (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 $(v(A)^\perp)^g$ onto $(v(B)^\perp)^g$ 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 non-zero 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 $J_a \in \text{DGI}(A, A, \mathbb{Q})$ and restate (i), (ii), (iii) as conditions on the hypothetical J_a . This gives (i_a), (ii_a), (iii_a), (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 $\text{DGI}(A, A, K)$ which arises from this, the ideal J of maps which send each $V_i \rightarrow V_{i+1}$. Compute the isomorphism $\text{DGI}(A, A, K) \rightarrow \sum_i \text{GL}(V_i/V_{i+1})$. (This is Proposition 5.4.)
 - (c) Compute the isomorphism from the Galois invariant elements of $\text{DGI}(A, A, K)/J$ 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 $\text{DGI}(A, A, \mathbb{Q})$ which arises from step 6. The map is a conjugation by some matrix J_f and we have conditions (i_g), (ii_g), (iii_g), (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 (i_h), (ii_h), (iii_h), (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) 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 $G_{41}F_{41}G_{41}$.

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. 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 non-singular matrices explicit. PETJ 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 their support and hospitality.

This work was supported by US NSF grants DMS9900265 (KHK, FR) and DMS9700130 (PETJ), and by the Norwegian NFR (Norges Forskningsråd) and the University of Oslo, Norway (OB, PETJ).

*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. Math.* **83**(2) (1966), 437–456.
- [Bla86] B. Blackadar. *K-theory for Operator Algebras (MSRI Publication Series, 5)*. Springer, New York–Heidelberg–Berlin–Tokyo, 1986.

- [BoSh66] Z.I. Borevich and I.R. Shafarevich. *Number Theory (Pure and Applied Mathematics, 20)*. Academic Press, New York–London, 1966. Translated from the Russian *Teoriya Chisel*, Moscow, 1964, by N. Greenleaf.
- [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.
- [Bra72] O. Bratteli. Inductive limits of finite dimensional C^* -algebras. *Trans. Amer. Math. Soc.* **171** (1972), 195–234.
- [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. *Ergod. Th. & Dynam. Sys.* **20** (2000), 1639–1656.
- [BJKR99b] O. Bratteli, P. E. T. Jorgensen, K. H. Kim and F. Roush. Computation of isomorphism invariants for stationary dimension groups, accepted by *Ergod. Th. & Dynam. Sys.*, and to appear as a sequel.
- [BJO99] O. Bratteli, P. E. T. Jorgensen and V. Ostrov's'kyi. Representation theory and numerical AF-invariants: the representations and centralizers of certain states on $\mathcal{O}_d$. *Mem. Amer. Math. Soc.* submitted
- [Buc86] J. Buchmann. *Generalized Continued Fractions and Number Theoretic Computations (Berichte der Mathematisch-Statistischen Sektion in der Forschungsgesellschaft Joanneum, 269)*. Forschungszentrum Graz Mathematisch-Statistische Sektion, Graz, 1986, Paper from the sixteenth Styrian mathematical symposium held in Stift Rein/Graz, September 21–26, 1986.
- [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) (Proc. Symp. in Pure Mathematics, 28)*. Ed. F. E. Browder. American Mathematical Society, Providence, RI, 1976, pp. 323–378.
- [DHS99] F. Durand, B. Host and S. Skau. Substitutional dynamical systems, Bratteli diagrams, and dimension groups. *Ergod. Th. & Dynam. Sys.* **19** (1999), 953–993.
- [Eff81] E. G. Effros. *Dimensions and C^* -algebras (CBMS Regional Conf. Series in Mathematics, 46)*. Conference Board of the Mathematical Sciences, Washington, 1981.
- [Eli76] G. A. Elliott. On the classification of inductive limits of sequences of semisimple finite-dimensional algebras. *J. Algebra* **38** (1976), 29–44.
- [GrSe80a] F. Grunewald and D. Segal. Some general algorithms, I: Arithmetic groups. *Ann. Math.* **112**(2) (1980), 531–583.
- [GrSe80b] F. Grunewald and D. Segal. Some general algorithms, II: Nilpotent groups. *Ann. Math.* **112**(2) (1980), 585–617.
- [Han81] D. Handelman. Positive matrices and dimension groups affiliated to C^* -algebras and topological Markov chains. *J. Operator Theory* **6** (1981), 55–74.
- [Her69] H. Hermes. *Enumerability, Decidability, Computability: An Introduction to the Theory of Recursive Functions*. Springer, 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] H. Hermes. *Aufzählbarkeit, Entscheidbarkeit, Berechenbarkeit: Einführung in die Theorie der rekursiven Funktionen*, 3rd edn. Springer, Berlin, 1978.
- [HiSi00] M. Hindry and J. H. Silverman. *Diophantine Geometry: An Introduction (Graduate Texts in Mathematics, 201)*. Springer, New York, 2000.
- [Jac97] J. Jacklitch. Homeomorphisms of 1-dimensional hyperbolic attractors. *Thesis Preprint*, 1997, see also *Geometry and Topology in Dynamics* (Winston-Salem, NC, 1998/San Antonio) *Contemp. Math.* **246** (1999), 1–15.
- [Jac75] N. Jacobson. *Lectures in Abstract Algebra, Vol. III: Theory of Fields and Galois Theory (Graduate Texts in Mathematics, 32)*. Springer, New York–Heidelberg, 1975, second corrected printing.
- [Kap69] I. Kaplansky. *Infinite Abelian Groups*, revised edn. The University of Michigan Press, Ann Arbor, 1969.
- [KaMa51] I. Kaplansky and G. W. Mackey. A generalization of Ulm's theorem. *Summa Brasil. Math.* **2** (1951), 195–202.
- [Kit98] B. P. Kitchens. *Symbolic Dynamics: One-sided, Two-sided and Countable State Markov Shifts*. Universitext, Springer, Berlin, 1998.

- [KiRo79] K. H. Kim and F. W. Roush. Some results on decidability of shift equivalence. *J. Combin. Inform. Syst. Sci.* **4** (1979), 123–146.
- [KiRo88] K. H. Kim and F. W. Roush. Decidability of shift equivalence. *Dynamical Systems (College Park, MD, 1986–87) (Lecture Notes in Mathematics, 1342)*. Ed. J. C. Alexander. Springer, Berlin–New York, 1988, pp. 374–424.
- [Knu81] D. E. Knuth. *The Art of Computer Programming: Vol. 2: Seminumerical Algorithms*, 2nd edn. Addison-Wesley Publishing Co., Reading, MA, 1981.
- [Kob84] N. Koblitz. *p -adic Numbers, p -adic Analysis, and Zeta-Functions (Graduate Texts in Mathematics, 58)*, 2nd edn. Springer, 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, 45)*. Academic Press, New York–London, 1972.
- [PaTa95] J. Palis and F. Takens. *Hyperbolicity and Sensitive Chaotic Dynamics at Homoclinic Bifurcations (Cambridge Studies in Advanced Mathematics, 35)*. Cambridge University Press, 1993.
- [PoZa97] M. Pohst and H. Zassenhaus. *Algorithmic Algebraic Number Theory (Encyclopedia of Mathematics and its Applications, 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*, 2nd edn. Universitext, Springer, New York, 1998.
- [Ser77] J.-P. Serre. *Linear Representations of Finite Groups (Graduate Texts in Mathematics, 42)*. Springer, New York–Heidelberg, 1977.
- [Ser79] J.-P. Serre. *Local Fields (Graduate Texts in Mathematics, 67)*. Springer, New York–Berlin, 1979.
- [Ser98] J.-P. Serre. *Abelian l -adic Representations and Elliptic Curves (Research Notes in Mathematics, 7)*. A K Peters, Ltd., Wellesley, MA, 1998, revised reprint of the 1968 original by W. A. Benjamin, Inc.
- [SwVo00] R. Swanson and H. Volkmer. Invariants of weak equivalence in primitive matrices. *Ergod. Th. & Dynam. Sys.* **20** (2000), 611–626.
- [vdW91] B. L. van der Waerden. *Algebra, Vol. II*. Springer, 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.