Symmetries and Reversing Symmetries of Toral Automorphisms

MICHAEL BAAKE[1)] and JOHN A. G. ROBERTS[2)]

1) Institut für Theoretische Physik, Universität Tübingen,
Auf der Morgenstelle 14, 72076 Tübingen, Germany[1]
michael.baake@uni-tuebingen.de

2) Department of Mathematics, La Trobe University,
VIC 3086, Australia[2]
jag.roberts@latrobe.edu.au

Abstract

Toral automorphisms, represented by unimodular integer matrices, are investigated with respect to their symmetries and reversing symmetries. We characterize the symmetry groups of $\mathrm{GL}(n,\mathbb{Z})$ matrices with simple spectrum through their connection with unit groups in orders of algebraic number fields. For the question of reversibility, we derive necessary conditions in terms of the characteristic polynomial and the polynomial invariants. We also briefly discuss extensions to (reversing) symmetries within affine transformations, to $\mathrm{PGL}(n,\mathbb{Z})$ matrices, and to the more general setting of integer matrices beyond the unimodular ones.

Introduction

Unimodular integer $n \times n$ matrices form the matrix group $\mathrm{GL}(n,\mathbb{Z})$. The hyperbolic elements (i.e. those having no eigenvalues on the unit circle) induce interesting dynamical systems (the so-called "cat maps") on the n-dimensional torus, such as the famous example with $n = 2$ in [6, Ch. 1, Ex. 1.16]:

$$M \;=\; \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} . \tag{1}$$

[1]Address from April 1, 2001: Institut für Mathematik und Informatik, Universität Greifswald, Jahnstr. 15a, 17487 Greifswald, Germany; mbaake@mail.uni-greifswald.de

[2]Address from July 1, 2001: School of Mathematics, The University of New South Wales, Sydney, NSW 2052, Australia

Such hyperbolic toral automorphisms are examples of hyperbolic dynamical systems that are ergodic and mixing [34], and also are topological Anosov systems [14], hence of interest in the theory of Smale spaces.

Although induced from a linear system of ambient n-dimensional (affine) space, the dynamics of unimodular hyperbolic integer matrices on the n-dimensional torus is rather complicated. Even so, the fact that the dynamics on the torus is generated by a simple linear object means that such systems serve as model systems in symbolic dynamics (e.g. [1, 14, 3]) and in many applications, and there is an enormous literature on them, see [23]. Also, in the physics literature, cat maps are a popular area of study since they can be quantized and their quantum and semiclassical properties identified (e.g. [37, 24] and refs. therein). In this respect, there is also interest in studying the spectral statistics of nonlinearly perturbed cat maps in connection with probing the relationship between the spectral statistics of random matrix theory and the presence or absence of certain symmetries [25].

Hyperbolic toral automorphisms also play a prominent role in the theory of quasicrystals through their appearance as inflation symmetries, see [8, 10] and references therein. Formulated for tilings, this means that a certain dissection of the tiles into smaller homothetic copies of themselves, followed by a global blowup of the entire tiling, brings the tiling back to itself. In an underlying higher-dimensional space, from which the tilings emerge by a projection method, this inflation symmetry is then a lattice automorphism, and hence represented by an integer matrix. Furthermore, in the one-dimensional case, these symmetries give rise to interesting non-linear dynamical systems called *trace maps* [9, 38, 17] that have extensively been used to study the physical properties of one-dimensional quasicrystals.

Symmetry is a much studied concept in both group theory and dynamical systems and our purpose here is to address this for (hyperbolic) toral automorphisms. For a dynamical system, it is always helpful to know the symmetries and reversing (or time-reversal) symmetries to gain information on the dynamics [40, 28]. If the dynamical system is F, an automorphism of some topological space (e.g. some manifold) to itself, then an automorphism G is called a *symmetry* of F if it conjugates F to itself (i.e. G commutes with F), and a *reversing symmetry* of F if it conjugates F to its inverse (equivalently, its time-reverse) F^{-1}.

Taken together, the symmetries and reversing symmetries of F form a group $\mathcal{R}(F)$ and in some recent articles [11, 12, 19, 39, 41] group theoretic and algebraic methods have been employed to study the structure of $\mathcal{R}(F)$ in general, or for specific groups of dynamical systems. This entails restricting the search for possible (reversing) symmetries of F to some (seemingly) natural set. For hyperbolic toral automorphisms, this is made very neat via

Fact 1 [4] *Two toral automophisms generated by elements M_1 and M_2 of* $\mathrm{GL}(n,\mathbb{Z})$

are topologically conjugate via a homeomorphism h of the torus if and only if M_1 and M_2 are conjugate in $\mathrm{GL}(n, \mathbb{Z})$*. Furthermore, if M_1 and M_2 are hyperbolic, then h corresponds to the action of an element M_h of* $\mathrm{GL}(n, \mathbb{Z})$*, or to the affine extension, with a rational translation, of such an element. In either case, M_h then conjugates M_1 to M_2 in* $\mathrm{GL}(n, \mathbb{Z})$. □

This result reduces the analysis of (reversing) symmetries of hyperbolic toral automorphisms to the study of conjugacy in the matrix group $\mathrm{GL}(n, \mathbb{Z})$, a problem of independent interest.

In the case of $\mathrm{GL}(2, \mathbb{Z})$ and $\mathrm{PGL}(2, \mathbb{Z})$, we previously gave a rather complete classification, see [12] for a detailed account or [11, 7] for a summary (see also [2] for related work). The main difficulty of studying similarity when the matrix entries are restricted to integers is that one can no longer refer to the usual normal forms of matrices over $\mathbb{C}$ or $\mathbb{R}$, but has to use discrete methods instead. Fortunately, there is a strong connection with algebraic number theory, see [44] for an introduction, and this connection is certainly not restricted to the two-dimensional situation.

It is thus the aim of this article to extend the conjugacy investigations of our earlier article [12] to the setting of matrices in $\mathrm{GL}(n, \mathbb{Z})$. The answers will be less complete and also less explicit, but the connection to unit groups in orders of algebraic number fields is still strong enough to give quite a number of useful and general results, both on symmetries and reversing symmetries. Our main results are Theorem 1 in Section 2.1 for symmetries, and Theorems 2 and 3 in Section 2.3 for reversing symmetries. From a purely algebraic point of view, the results derived below are actually rather straight-forward. However, these results, and the methods used to derive them, are not at all common in the dynamical systems community. Therefore, this article is also meant to introduce and review some of these techniques, and we try to spell out the details or give rather precise references at least. Furthermore, as with our article [12], the results of this paper have relevance to both the dynamics community and to the quasicrystal community.

Some results in the literature which are related to our study here are as follows. In [33], it is shown that for an open and dense subset of hyperbolic automorphisms of the n-dimensional torus, their set of symmetries is trivial, i.e. just powers of the map (up to a factor ± 1). Very recently, the authors of [22] have considered certain classes of $\mathbb{Z}^d$-actions ($d \geq 2$) by toral automorphisms. Some of the results, in particular on centralizers of these actions, have a similar flavour to ours. Furthermore, [22] is concerned with various levels of conjugacy between these actions, including *measure-theoretic* conjugacy. The relation of this with topological conjugacy and algebraic conjugacy (i.e. conjugacy within $\mathrm{GL}(n, \mathbb{Z})$) was previously addressed in [3, 14]. For example, it follows from these references that, whenever hyperbolic matrices M_1 and M_2 in $\mathrm{GL}(n, \mathbb{Z})$ have the same value of *entropy* (which can be calculated from their eigenvalues), then the induced toral automorphisms are *measure-theoretically* conjugate even though they may not be algebraically or topologically conjugate. This result involves the construction of Markov partitions for hyperbolic toral automorphisms, another active area at present [1].

The article is organized as follows. We start with a section on the background material, including the group theoretic setup we use and a recollection of those results from algebraic number theory that we will need later on. Section 2 is the main part of this article. Here, we derive the structure of the symmetry group of toral automorphisms with simple spectrum and discuss reversibility. Section 3 extends the set of possible symmetries to affine transformations and summarizes the analogous problem for projective matrices. It also discusses the extension of (reversing) symmetries to matrices that are no longer unimodular.

1 Setting the scene

In this Section, we explain in more detail what we mean by symmetries and reversing symmetries, and we also recall some results from algebra and algebraic number theory that we will need.

1.1 Symmetries and reversing symmetries

For a general setting, consider some (topological) space Ω, and let $\mathrm{Aut}(\Omega)$ be its group of homeomorphisms or, more generally, a subgroup of homeomorphisms of Ω which preserve some additional structure of Ω. Consider now an element $F \in \mathrm{Aut}(\Omega)$ which, by definition, is invertible. Then, the group

$$\mathcal{S}(F) \; := \; \{G \in \mathrm{Aut}(\Omega) \mid G \circ F = F \circ G\} \tag{2}$$

is called the *symmetry group* of F in $\mathrm{Aut}(\Omega)$. In group theory, it is called the *centralizer* of F in $\mathrm{Aut}(\Omega)$, denoted by $\mathrm{cent}_{\mathrm{Aut}(\Omega)}(F)$. This group certainly contains all powers of F, but often more.

Quite frequently, one is also interested in mappings $R \in \mathrm{Aut}(\Omega)$ that conjugate F into its inverse,

$$R \circ F \circ R^{-1} \; = \; F^{-1} \, . \tag{3}$$

Such an R is called a *reversing symmetry* of F, and F is then called reversible. We will, in general, not use different symbols for symmetries and reversing symmetries from now on, because together they form a group,

$$\mathcal{R}(F) \; := \; \{G \in \mathrm{Aut}(\Omega) \mid G \circ F \circ G^{-1} = F^{\pm 1}\} \, , \tag{4}$$

the so-called *reversing symmetry group* of F, see [26] for details. If $\langle F \rangle$ denotes the group generated by F, $\mathcal{R}(F)$ is a subgroup of the *normalizer* of $\langle F \rangle$ in $\mathrm{Aut}(\Omega)$.

There are two possibilities: either $\mathcal{R}(F) = \mathcal{S}(F)$ (if F is an involution or if it has no reversing symmetry) or $\mathcal{R}(F)$ is a C_2-extension (the cyclic group of order 2) of $\mathcal{S}(F)$ which means that $\mathcal{S}(F)$ is a normal subgroup of $\mathcal{R}(F)$ and the factor group is

$$\mathcal{R}(F)/\mathcal{S}(F) \;\simeq\; C_2 \,. \tag{5}$$

The underlying algebraic structure has fairly strong consequences. One is that reversing symmetries cannot be of odd order [26], another one is the following product structure [12, Lemma 2].

Fact 2 *If F (with $F^2 \neq Id$) has an involutory reversing symmetry R, the reversing symmetry group of F is given by*

$$\mathcal{R}(F) \;=\; \mathcal{S}(F) \times_s C_2 \,, \tag{6}$$

i.e. it is a semi-direct product.[3] □

We can say more about the structure of $\mathcal{R}(F)$ if we restrict the possibilities for $\mathcal{S}(F)$, e.g. if we assume that $\mathcal{S}(F) \simeq C_\infty$ or $\mathcal{S}(F) \simeq C_\infty \times C_2$ with the C_2 being a subgroup of the centre of $\mathrm{Aut}(\Omega)$, compare also [19] for a group theoretic discussion. This situation will appear frequently below.

1.2 (Reversing) symmetries of powers of a mapping

In what follows, we summarize some of the concepts and results of Ref. [27] and, in particular, Ref. [26]. It may happen that some power of F has more symmetries than F itself (we shall see examples later on), i.e. $\mathcal{S}(F^k)$ (for some $k > 1$) is larger than $\mathcal{S}(F)$ which is contained as a subgroup. The analogous possibility exists for $\mathcal{R}(F^k)$ versus $\mathcal{R}(F)$. In such a situation, we say that F possesses additional (reversing) k-symmetries.

It is trivial that mappings F of finite order (with $F^k = Id$, say) possess the entire group $\mathrm{Aut}(\Omega)$ as k-symmetry group. Let us thus concentrate on mappings $F \in \mathrm{Aut}(\Omega)$ of *infinite* order. We denote by $\mathcal{S}_\infty(F)$ the set of automorphisms that commute with *some* positive power of F. This set can be seen as the inductive limit of $\mathcal{S}(F^k)$ as $k \to \infty$, with divisibility as partial order on $\mathbb{N}$, and $\mathcal{S}_\infty(F)$ is thus a subgroup of $\mathrm{Aut}(\Omega)$. Let $\#_F(G)$ denote the minimal k such that $G \circ F^k = F^k \circ G$. Then

$$\mathcal{S}_\infty(F) \;=\; \{\, G \in \mathrm{Aut}(\Omega) \mid \#_F(G) < \infty \,\} \,. \tag{7}$$

[3] We use $N \times_s H$ for the semi-direct product of two groups N and H, with N being the normal subgroup.

Of course it may happen that $\#_F(G) \equiv 1$ on $\mathcal{S}_\infty(F)$ which means that no power of F has additional symmetries. On the other hand, if $\#_F(G) > 1$, we call G a genuine or true[4] k-symmetry. This happens if and only if the mapping $G \mapsto F \circ G \circ F^{-1}$ generates a proper k-cycle. We shall meet this phenomenon later on.

Quite similarly, one defines reversing k-symmetries and their orbit structure [26], but we will not expand on that here.

1.3 Some recollections from algebraic number theory

Much of what we state and prove below can be seen as an application of several well-known results from algebraic number theory. The starting point is the connection between algebraic number theory and integral matrices, see [44] for an introduction.

To fix notation, let $\mathrm{Mat}(n, \mathbb{Z})$ denote the ring of integer[5] $n \times n$-matrices. An element M of it is called *unimodular* if $\det(M) = \pm 1$, and the subset of all unimodular matrices forms the group $\mathrm{GL}(n, \mathbb{Z})$. For the *characteristic polynomial* of a matrix M, we use the convention

$$P(x) \;:=\; \det(x\mathbf{1} - M) \;=\; \prod_{i=1}^{n} (x - \lambda_i) \tag{8}$$

where $\lambda_1, \dots, \lambda_n$ denote the eigenvalues of M. With this convention, $P(x)$ is *monic*, i.e. its leading coefficient is 1. If M is an integer matrix, $P(x)$ has integer coefficients only, so all eigenvalues of M are *algebraic integers*. Conversely, the set of algebraic integers, which we denote by $\mathcal{A}$, consists of all numbers that appear as roots of monic integer polynomials.

To show the intimate relation more clearly, let us recall the following property (see item (b) on p. 306 of [44]):

Fact 3 *Let $P(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ be a monic polynomial with integer coefficients a_i which is irreducible over $\mathbb{Z}$. Let α be any root of it, and A an integer matrix that has $P(x)$ as its characteristic polynomial. Then, the rings $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[A]$ are isomorphic.* $\square$

We write $\mathbb{Z}[x]$ for the ring of polynomials in x with $\mathbb{Z}$-coefficients, see [29, p. 90] for details. Clearly, Fact 3 also extends to the isomorphism of the polynomial rings $\mathbb{Q}[\alpha]$ and $\mathbb{Q}[A]$. We refer to [29, Ch. IV] for background material. Let us only add

[4] Although the distinction between true and other k-symmetries is necessary in general, we shall usually drop the attribute "true" whenever misunderstandings are unlikely.

[5] Here, and in what follows, integer means rational integer, i.e. an integer in $\mathbb{Q}$. Other kinds of integers, such as algebraic, will be specified explicitly.

that a polynomial in $\mathbb{Z}[x]$ is irreducible over $\mathbb{Z}$ if and only if it is irreducible over $\mathbb{Q}$, see [29, Thm. IV.2.3].

Let $P(x)$ be any (i.e. not necessarily irreducible) monic integer polynomial of degree n. In general, there are many different matrices A which have $P(x)$ as their characteristic polynomial, and even different matrix *classes* (we say that $A, B \in \mathrm{Mat}(n, \mathbb{Z})$ belong to the same matrix class if they are conjugate by a $\mathrm{GL}(n, \mathbb{Z})$-matrix C, i.e. $A = CBC^{-1}$). Let us recall the following helpful result on the number of matrix classes, see [44, Thm. 5] for details:

Fact 4 *Let $P(x)$ be a monic polynomial of order n with integer coefficients that is irreducible over $\mathbb{Z}$, and let α be any of its roots. Then the number of matrix classes generated by matrices $A \in \mathrm{Mat}(n, \mathbb{Z})$ with $P(A) = 0$ equals the number of ideal classes (or class number, for short) of the order $\mathbb{Z}[\alpha]$. In particular, this class number is finite, and it is larger than or equal to the class number of the maximal order $\mathcal{O}_{\max}$ of $\mathbb{Q}(\alpha)$.* □

Let us explain some of the terms used here. If α is an algebraic number, $\mathbb{Q}(\alpha)$ denotes[6] the smallest field extension of the rationals that contains α. Its degree, n, is the degree of the irreducible monic integer polynomial that has α as its root. The set $\mathcal{O}_{\max} := \mathbb{Q}(\alpha) \cap \mathcal{A}$ is the ring of (algebraic) integers in $\mathbb{Q}(\alpha)$, and is called its *maximal order*. More generally, a subring $\mathcal{O}$ of $\mathcal{O}_{\max}$ is called an *order*, if it contains 1 and if its rational span, $\mathbb{Q}\mathcal{O}$, is all of $\mathbb{Q}(\alpha)$. A subset of $\mathcal{O}$ is called an *ideal* if it is both a $\mathbb{Z}$-module (i.e. closed under addition and subtraction) and closed under multiplication by arbitrary numbers from $\mathcal{O}$. The ideals come in classes that are naturally connected to the matrix classes introduced above, see [16, 44] for further details.

An element $\varepsilon \in \mathbb{Q}(\alpha)$ is called a *unit* (or, more precisely[7], a unit in $\mathcal{O}_{\max}$) if both ε and its inverse, ε^{-1}, are algebraic integers and hence are in $\mathcal{O}_{\max}$. This happens if and only if the corresponding matrix is unimodular, i.e. if any monic integer polynomial $P(x)$ that has ε as a root has coefficient $a_0 = \pm 1$. So, matrices in $\mathrm{GL}(n, \mathbb{Z})$ and units in algebraic number fields are two facets of the same coin. The units of $\mathcal{O}_{\max}$ form a group under multiplication, denoted by $\mathcal{O}_{\max}^{\times}$ in the sequel. Similarly, if $\mathcal{O} \subset \mathcal{O}_{\max}$ is any order of $\mathbb{Q}(\alpha)$, we write $\mathcal{O}^{\times}$ for its group of units, which is then a subgroup of $\mathcal{O}_{\max}^{\times}$.

Independently of whether the monic polynomial $P(x)$ is irreducible or not, there is always at least one matrix which has characteristic polynomial $P(x)$, namely the

[6] Note the difference between the meaning of $\mathbb{Q}[\alpha]$ and $\mathbb{Q}(\alpha)$.

[7] This distinction is useful if orders other than $\mathcal{O}_{\max}$ appear.

so-called (left) *companion matrix*:

$$A^{(\ell)} \;=\; \begin{pmatrix} 0 & 1 & & & \mathbf{0} \\ 0 & 0 & 1 & & \\ \vdots & & \ddots & \ddots & \\ 0 & \cdot & \cdot & 0 & 1 \\ -a_0 & \cdot & \cdot & -a_{n-2} & -a_{n-1} \end{pmatrix}. \tag{9}$$

Consequently, the class number is ≥ 1 (if $P(x)$ is irreducible, the companion matrix actually corresponds to the principal ideal class, see [44, Thm. 9]). Another obvious choice, always belonging to the same matrix class, is the (right) companion matrix, $A^{(r)}$, obtained from $A^{(\ell)}$ by reflection in both diagonal and anti-diagonal, i.e.

$$A^{(r)} \;=\; RA^{(\ell)}R \tag{10}$$

with the involution

$$R \;=\; \begin{pmatrix} \mathbf{0} & & 1 \\ & \cdot^{\cdot^{\cdot}} & \\ 1 & & \mathbf{0} \end{pmatrix}. \tag{11}$$

This matrix will reappear several times in what follows.

2 $\mathrm{GL}(n, \mathbb{Z})$ matrices and toral automorphisms

Let us generally assume that $n \geq 2$. The toral automorphisms of the n-torus $\mathbb{T}^n := \mathbb{R}^n/\mathbb{Z}^n$ can be represented by the unimodular $n \times n$-matrices with integer coefficients which form the group $\mathrm{GL}(n, \mathbb{Z})$. It now plays the role of $\mathrm{Aut}(\Omega)$ from Section 1.1. Note that the elements of $\mathrm{GL}(n, \mathbb{Z})$ preserve the linear structure of the torus.

2.1 Symmetries

The first thing we will look at, given a toral automorphism $M \in GL(n, \mathbb{Z})$, is its symmetry group within the class of toral automorphisms. So, we want to determine the centralizer of M in $\mathrm{GL}(n, \mathbb{Z})$,

$$\mathcal{S}(M) \;=\; \mathrm{cent}_{\mathrm{GL}(n,\mathbb{Z})}(M) \;=\; \{G \in \mathrm{GL}(n, \mathbb{Z}) \;\mid\; MG = GM\}. \tag{12}$$

To be more precise, we are mainly interested in the structure of the symmetry group rather than in explicit sets of generators and relations. The former is invariant under conjugation, i.e. if we know it for an element M, we also know it for any other element of the form BMB^{-1} because

$$\mathcal{S}(BMB^{-1}) \;=\; B\,\mathcal{S}(M)\,B^{-1}\,. \tag{13}$$

The characteristic polynomial (8) of a matrix $M \in \mathrm{GL}(n,\mathbb{Z})$ is monic and has integer coefficients, so its roots are algebraic integers. Two principal situations can occur: the polynomial is either *reducible* over $\mathbb{Z}$ (which happens if and only if one of the eigenvalues of M, and hence all, is an algebraic integer of degree less than n) or it is *irreducible*. In the latter case, since we are working over $\mathbb{Q}$ (which has characteristic zero and is thus a perfect field), we know that the roots must be pairwise distinct [29, Cor. V.6.12]. So we have

Fact 5 *Let M be an integer matrix with irreducible characteristic polynomial. Then M is simple and hence diagonalizable over $\mathbb{C}$.* $\square$

Here, M is called *simple* if it has no repeated eigenvalues (which is also called separable elsewhere). This case will be dealt with completely.

If the characteristic polynomial is reducible, the matrix can still be simple, and we will see the general answer for this case, too. Beyond that, M can either be semi-simple (i.e. diagonalizable over $\mathbb{C}$) or not, and we will not be able to say much about this case. This is really not surprising, as this situation is closely related to the rather difficult classification problem of crystallographic point groups, see [15] for answers in dimensions ≤ 4 and [35] for a recent survey.

Let us now state one further prerequisite for tackling the symmetry question. In view of later extensions, we do this in slightly more generality than needed in the present section. Recall that an $n\times n$-matrix M, acting on a vector space V, is called *cyclic*, if a vector $v \in V$ exists such that $\{v, Mv, M^2v, \dots, M^{n-1}v\}$ is a basis of V. Also, the monic polynomial Q of minimal degree that annihilates M, i.e. $Q(M) = 0$, is called the *minimal polynomial* of M. By the Cayley-Hamilton theorem [29, Thm. XIV.3.1], Q always is a factor of the characteristic polynomial of M.

Fact 6 *Let $M \in \mathrm{Mat}(n,\mathbb{Q})$ be a rational matrix, with characteristic polynomial $P(x)$ and minimal polynomial $Q(x)$. Then the following assertions are equivalent.*

(*a*) *The matrix M is cyclic.*

(*b*) *The degree of $Q(x)$ is n.*

(*c*) $P(x) = Q(x)$.

(*d*) $G \in \mathrm{Mat}(n,\mathbb{Q})$ *commutes with* $M \iff G \in \mathbb{Q}[M]$.

Proof: A convenient source is [21, Ch. III]. The equivalence of statements (a) to (c) is a consequence of Thm. III.2. The equivalence of (a) with (d) follows from Thm. III.17, and the Corollary following it, together with the Corollary of Ch. III.17. Alternatively, see [5, Cor. 5.5.16]. $\square$

Let us add a general example here. If K is a field and $M \in \mathrm{GL}(n, K)$ *any* invertible matrix, it clearly commutes with its inverse, M^{-1}. The latter can now always be written as a K-polynomial in M. Explicitly, let us write the minimal polynomial as $Q(x) = \sum_{\ell=0}^{r} a_\ell \, x^\ell$, where $r \leq n$, $a_r = 1$ and $a_0 \neq 0$. Then

$$M^{-1} \; = \; -\frac{1}{a_0} \sum_{\ell=0}^{r-1} a_{\ell+1} M^\ell \, . \tag{14}$$

Using $Q(M) = 0$, the verification of $M^{-1}M = \mathbf{1}$ is a straight-forward calculation.

Lemma 1 *Let $M \in \mathrm{GL}(n, \mathbb{Z})$ have a characteristic polynomial $P(x)$ that is irreducible over $\mathbb{Z}$, and let λ be a root of $P(x)$. Then the centralizer of M in $\mathrm{GL}(n, \mathbb{Z})$ is isomorphic to a subgroup of finite index of $\mathcal{O}^\times_{\max}$, the unit group in the ring of integers of the algebraic number field $\mathbb{Q}(\lambda)$.*

Proof: By assumption, $P(x)$ is also the minimal polynomial of M, so any $\mathrm{GL}(n, \mathbb{Z})$-matrix which commutes with M is, by Fact 6, a polynomial in M with rational coefficients. Consequently, $\mathcal{S}(M)$ is isomorphic to a subset of $\mathbb{Q}[M]$ that forms a group under (matrix) multiplication.

Let $(P(x))$ denote the ideal in $\mathbb{Q}[x]$ generated by our polynomial $P(x)$. Then $\mathbb{Q}[x]/(P(x)) \simeq \mathbb{Q}[\lambda]$, see [29, p. 224], and $\mathbb{Q}[\lambda] \simeq \mathbb{Q}[M]$, by Fact 3 resp. the remark following it. Since λ is algebraic over $\mathbb{Q}$ and $P(x)$ is irreducible, we know by [29, Prop. V.1.4] that $\mathbb{Q}[\lambda] = \mathbb{Q}(\lambda)$ is an algebraic number field, of degree n over $\mathbb{Q}$. Under the isomorphism $\mathbb{Q}[M] \simeq \mathbb{Q}(\lambda)$, $\mathrm{GL}(n, \mathbb{Z})$-matrices correspond to units in $\mathbb{Q}(\lambda)$, hence $\mathcal{S}(M)$ must be isomorphic to a subgroup of $\mathcal{O}^\times_{\max}$, the unit group of the maximal order of $\mathbb{Q}(\lambda)$.

Observe that every matrix in $\mathbb{Z}[M]$ commutes with M, in particular those of $\mathbb{Z}[M] \cap \mathrm{GL}(n, \mathbb{Z})$, which form a subgroup of $\mathcal{S}(M)$. But $\mathbb{Z}[M] \simeq \mathbb{Z}[\lambda]$ means that this subgroup is isomorphic to the unit group $\mathbb{Z}[\lambda]^\times$. So, if we identify $\mathcal{S}(M)$ with its image in $\mathbb{Q}(\lambda)$ under the isomorphism, it is sandwiched between $\mathbb{Z}[\lambda]^\times$ and $\mathcal{O}^\times_{\max}$. Note that $\mathbb{Z}[\lambda] \subset \mathcal{O}_{\max}$ is an order.

Finally, recall that the unit group of an order $\mathcal{O}$ is a finitely generated Abelian group, and that it is always of maximal rank, see [31, Thm. I.12.12] or [13, Sec. 4, Thm. 5], i.e. its rank equals that of the unit group of the maximal order $\mathcal{O}_{\max}$. In particular, the group-subgroup index $[\mathcal{O}^\times_{\max} : \mathbb{Z}[\lambda]^\times]$ is finite, and $\mathcal{S}(M)$ must then also be of finite index in $\mathcal{O}^\times_{\max}$. $\square$

Let us comment on this result. First of all, it does not matter which root λ_i of $P(x)$ we choose, as all the n (possibly different) realizations $\mathbb{Q}(\lambda_i)$ are mutually isomorphic, and so are their unit groups. Explicit isomorphisms are given by the elements of the Galois group of the splitting field $\mathcal{K} = \mathbb{Q}(\lambda_1, \dots, \lambda_n)$ of $P(x)$, see [29, Ch. VI.2] for details. Note also that, in general, $\mathbb{Q}(\lambda)$ will be a true subfield of the splitting field $\mathcal{K}$ – so, it is really the unit group of $\mathbb{Q}(\lambda)$ that matters, and not the unit group of $\mathcal{K}$.

Another way to view the result, in a more matrix oriented way (and similar to our approach in [12]), is to look at the diagonalization of M,

$$UMU^{-1} \; = \; \mathrm{diag}(\lambda_1, \dots, \lambda_n)\,. \tag{15}$$

Here, U^{-1} can be arranged to have its j-th column in the field $\mathbb{Q}(\lambda_j)$, the smallest field extension of $\mathbb{Q}$ that contains λ_j, because one can solve the corresponding eigenvector equation in it. In fact, we only have to do this for the first column — the others are then obtained by applying appropriate Galois automorphisms to the first one.

For any other matrix $G \in \mathrm{GL}(n, \mathbb{Z})$ with $[G, M] = GM - MG = 0$, we then have

$$[UGU^{-1}, UMU^{-1}] \; = \; U[G, M]U^{-1} \; = \; 0\,.$$

But only diagonal matrices can commute with $\mathrm{diag}(\lambda_1, \dots, \lambda_n) = UMU^{-1}$ because the eigenvalues are pairwise distinct. So, we must have

$$UGU^{-1} \; = \; \mathrm{diag}(\mu_1, \dots, \mu_n)\,,$$

with all $\mu_i \in \mathbb{Q}(\lambda_i)$ units. They are, however, not independent but obtained from one another by the same set of Galois automorphisms that were used to link the columns of the matrix U^{-1}, which is why we get the result.

Lemma 1 raises the question: What *is* the unit group of the maximal order in $K = \mathbb{Q}(\lambda)$? The answer is given by Dirichlet's unit theorem, see [16, Sec. 11.C] or [36, p. 334]. Group the roots of the irreducible polynomial $P(x)$ into n_1 real roots and n_2 pairs of complex conjugate roots, so that $n = n_1 + 2n_2$. (In other words: we have n_1 real and n_2 pairs of complex conjugate realizations of the abstract number field $\mathbb{Q}(\lambda)$).

Fact 7 *Let λ be an algebraic number of degree $n = n_1 + 2n_2$, with n_1 and n_2 as described above. Then, the units in the maximal order $\mathcal{O}_{\max}$ of the algebraic number field $K = \mathbb{Q}(\lambda)$ form the group*

$$E(K) \; = \; \mathcal{O}_{\max}^{\times} \; \simeq \; T \times \mathbb{Z}^{n_1+n_2-1} \tag{16}$$

where $T = \mathcal{O}_{\max} \cap \{$roots of unity$\}$ is a finite Abelian group and cyclic. □

In particular, this means that T, which is also called the *torsion subgroup* of $E(K)$, is generated by one element. In many cases below, we will simply find $T \simeq C_2$. Combining now Lemma 1 with Fact 7, we immediately obtain

Proposition 1 *If the characteristic polynomial of $M \in \mathrm{GL}(n,\mathbb{Z})$ is irreducible over $\mathbb{Z}$, the symmetry group $\mathcal{S}(M) \subset \mathrm{GL}(n,\mathbb{Z})$ is isomorphic to a subgroup of $E(K)$ of* (16) *of maximal rank, i.e. we have*

$$\mathcal{S}(M) \;\simeq\; T' \times \mathbb{Z}^{n_1+n_2-1}$$

where T' is a subgroup of the torsion group T as it appears in (16). $\square$

This result appears also as [22, Prop. 3.7]. Note that Proposition 1 does *not* imply that the torsion-free parts of $\mathcal{S}(M)$ and $E(K)$ are the same, only that they are isomorphic. In fact, a typical situation will be that they are different in the sense that $E(K)$ is generated by the fundamental units, but $\mathcal{S}(M)$ only by suitable powers thereof.

What, in turn, can we say about the torsion group T' in Proposition 1? Whenever the characteristic polynomial $P(x)$ of $M \in \mathrm{GL}(n,\mathbb{Z})$ is irreducible and has at least one *real* root (e.g. if n is odd), α say, then $K = \mathbb{Q}(\alpha)$ is real, and $\mathbb{Q}(\alpha) \cap S^1 = \{\pm 1\}$, where S^1 is the unit circle. Consequently, the torsion subgroup of $E(K)$ in this case is $T = \{\pm 1\} \simeq C_2$. Since a toral automorphism always commutes with $\pm\mathbf{1}$, we obtain

Corollary 1 *If the characteristic polynomial of $M \in \mathrm{GL}(n,\mathbb{Z})$ is irreducible over $\mathbb{Z}$ and possesses a real root, the torsion group in Proposition* 1 *is $T' \simeq C_2$. In particular, this holds whenever the degree of $P(x)$ is odd.* $\square$

With reference to this Corollary, it follows from [22, Lemma 4.2] that, if the characteristic polynomial is irreducible and *all* eigenvalues are real, then every element of $\mathcal{S}(M)$ other than $\{\pm\mathbf{1}\}$ is hyperbolic.

Let us look at two examples in $\mathrm{GL}(3,\mathbb{Z})$, namely

$$M_1 \;=\; \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix} \;\text{ and }\; M_2 \;=\; \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}, \tag{17}$$

which are taken from [30, Eqs. (5.21) and (5.3)]. They have been studied thoroughly in the context of inflation generated one-dimensional quasicrystals with a cubic irrationality as inflation factor. We have $\det(M_1) = 1$, $\det(M_2) = -1$, and the characteristic polynomials are $P_1(x) = x^3 - x^2 - 1$ and $P_2(x) = x^3 - 2x^2 - x + 1$, both irreducible over $\mathbb{Z}$. Both matrices are hyperbolic, and the largest eigenvalue in each case is a Pisot-Vijayaraghavan number, i.e. an algebraic integer $\alpha > 1$ all algebraic conjugates[8] of which lie inside the unit circle, see [42] for details.

Now, M_1 has one real and a pair of complex conjugate roots, so our above results lead to $\mathcal{S}(M_1) \simeq C_2 \times \mathbb{Z}$, where the infinite cyclic group is actually generated by M_1 itself because its real root is a fundamental unit. M_2, in turn, has three real roots, and we thus get $\mathcal{S}(M_2) \simeq C_2 \times \mathbb{Z}^2$. As generators of $\mathbb{Z}^2$, one may choose M_2 and M_2' where

$$M_2' \;=\; \begin{pmatrix} 0 & 1 & 0 \\ 1 & -1 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

which can be checked explicitly. This is an example of a Cartan action in the sense of [22, Sec. 4]. It is also of relevance in connection with planar quasicrystals with sevenfold symmetry, see [30, Sec. 5.2] for details, where the three-dimensional toral automorphism M_2 shows up in the cut and project description of special directions in the quasicrystal. Other examples related to planar quasicrystals with 8-, 10- and 12-fold symmetry, in which the torsion subgroup T' of Proposition 1 is different from C_2, will be given in Section 2.2.

Let us now return to the general discussion and extend the previous results to the case that M is simple, and hence diagonalizable (over $\mathbb{C}$) with pairwise different eigenvalues. Since diagonal matrices with pairwise different entries only commute with diagonal matrices, we have:

Corollary 2 *If $M \in \mathrm{GL}(n,\mathbb{Z})$ is simple, $\mathcal{S}(M) \subset \mathrm{GL}(n,\mathbb{Z})$ is Abelian.* □

Note that the converse is not true: even if M is only semi-simple, or not even that (i.e. not diagonalizable), $\mathcal{S}(M)$ can still be Abelian, e.g. if M observes the conditions of Fact 6. As far as we are aware, not even the Abelian subgroups of $\mathrm{GL}(n,\mathbb{Z})$ are fully classified, see [32, 35] and references given there for background material.

Let $P(x)$ be the characteristic polynomial of a simple matrix M. If it is reducible over $\mathbb{Z}$, it factorizes as $P(x) = \prod_{i=1}^{\ell} P_i(x)$ into irreducible monic polynomials $P_i(x)$.

Theorem 1 *Let $M \in \mathrm{GL}(n,\mathbb{Z})$ be simple and let its characteristic polynomial be $P(x) = \prod_{i=1}^{\ell} P_i(x)$, with $P_i(x)$ irreducible over $\mathbb{Z}$. Then, the symmetry group of M, $\mathcal{S}(M) \subset \mathrm{GL}(n,\mathbb{Z})$, is a finitely generated Abelian group of the form*

$$\mathcal{S}(M) \;=\; T \times \mathbb{Z}^r \tag{18}$$

where T is a finite Abelian group of even order, with at most ℓ generators. Furthermore, if the irreducible component $P_i(x)$ has $n_1^{(i)}$ real roots and $n_2^{(i)}$ pairs of complex

[8] If α is a root of the $\mathbb{Z}$-irreducible, monic polynomial p, then the other roots of p are the algebraic conjugates of α.

conjugate roots, the rank r of the free Abelian group in (18) *is given by*

$$r \;=\; \sum_{i=1}^{\ell} (n_1^{(i)} + n_2^{(i)} - 1)\,. \tag{19}$$

PROOF: Since M is simple, the degree of its minimal polynomial is n and Fact 6 tells us that $\mathrm{cent}_{\mathrm{Mat}(n,\mathbb{Q})}(M) = \mathbb{Q}[M]$. As $P(x)$ has no repeated factors (so that $\mathbb{Q}[M]$ contains no radicals), we get, by [21, Thm. III.4],

$$\mathbb{Q}[M] \;\simeq\; \mathbb{Q}[\alpha_1] \oplus \ldots \oplus \mathbb{Q}[\alpha_\ell] \tag{20}$$

where α_i is any root[9] of $P_i(x)$, for $1 \leq i \leq \ell$.

Under the assumptions made, each $\mathbb{Q}[\alpha_i] = \mathbb{Q}(\alpha_i)$ is a field. Since a $\mathrm{GL}(n,\mathbb{Z})$-matrix in $\mathbb{Q}[M]$ will correspond to a unit in each of the $\mathbb{Q}(\alpha_i)$, we can now apply Lemma 1 to each component, giving (18) as the direct sum of ℓ unit groups. The rank in (19) follows now from Proposition 1.

The torsion part T is a finitely generated Abelian group, with (at most) one generator per irreducible component of $P(x)$, of which there are ℓ. Clearly, $\mathcal{S}(M)$ always contains the elements $\pm\mathbf{1}$, so $\{\pm 1\} \simeq C_2$ is a subgroup of T. The order of T is then divisible by 2, hence even. $\square$

Although Theorem 1 does not give the general answer to the question for the symmetry group $\mathcal{S}(M)$, it certainly gives the *generic* answer, because the property of M having simple spectrum is generic. But what about the remaining cases? Without further elaborating on this, let us summarize a few aspects and otherwise refer to the literature [32, 35] for a summary of methods to actually determine the precise centralizer.

If $M \in \mathrm{GL}(n,\mathbb{Z})$ is semi-simple, but not simple, its characteristic polynomial contains a square, and whether or not $\mathcal{S}(M)$ is still Abelian (and then of the above form) depends on whether or not the minimal polynomial of M has degree n, see Fact 6. Note, in particular, that the following situation can emerge. If $P(x)$ has a repeated factor, but the corresponding matrix M is a block matrix, then the two blocks giving the same factor of $P(x)$ can still be inequivalent, if the corresponding class number is larger than one which equals the number of different matrix classes, see Fact 4.

If M is not even semi-simple, things get even more involved. We can still have Abelian symmetry groups, e.g. if M is a Jordan block such as $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, compare the results of [12, Sec. 2.1.2] on parabolic automorphisms of $\mathbb{T}^2$. Clearly, this also follows from Fact 6: if $M \in \mathrm{GL}(n,\mathbb{Z})$ is conjugate to a single Jordan block, its minimal

[9] Note that the α_i have pairwise different minimal polynomials by assumption, but that $\mathbb{Q}[\alpha_i] \simeq \mathbb{Q}[\alpha_j]$ for $i \neq j$ is still possible.

polynomial has degree n and all $\mathrm{GL}(n,\mathbb{Z})$-matrices which commute with M are in $\mathbb{Q}[M]$. This remains true if such a block occurs in a matrix that otherwise has simple spectrum disjoint from 1.

Corollary 3 *Let $M \in \mathrm{GL}(n,\mathbb{Z})$. If the minimal polynomial of M has degree n, then $\mathcal{S}(M) \subset \mathrm{GL}(n,\mathbb{Z})$ is Abelian.* $\square$

In a wider setting for symmetries, a stronger statement can be formulated, see Proposition 5 below and the comments following it.

The general classification, however, and the non-Abelian cases in particular, gets increasingly difficult with growing n and has been completed only for small n, see [32] and references given there. Nevertheless, for any given M, the centralizer can be determined explicitly by means of various algorithmic program packages.

Before we discuss the connection of our approach to quasicrystallography in a separate section, let us illustrate Theorem 1 with a recent example of a 4D cat map taken from [37, Eq. 3.21], namely

$$M \;=\; \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 2 & 1 \\ 0 & 1 & 1 & 2 \end{pmatrix}. \tag{21}$$

The characteristic polynomial is $P(x) = x^4 - 4x^3 + 5x^2 - 4x + 1$ which is reducible over $\mathbb{Z}$ and splits as

$$P(x) \;=\; P_1(x)\, P_2(x) \;=\; (x^2 - 3x + 1)(x^2 - x + 1)$$

into $\mathbb{Z}$-irreducible polynomials. Since P_1 has two real and P_2 one pair of complex conjugate roots, Theorem 1 gives $\mathcal{S}(M) \simeq T' \times \mathbb{Z}$, with T' a subgroup of $T = C_2 \times C_6$. Also, since no root of P_1 is a fundamental unit of the corresponding maximal order (which is $\mathbb{Z}[\tau]$ with $\tau = (1+\sqrt{5}\,)/2$), the generator of the infinite cyclic group in $\mathcal{S}(M)$ could still differ from M.

To determine the details, one easily checks that the most general matrix to commute with M is

$$G \;=\; \begin{pmatrix} a & b & -c & -d \\ b & a & -d & -c \\ c & d & a+2c+d & a+c+2d \\ d & c & a+c+2d & a+2c+d \end{pmatrix}.$$

A necessary condition for G to be in $\mathrm{GL}(4,\mathbb{Z})$ is then $a,b,c,d \in \mathbb{Z}$. This allows to exclude the existence of a root of M in $\mathcal{S}(M)$, and also no element of third order is possible. So we obtain

$$\mathcal{S}(M) \;=\; C_2 \times C_2 \times \langle M \rangle\,.$$

We will revisit this example below in the context of reversibility.

2.2 Three examples from planar quasicrystallography

Planar tilings with 8-, 10- and 12-fold symmetry play an important role in the description of so-called quasicrystalline T-phases, see [8] for background material. They are of interest also in the present context because hyperbolic toral automorphisms show up through their inflation symmetries.

For the 8-fold case, consider the polynomial

$$P(x) \;=\; x^4 + 1 \tag{22}$$

which has ξ, ξ^3, ξ^5, and ξ^7 as roots, $\xi = e^{2\pi i/8}$, which are primitive. So, $P(x)$ is irreducible over $\mathbb{Z}$, and Lemma 1 and Proposition 1 apply. In fact, $\mathbb{Q}(\xi)$ here is a cyclotomic field [45] with class number one, maximal order $\mathbb{Z}[\xi]$ and unit group $\mathbb{Z}[\xi]^\times \simeq C_8 \times \mathbb{Z}$.

If we denote the actual matrices that represent the generators for the groups C_8 and $\mathbb{Z}$ by M and G, respectively, it is natural to take the companion matrix of $P(x)$ for M and to choose G accordingly, resulting in

$$M \;=\; \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \end{pmatrix}, \quad G \;=\; \begin{pmatrix} 1 & 1 & 0 & -1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ -1 & 0 & 1 & 1 \end{pmatrix}. \tag{23}$$

By construction, M is a matrix of order 8. So, $\mathcal{S}(M) = \langle M, G\rangle \simeq C_8 \times \mathbb{Z}$. What is more, anticipating the next Section, M turns out to be reversible with the matrix R of (11) as reversing symmetry. Using Fact 2 and observing $[G, R] = 0$, this means that $\mathcal{R}(M) = \langle M, G, R\rangle \simeq D_8 \times \mathbb{Z}$. This, together with two similar examples, is summarized in Table 1.

Note that the case of 12-fold symmetry is more complicated because the fundamental unit in $\mathbb{Z}[\xi]$, for $\xi = e^{2\pi i/12}$, is the square root of $(2 + \sqrt{3}\,)\xi$, and hence not a simple homothety. This means that the representing matrix does not commute with R. The reversing symmetry group of this case, $(C_{12} \times \mathbb{Z}) \times_s C_2$, does contain a subgroup of the form $D_{12} \times \mathbb{Z}$ though: it is generated by M, $G' = M^{-1}G^2$ and R, where G' corresponds to the non-fundamental unit $2 + \sqrt{3}$.

2.3 Reversibility

The examples of Section 2.2 were reversible, i.e. they fulfilled $GMG^{-1} = M^{-1}$ for some $G \in \mathrm{GL}(4, \mathbb{Z})$, in particular for the involution $R \in \mathrm{GL}(4, \mathbb{Z})$ of (11). It is easy to check that this is also true for M of (21). However, as we will see below, neither of the examples of (17) are reversible in $\mathrm{GL}(3, \mathbb{Z})$.

	8-fold	10-fold	12-fold
$P(x)$	x^4+1	$x^4+x^3+x^2+x+1$	x^4-x^2+1
M	$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & -1 & -1 & -1 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 1 & 0 \end{pmatrix}$
$\langle M \rangle$	C_8	C_5	C_{12}
G	$\begin{pmatrix} 1 & 1 & 0 & -1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ -1 & 0 & 1 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 1 & 1 \\ -1 & 0 & -1 & 0 \\ 0 & -1 & 0 & -1 \\ 1 & 1 & 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ -1 & 0 & 1 & 1 \end{pmatrix}$
$\mathcal{S}(M)$	$C_8 \times \mathbb{Z}$	$C_{10} \times \mathbb{Z}$	$C_{12} \times \mathbb{Z}$
$\mathcal{R}(M)$	$D_8 \times \mathbb{Z}$	$D_{10} \times \mathbb{Z}$	$(C_{12} \times \mathbb{Z}) \times_s C_2$

Table 1: Symmetries and reversing symmetries for three examples from quasicrystallography. The symmetry group is $\mathcal{S}(M) = \langle \pm M, G \rangle$, and, similarly, $\mathcal{R}(M) = \langle \pm M, G, R \rangle$, with R as in Eq. (11) for all three examples.

In this Section, we are concerned with determining when reversibility can occur in $\mathrm{GL}(n,\mathbb{Z})$, and what we can say about the nature of the reversing symmetry $G \in \mathrm{GL}(n,\mathbb{Z})$, e.g. whether it can be taken to be an involution so that, by Fact 2, the reversing symmetry group $\mathcal{R}(M) \subset \mathrm{GL}(n,\mathbb{Z})$ is a semi-direct product. Note that if $M \in \mathrm{GL}(n,\mathbb{R})$ is reversible, it has been shown that there always exists an involutory reversing symmetry in $\mathrm{GL}(n,\mathbb{R})$ [43, Thm. 2.1]. Already for $\mathrm{GL}(2,\mathbb{Z})$, this is no longer true [41]: the matrix $M = \left(\begin{smallmatrix} 5 & 7 \\ 7 & 10 \end{smallmatrix}\right)$ is reversible in $\mathrm{GL}(2,\mathbb{Z})$ with the reversing symmetry $G = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ of order 4, but with no involutory reversing symmetry in $\mathrm{GL}(2,\mathbb{Z})$.

While reversibility was still a frequent phenomenon in $\mathrm{GL}(2,\mathbb{Z})$, see [12], it becomes increasingly restrictive with growing n. To see this, let us consider necessary conditions for reversibility. If $M \in \mathrm{GL}(n,\mathbb{R})$ is reversible, then $M^{-1} = GMG^{-1}$ for some matrix G, and M and M^{-1} must have the same characteristic polynomial, $P(x)$. On the other hand, the spectrum of M must then be self-reciprocal, i.e. with λ also $1/\lambda$ must be an eigenvalue, with matching multiplicities. Recall that $P(x) = \prod_{i=1}^{n}(x-\lambda_i)$ and observe that

$$\prod_{i=1}^{n}\Big(x - \frac{1}{\lambda_i}\Big) \;=\; \frac{(-1)^n x^n}{\det(M)} \prod_{i=1}^{n}\Big(\frac{1}{x} - \lambda_i\Big). \tag{24}$$

But by assumption, $\prod_{i=1}^{n}(x-\lambda_i) = \prod_{i=1}^{n}(x - \frac{1}{\lambda_i})$, so we arrive at

Proposition 2 *A necessary condition for the matrix $M \in \mathrm{GL}(n, \mathbb{R})$ to be reversible is* $\mathrm{spec}(M) = \mathrm{spec}(M^{-1})$ *and thus the equation*

$$P(x) \;=\; \frac{(-1)^n x^n}{\det(M)}\, P(1/x) \tag{25}$$

which we call the self-reciprocity of $P(x)$. □

One immediate consequence is the following.

Corollary 4 *If $M \in \mathrm{GL}(n, \mathbb{R})$ is reversible,* $\det(M) = \pm 1$*. If, in addition, the multiplicity of the eigenvalue $\lambda = -1$ is even (allowing for multiplicity 0 if -1 is not an eigenvalue of M), then* $\det(M) = 1$*.*

PROOF: Observe that the reversibility of M implies $G = MGM$. Taking determinants gives the first assertion because neither M nor G is singular.

Next, note that $\lambda = \pm 1$ are the only complex numbers with $\lambda = 1/\lambda$. All other eigenvalues come in reciprocal pairs. Since the determinant is the product over all eigenvalues, the second statement follows. □

It might be instructive to reformulate Proposition 2 and Corollary 4 in terms of elementary symmetric polynomials. Let S_k, $k = 0, 1, \ldots, n$, denote the k-th elementary symmetric polynomial in n indeterminates. The S_k are given by $S_0 \equiv 1$ and

$$S_k(x_1, \ldots, x_n) \;=\; \sum_{i_1 < \ldots < i_k} x_{i_1} \cdot \ldots \cdot x_{i_k} \,. \tag{26}$$

They are algebraically independent over $\mathbb{Z}$ and have the generating function

$$\sum_{k=0}^{n} S_k(x_1, \ldots, x_n)\, t^k \;=\; \prod_{i=1}^{n} (1 + x_i t) \tag{27}$$

where t is another indeterminate.

With this, we get $P(x) = x^n + \sum_{k=1}^{n} (-1)^k S_k(\lambda_1, \ldots, \lambda_n)\, x^{n-k}$, for a characteristic polynomial $P(x)$, and $x^n P(1/x) = 1 + \sum_{k=1}^{n} (-1)^k S_k(\lambda_1, \ldots, \lambda_n)\, x^k$. A comparison with Proposition 2 reveals that

$$S_k(\lambda_1, \ldots, \lambda_n) \;=\; \det(M) \cdot S_{n-k}(\lambda_1, \ldots, \lambda_n) \tag{28}$$

for all $0 \le k \le n$. For $k = 0$, this is just the statement that $\det(M) = \pm 1$. Note that the elementary symmetric polynomials, when evaluated at the roots of $P(x)$, reproduce (up to a sign) the entries of the last row of the left companion matrix (9).

Turning now to the reversibility of matrices in $\mathrm{GL}(n, \mathbb{Z})$, we first observe that, generically, the reversible cases can only occur when n is even and $\det(M) = +1$:

Proposition 3 *Consider $M \in \mathrm{GL}(n, \mathbb{Z})$ and let $P(x)$ be the characteristic polynomial of M. If $n > 1$ is odd or $\det(M) = -1$ we have:*

(*a*) *if M is reversible in $\mathrm{GL}(n, \mathbb{Z})$, $P(x)$ is reducible over $\mathbb{Z}$, and the spectrum of M contains 1 or -1;*

(*b*) *if $P(x)$ is irreducible over $\mathbb{Z}$, M cannot be reversible in $\mathrm{GL}(n, \mathbb{Z})$.*

PROOF: If M is reversible, $\lambda \in \mathrm{spec}(M)$ implies $1/\lambda \in \mathrm{spec}(M)$, so the eigenvalues are either ± 1 or have to come in pairs, $\lambda \neq 1/\lambda$. If n is odd, we must have at least one eigenvalue that is ± 1, and that gives a factor[10] $(x \mp 1)$ in $P(x)$. On the other hand, if $\det(M) = -1$, we must have at least one eigenvalue that is -1 which gives a factor $(x + 1)$ in $P(x)$.

Conversely, if $P(x)$ is irreducible over $\mathbb{Z}$, $\mathrm{spec}(M)$ cannot contain an eigenvalue of the form ± 1, and n odd or $\det(M) = -1$ is then incompatible with M being reversible. □

It is clear from this that reversibility is rather restrictive. If $P(x)$ splits into irreducible components $P_i(x)$, then each is subject to the constraints described above, or has to be matched with its reciprocal partner polynomial – if that would be an integer polynomial at all. In particular, if $P(x)$ is reducible but contains an isolated irreducible factor of odd order ≥ 3, or of even order with constant term -1, reversibility of M is ruled out. For example, this confirms that M_1 and M_2 of (17) are not reversible (in fact, they are not even reversible in $\mathrm{GL}(3, \mathbb{R})$).

The key problem in deciding upon similarity of M and M^{-1} in $\mathrm{GL}(n, \mathbb{Z})$ is that $\mathbb{Z}$ is not a field. But it is clear that the corresponding similarity within $\mathrm{GL}(n, \mathbb{Q})$ (the matrix entries now belonging to the field of rationals) is both a necessary condition and a much easier problem. It would not help to further extend $\mathbb{Q}$ to $\mathbb{R}$ due to the following result, see [29, Cor. XIV.2.3].

Fact 8 *A matrix $M \in \mathrm{GL}(n, \mathbb{Z})$ is similar to M^{-1} within the group $\mathrm{GL}(n, \mathbb{R})$ if and only if this is already the case in $\mathrm{GL}(n, \mathbb{Q})$.* □

In the light of this, let us first recall some facts about normal forms over $\mathbb{Q}$, where similarity is (in theory) a decideable problem. The normal form of a matrix M is based on its *polynomial invariants*, or *invariants* for short, see [29, Sec. XIV.2]. They are often also called the *invariant factors* of M (or, more explicitly, of $(x\mathbf{1} - M)$), compare [5, Def. 4.4.6], meaning certain polynomials that derive from the matrix $(x\mathbf{1} - M)$, see below. The following result is a direct consequence of [29, Thm. XIV.2.6] or [5, Thm. 5.3.3].

[10]In both cases, one notes that whenever ± 1 is a root of a polynomial over $\mathbb{Z}$, factoring out $(x \mp 1)$ can be done over $\mathbb{Z}$.

Fact 9 *Two matrices in* $\mathrm{Mat}(n,\mathbb{Q})$ *are* $\mathrm{GL}(n,\mathbb{Q})$*-similar if and only if they have the same polynomial invariants. In particular, this applies to* M *and* M^{-1} *for any* $M \in \mathrm{GL}(n,\mathbb{Z})$. $\square$

Let us briefly recall how the polynomial invariants $q_1, \dots, q_r$ of a matrix $M \in \mathrm{Mat}(n,\mathbb{Z})$ can be found, where $r \leq n$ is a uniquely determined integer that depends on M. We formulate this for integer matrices, but it applies, with little change, also to rational ones. Set $p_0 = 1$ and let p_k (for $1 \leq k \leq n$) be the greatest common divisor of all minors of $(x\mathbf{1} - M)$ of order k, so that p_k clearly divides p_{k+1}, and $p_n = P(x) = \det(x\mathbf{1} - M)$. Let ℓ denote the largest integer k for which $p_k = 1$ and define $q_i = p_{\ell+i}/p_{\ell+i-1}$, where $1 \leq i \leq r = n - \ell$. These polynomials over $\mathbb{Z}$ are the polynomial invariants of M and satisfy the following divisibility property:

$$q_i \mid q_{i+1} \, . \tag{29}$$

The prime factors of q_i over $\mathbb{Z}$, taken with their multiplicity, are called its *elementary divisors*. The product of the invariant factors of M (equivalently, the product of all their elementary divisors) gives the characteristic polynomial $P(x)$ of M. The minimal polynomial $Q(x)$ of M is $q_r = p_n/p_{n-1}$.

A systematic way to find the invariant factors of M is to bring $(x\mathbf{1} - M)$, seen as a matrix over the principal ideal domain $\mathbb{Z}[x]$, into its so-called *Smith normal form* which is the diagonal matrix $\mathrm{diag}(1, \dots, 1, q_1(x), \dots, q_r(x))$, see [5, Ch. 5.3] for details. Its calculation is a computationally difficult exercise in general, but for small n, it can be easily be found with algebraic program packages. The invariant factors completely determine the *Frobenius normal form* of the matrix M:

Fact 10 *Let* $M \in \mathrm{Mat}(n,\mathbb{Z})$ *have polynomial invariants* $q_1, \dots, q_r$ *of degrees* $n_1, \dots, n_r$*, with* $n_1 + \ldots + n_r = n$*. Then* M *is* $\mathrm{GL}(n,\mathbb{Q})$*-similar to a block diagonal matrix* $[B_1, \dots, B_r]$ *where* B_i *is the* $n_i \times n_i$ *left companion matrix of the polynomial* q_i. $\square$

The existence of a block diagonal matrix similar to M is equivalent to the statement that M leaves invariant a set of (cyclic) subspaces of $\mathbb{Q}^n$ with respective dimensions $n_1, \dots, n_r$, see [29, Thm. XIV.2.1] for details. One can actually give more refined normal forms by using the elementary divisors of each invariant to replace the diagonal blocks B_i with subblock decompositions based upon the elementary divisors and their multiplicities. Combining Fact 9 and Fact 10, matrices with the same polynomial invariants can both be brought to the same Frobenius normal form.

Fact 10 highlights the left companion matrices B_i. For what follows, we are interested in the reversibility of such matrices. In this respect, let $M^{(\ell)}$ and $M^{(r)}$ be the left and right companion matrices corresponding to a polynomial $P(x)$. Suppose $P(x)$ conforms to the reciprocity condition (25) of Proposition 2. Then one can check that $M^{(r)}$ is the *inverse* of $M^{(\ell)}$. But we already know from (10) that $M^{(r)} = RM^{(\ell)}R^{-1}$ where $R = R^{-1}$ is the involution from (11). Combining this with the normal form above, we obtain:

Theorem 2 *Let $M \in \mathrm{GL}(n, \mathbb{Z})$. Then, M is reversible in $\mathrm{GL}(n, \mathbb{Q})$ if and only if each of the polynomial invariants of M satisfies the reciprocity condition* (25) *separately. In this situation, the reversing symmetry can be chosen to be an involution.*

PROOF: By Fact 10, $M = SDS^{-1}$ where $S \in \mathrm{GL}(n, \mathbb{Q})$ and $D \in \mathrm{GL}(n, \mathbb{Z})$ is a block diagonal matrix of the form $D = [B_1, \ldots, B_r]$, where $r \geq 1$ and $B_i \in \mathrm{GL}(n_i, \mathbb{Z})$ is the left companion matrix corresponding to the invariant q_i of degree n_i. It follows that $M^{-1} = SD^{-1}S^{-1}$ where $D^{-1} = [B_1^{-1}, \ldots, B_r^{-1}]$. Consequently, M and M^{-1} are similar if and only if D and D^{-1} are similar.

Suppose that each of the polynomial invariants satisfies the condition (25). Then, from the remark before Theorem 2, B_i^{-1} is the right companion matrix corresponding to q_i and is similar to B_i via the involution $R_i \in \mathrm{GL}(n_i, \mathbb{Z})$ which consists of 1's on its anti-diagonal, as in (11). It follows that D is similar to D^{-1} via the block diagonal involution $R := [R_1, \ldots, R_r]$, and so M and M^{-1} are similar by the involution SRS^{-1}.

On the other hand, suppose that M is similar to M^{-1} in $\mathrm{GL}(n, \mathbb{Q})$. Hence, the corresponding block diagonal matrices D and D^{-1} are also similar in $\mathrm{GL}(n, \mathbb{Q})$, via some element G. Now, to each block B_i of D corresponds an invariant vector subspace V_i of $\mathbb{Q}^n$ of dimension n_i. A subspace V_i is thus either mapped by G to itself (it is a *symmetric* subspace) or to another subspace V_j of the same dimension. In the first case, B_i must be conjugate to its inverse via the restriction of G to V_i. This means that the characteristic polynomial of B_i, which is q_i, must satisfy the condition (25). On the other hand, if V_i is mapped to V_j by G with $n_i = n_j$, it follows that the invariants q_i and q_j differ by at most a sign. They thus share the same roots and must each satisfy condition (25) on their own. $\square$

If M has only one non-trivial invariant, $q_1(x)$, it follows from the above discussion that its characteristic polynomial $P(x)$ coincides with its minimal polynomial $Q(x)$ and both equal $q_1(x)$ (so M is cyclic from Fact 6). Conversely, M cyclic means it has only one invariant. The previous Theorem now gives:

Corollary 5 *If $M \in \mathrm{GL}(n, \mathbb{Z})$ has only one polynomial invariant, in particular if the characteristic polynomial $P(x)$ is irreducible over $\mathbb{Z}$, then M is reversible in $\mathrm{GL}(n, \mathbb{Q})$ if and only if its characteristic polynomial $P(x)$ satisfies the reciprocity condition* (25). $\square$

Note that Theorem 2 and Corollary 5 do not extend to requiring, for reversible M, that the elementary divisors within an invariant polynomial satisfy (25). For example, any matrix in $\mathrm{GL}(4,\mathbb{Z})$ with one invariant polynomial $q_1(x) = P(x) = (x^2 - x - 1)(x^2 + x - 1)$ is reversible in $\mathrm{GL}(4,\mathbb{Q})$ although the elementary divisors separately violate (25).

Let us give some illustrations of the use of Theorem 2 and Corollary 5 for small values of n. These results show that all $M \in \mathrm{SL}(2,\mathbb{Z})$ are reversible in $\mathrm{GL}(2,\mathbb{Q})$ because their invariant factors fall into one of the following cases:

1. $q_1(x) = q_2(x) = (x \pm 1)$, so $r = 2$ and $M = \mp\mathbf{1}$;
2. $q_1(x) = P(x) = x^2 - \mathrm{tr}(M)x + 1$, so $r = 1$ and $P(x)$ is self-reciprocal.

Yet, we know from [12] that $\mathrm{SL}(2,\mathbb{Z})$ matrices exist that are not reversible in $\mathrm{GL}(2,\mathbb{Z})$ (see also Section 3.3 below for further discussion). Furthermore, if $M \in \mathrm{GL}(2,\mathbb{Z})$ with $\det M = -1$, then it can only have one polynomial invariant, $q_1(x) = P(x) = x^2 - \mathrm{tr}(M)x - 1$. By Proposition 3 or Corollary 5, M is reversible in $\mathrm{GL}(2,\mathbb{Z})$ if and only if M has eigenvalues $\lambda = \pm 1$ and $q_1(x)$ factors into $(x-1)(x+1)$, in which case $M \in \mathrm{GL}(2,\mathbb{Z})$ is an involution and reversible, with reversing symmetry as itself. This approach gives another way of retrieving some of the results of [12] on the reversibility in $\mathrm{GL}(2,\mathbb{Z})$.

Turning to $\mathrm{GL}(3,\mathbb{Z})$, Proposition 3 implies that if M is reversible then $P(x)$ must have a factor $(x \pm 1)$. In other words, $(x \pm 1)^i$, for some $1 \leq i \leq 3$, is an elementary divisor of $P(x)$. If M has more than one polynomial invariant, then the divisibility property (29) implies that $P(x)$ completely decomposes into a product of 3 factors of the form $(x \pm 1)$. Generically, however, this will not happen and instead M is reversible in $\mathrm{GL}(3,\mathbb{Q})$ if and only if it has only one invariant of the form $q_1(x) = P(x) = (x \pm 1)(x^2 - (\mathrm{tr}(M) \pm 1)x + 1)$.

For $\mathrm{GL}(4,\mathbb{Z})$, elements with three or four polynomial invariants are diagonal matrices with $+1$'s or (an even number of) -1's on the diagonal. They are all reversible. Reversible elements with two invariants must have $q_1(x) = (x \pm 1)$ and $q_2(x) = (x \pm 1)(x^2 - (\mathrm{tr}(M) \pm 2)x + 1)$, or $q_1(x) = q_2(x)$, a monic quadratic polynomial with constant term $+1$.

As n increases, Theorem 2 can exclude many matrices from being reversible in $\mathrm{GL}(n,\mathbb{Z})$ because they are not reversible in $\mathrm{GL}(n,\mathbb{Q})$. In particular, we can ask for an example M with more than one polynomial invariant where the characteristic polynomial $P(x)$ satisfies (25), yet M is irreversible in $\mathrm{GL}(n,\mathbb{Q})$ because it violates Theorem 2. If we take $n \geq 2$ and even, the first possibility appears in $\mathrm{GL}(8,\mathbb{Z})$. For example, we can take a matrix with invariants $q_1(x) = x^2 - x - 1$ and $q_2(x) = (x^2 - x - 1)(x^2 + x - 1)^2$. Both polynomials violate the reciprocity condition (25) but they compensate each other so that their product, the characteristic polynomial, does satisfy the condition. The Frobenius normal form with these invariants is the block diagonal matrix $M = [B_1, B_2]$,

$$M \;=\; \left(\begin{array}{cc|cccccc} 0 & 1 & & & & & & \\ 1 & 1 & & & \multicolumn{2}{c}{\mathbf{0}} & & \\ \hline & & 0 & 1 & 0 & 0 & 0 & 0 \\ & & 0 & 0 & 1 & 0 & 0 & 0 \\ \multicolumn{2}{c|}{\mathbf{0}} & 0 & 0 & 0 & 1 & 0 & 0 \\ & & 0 & 0 & 0 & 0 & 1 & 0 \\ & & 0 & 0 & 0 & 0 & 0 & 1 \\ & & 1 & -1 & -4 & 3 & 4 & -1 \end{array}\right). \tag{30}$$

This matrix is not reversible in $\mathrm{GL}(8, \mathbb{Z})$ (though its square is, see Section 3.2 below).

It now remains to assess reversibility in $\mathrm{GL}(n, \mathbb{Z})$ of unimodular matrices that are already reversible in $\mathrm{GL}(n, \mathbb{Q})$. For $n = 2$, we were able to solve this problem in [12] using a special algebraic structure (the amalgamated free product) of $\mathrm{PGL}(2, \mathbb{Z})$, see also [2] for an alternative approach. Such a structure is not available for $n \geq 3$.

Important examples of unimodular integer matrices which are reversible in the group $\mathrm{GL}(n, \mathbb{Q})$ are the *symplectic* matrices $\mathrm{Sp}(2n, \mathbb{Z}) \subset \mathrm{SL}(2n, \mathbb{Z})$. Recall that a symplectic matrix $M \in \mathrm{Sp}(2n, \mathbb{R})$ satisfies $M^t J M = J$ where M^t denotes the transpose of M and J is the $2n \times 2n$ integer block matrix

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

of order 4. Since in general

$$M^t J M \;=\; J \quad \Rightarrow \quad M^t \;=\; J M^{-1} J^{-1}\,, \tag{31}$$

it follows that $M \in \mathrm{Sp}(2n, \mathbb{R})$ is reversible if and only if M is similar to M^t in $\mathrm{GL}(2n, \mathbb{R})$. But any invertible square matrix with entries in a field F is similar to its transpose in $\mathrm{GL}(m, F)$, see [5, Prop. 5.3.7] (but this need not be true e.g. in $\mathrm{GL}(m, \mathbb{Z})$). In particular, $M \in \mathrm{Sp}(2n, \mathbb{Z})$ is reversible in $\mathrm{GL}(2n, \mathbb{Q})$ and its invariant factors will all satisfy (25). Also, it is clear from (31) that if M is symplectic and symmetric, then $M^t = M = J M^{-1} J^{-1}$ so that M is actually reversible in $\mathrm{GL}(2n, \mathbb{Z})$.

Orthogonal integer matrices $U \in \mathrm{GL}(n, \mathbb{Z})$ which satisfy $U U^t = \mathbf{1}$ are other examples of unimodular integer matrices which are always reversible in $\mathrm{GL}(n, \mathbb{Q})$ (since $U^{-1} = U^t$ and, as before, U^t and U are similar in $\mathrm{GL}(n, \mathbb{Q})$).

We make some further remarks on the problem of deciding reversibility within $\mathrm{GL}(n, \mathbb{Z})$. Firstly, note that in the proof of Theorem 2 above, when we used the reversibility of the left companion matrices with characteristic polynomials satisfying (25), this reversibility was in $\mathrm{GL}(n, \mathbb{Z})$ itself. Furthermore, the reversing symmetry R was an involution, so by Fact 2 we have the following result.

Theorem 3 *For each integer polynomial $P(x)$ of degree n that satisfies the necessary self-reciprocity condition* (25) *for reversibility, there is at least one reversible matrix class in* $\mathrm{GL}(n,\mathbb{Z})$*, represented by the left companion matrix $M^{(\ell)}$ of $P(x)$, and we have $\mathcal{R}(M^{(\ell)}) = \mathcal{S}(M^{(\ell)}) \times_s C_2$.* □

Secondly, by Fact 4, the number of representing matrix classes of an irreducible characteristic polynomial $P(x)$ equals the class number of the order $\mathbb{Z}[\alpha]$, with α any of the roots of $P(x)$. If this class number is one, there is *only* the class represented by the companion matrix. If the class number is two, one is the companion matrix class which we know to be reversible if the spectrum is self-reciprocal. But then, the other class must also be reversible because there is no further partner left.

Class numbers are widely studied in algebraic number theory, and one can find both extensive tables in books (e.g. see [20, 36]) and also various program packages to calculate them, e.g. the program package KANT[11].

Let us add another example, of rather different flavour, and look at an interesting class of algebraic integers, the so-called *Salem numbers*. They are the algebraic integers $\alpha > 1$ with all algebraic conjugates α' having modulus $|\alpha'| \leq 1$ and with at least one conjugate on the unit circle, see [42, Ch. III.3] for details. Salem's theorem then says that their degree is always even, that α and $1/\alpha$ are the only real conjugates, and that all other conjugates are on the unit circle. In particular, a Salem number is a unit. Putting our above results to work, we get

Corollary 6 *Each Salem number occurs as the eigenvalue of a reversible toral automorphism. If α is a Salem number of degree $n = 2m$, and M a corresponding* $\mathrm{GL}(n,\mathbb{Z})$ *matrix, then $\mathcal{S}(M) \simeq C_2 \times \mathbb{Z}^m$.* □

The polynomial $P(x) = x^4 - 2x^3 - 2x^2 - 2x + 1$ provides one of the simplest examples. Its roots are $\tau \pm \sqrt{\tau}$ (both real) and $-(\tau - 1) \pm i\sqrt{\tau - 1}$ (both on the unit circle), where $\tau = \big(1 + \sqrt{5}\,\big)/2$ is the golden number. The corresponding companion matrix M is not of finite order, and the reversing symmetry group is thus $\mathcal{R}(M) \simeq (C_2 \times \mathbb{Z}^2) \times_s C_2$.

Let us come back to the general discussion and ask for the properties of reversing symmetries. Let G be a reversing symmetry of M, so that $GM = M^{-1}G$ and hence also $GM^n = M^{-n}G$ for all $n \in \mathbb{Z}$. If $p(x)$ is any polynomial, we then also get $Gp(M) = p(M^{-1})G$. Since G is a reversing symmetry, G^2 is a symmetry. If we now assume that $M \in \mathrm{GL}(n,\mathbb{Z})$ has minimal polynomial of degree n, we get $G^2 \in \mathbb{Q}[M]$ from Fact 6, i.e. $G^2 = q(M)$ for some q with coefficients in $\mathbb{Q}$. Consequently, $Gq(M)G^{-1} = q(M^{-1})$, but also $Gq(M)G^{-1} = G^2 = q(M)$, so that $q(M) = q(M^{-1})$.

[11] See http://www.math.TU-Berlin.de/~kant/.

If $q(M)$ is a monomial, i.e. $q(M) = M^{\ell}$ for some ℓ, then $M^{2\ell} = 1$ and hence $G^4 = 1$. This case is also discussed in [19, Prop. 2(i)]. It clearly extends to the situation that $q(M^{-1}) = \bigl(q(M)\bigr)^{-1}$, which is more general. Apart from this, we recall the following result from [19, p. 21] (its proof, which was only contained in the preprint version of [19], is a coset counting argument).

Fact 11 *Let M be of infinite order. If the factor group $\mathcal{S}(M)/\langle M\rangle$ is finite, then any reversing symmetry G of M must be of finite order, and $G^{2k} = \mathbf{1}$ for some integer k that divides the order of the factor group.* □

Let us only add that, in line with our above argument, one first obtains $G^{2k} \in \langle M\rangle$ and hence $G^{4k} = \mathbf{1}$. But $\langle M\rangle \simeq \mathbb{Z}$ by assumption, so it cannot have a subgroup of order 2, and thus already $G^{2k} = \mathbf{1}$.

Fact 11 certainly applies to our scenario whenever M is not of finite order, but $\mathcal{S}(M)$ Abelian and of rank 1. This type of result is helpful because it restricts the search for reversing symmetries to one among elements of finite order. It is certainly possible to extend the result to other cases, but in general one has to expect reversing symmetries of infinite order, in particular if the rank of $\mathcal{S}(M)$ is ≥ 2. Even then some results are possible because it would be sufficient to know whether reversibility implied the existence of *some* reversing symmetries of finite order. However, this question is more involved and will not be discussed here.

3 Extensions and further directions

In this Section, we will summarize some additional aspects of our analysis, namely the extension of symmetries to affine mappings, the modifications needed to treat the related situation of the projective matrix group $\mathrm{PGL}(n,\mathbb{Z})$, and the extension of (reversing) symmetries from a group setting to that of (matrix) rings or semi-groups.

3.1 Extension to affine transformations

So far, we have mainly discussed linear transformations (w.r.t. the torus), but it is an interesting question what happens if one extends the search for (reversing) symmetries to the group of *affine* transformations, in particular in view of Fact 1. Since both arguments and results are the exact analogues of those for the case $n = 2$ as derived in [12], we will be very brief here.

In Euclidean n-space, the group of affine transformations is the semi-direct product $\mathcal{G}_a = \mathbb{R}^n \times_s \mathrm{GL}(n,\mathbb{R})$, with $\mathbb{R}^n$ (the translations) being the normal subgroup. Elements are written as (t, M) with $t \in \mathbb{R}^n$ and $M \in \mathrm{GL}(n,\mathbb{R})$, and the product of two transformations is $(t, M) \cdot (t', M') = (t + Mt', MM')$. The neutral element is $(0, \mathbf{1})$, and we have $(t, M)^{-1} = (-M^{-1}t, M^{-1})$.

If we now observe that $\mathbb{T}^n = \mathbb{R}^n/\mathbb{Z}^n$, it is immediately clear that the affine transformations of $\mathbb{T}^n$ form the group

$$\mathcal{G}_a^{\mathbb{T}^n} \; = \; \mathbb{T}^n \times_s \mathrm{GL}(n, \mathbb{Z}) \tag{32}$$

which is still a semi-direct product. Here, $\mathbb{T}^n$ can be written as $[0, 1)^n$ with addition mod. 1, and the product of transformations is modified accordingly.

If we now ask for an affine (reversing) symmetry of a matrix M (now being identified with the element $(0, M) \in \mathcal{G}_a^{\mathbb{T}^n}$) we find

Proposition 4 *The affine transformation (t, G) is a (reversing) symmetry of the toral automorphism $(0, M)$ if and only if*

(*a*) *G is a (reversing) symmetry of M in $\mathrm{GL}(n, \mathbb{Z})$ and*

(*b*) *$Mt = t$ (mod 1).*

Proof: We have $(t, G) \cdot (0, M) = (t, GM)$, and $(0, M^{\pm 1}) \cdot (t, G) = (M^{\pm 1}t, M^{\pm 1}G)$. Our assertion then follows from the uniqueness of factorization in semi-direct products. □

From the condition $Mt = t$ (mod 1) it is clear that we need not consider all translations in $\mathbb{T}^n$ but only those with *rational* components, which we denote as Λ_∞. For many concrete problems, it would actually be even more appropriate to restrict to discrete sublattices, e.g. to the so-called q-division points $\Lambda_q \simeq (C_q)^n$ which consists of all rational points with denominator q.

From the above result, it is clear that we can get (reversing) k-symmetries (recall the definitions from Section 1.2). In fact, the equation $M^k t = t$ on the torus has $a_k = |\det(M^k - \mathbf{1})|$ different solutions provided no eigenvalue of M^k is 1. Clearly,

$$a_k \; = \; \sum_{\ell | k} \ell \cdot c_\ell \tag{33}$$

where c_ℓ counts the true orbits of length ℓ, and the Möbius inversion formula gives

$$c_k \; = \; \frac{1}{k} \sum_{\ell | k} \mu(\tfrac{k}{\ell}) \cdot a_\ell \tag{34}$$

with the Möbius function $\mu(m)$ [16, p. 29]. If c_k is positive for some k, we get a k-symmetry (and, hence, eventually a reversing k-symmetry) of M. These numbers can easily be calculated explicitly, where a very natural tool is provided by the so-called dynamical or Artin-Mazur ζ-functions [18]. Here, the a_k's can be extracted from the series expansion of the logarithm of the ζ-function, while the c_k's appear as exponents of the factors of the Euler product expansion of the ζ-function itself.

3.2 The case of $\mathrm{PGL}(n,\mathbb{Z})$

Let us start by the observation that $\mathrm{PGL}(n,\mathbb{Z})$ can be described via quotienting w.r.t. $\{\pm\mathbf{1}\}$, i.e.

$$\mathrm{PGL}(n,\mathbb{Z}) \simeq \mathrm{GL}(n,\mathbb{Z})/\{\pm\mathbf{1}\}\,.$$

In other words, rather than consider single matrices M, one has to consider pairs, $[M] := \{\pm M\}$. Let us write $\mathcal{S}[M]$ for the new PGL case and keep the old notation for the GL situation treated above.

The modification needed for the symmetry analysis given above is then actually fairly trivial, as we always had $\pm\mathbf{1}$ among them, and we can simply factor that out. So, we get

$$\mathcal{S}[M] \;\simeq\; \mathcal{S}(M)/\{\pm\mathbf{1}\}\,. \tag{35}$$

The case of reversing symmetries, however, requires some care. Since we now calculate mod $\pm\mathbf{1}$, a projective matrix $[M]$ can also be reversible through $GMG^{-1} = -M^{-1}$. But if this happens, the square, M^2, is again reversible in the old sense. This mechanism can (and will) give rise to reversing 2-symmetries (recall Section 1.2 for the definition) in $\mathrm{GL}(n,\mathbb{Z})$. Whereas [12] gave examples in $\mathrm{GL}(2,\mathbb{Z})$, Eq. (31) shows that skew-symmetric symplectic matrices satisfying $M^t = -M$ are not reversible in $\mathrm{GL}(2n,\mathbb{Z})$ whereas their squares are reversible. Also, the example (30) is reversible in $\mathrm{PGL}(8,\mathbb{Z})$ since a $G \in \mathrm{GL}(8,\mathbb{Z})$ can be found, by direct calculation, that satisfies the relation $GMG^{-1} = -M^{-1}$.

Let us finally check what happens in the extension to affine transformations. In complete analogy to the case $n = 2$, see [12], one can show that the corresponding affine group is the semidirect product $\Lambda_2 \times_s \mathrm{PGL}(n,\mathbb{Z})$ with Λ_2 the 2-division points. This really is the consequence of identifying x with $-x$ on $\mathbb{T}^n$, and Λ_2 is the set of 2^n translations that satisfy the condition $t = -t \pmod 1$.

Now, the above Proposition 4 applies to the case of PGL-matrices in very much the same way, just the possible translations t are restricted to the 2-division points.

3.3 Symmetries among general integer matrices

For most of this article, we have focused on matrices in $\mathrm{GL}(n,\mathbb{Z})$ and their symmetries within the same group. However, none of the proofs given above depends on that restriction, and one can indeed also treat the case that both M and its symmetries are allowed to live in the larger set $\mathrm{Mat}(n,\mathbb{Z})$ which is a ring. This set is no longer a group w.r.t. multiplication. Nevertheless, we will continue to use the symbol $\mathcal{S}(M)$, now meaning

$$\mathcal{S}(M) \;:=\; \{G \in \mathrm{Mat}(n,\mathbb{Z}) \mid [M,G] = 0\}\,.$$

The most obvious extended symmetries which one gets in $\mathrm{Mat}(n, \mathbb{Z})$ are the integer multiples of the identity, but there really is a hierarchy of objects to look at, and it is most transparent if one phrases the situation for a matrix in $\mathrm{Mat}(n, \mathbb{Q})$ first:

Fact 12 *Let $M \in \mathrm{Mat}(n, \mathbb{Q})$ and let its characteristic polynomial $P(x)$ be irreducible over $\mathbb{Q}$. Let λ be any of its roots and $K = \mathbb{Q}(\lambda)$ the corresponding algebraic number field. Then the following statements hold.*

(a) $\mathrm{cent}_{\mathrm{Mat}(n,\mathbb{Q})}(M) \;\simeq\; K$.

(b) $\mathrm{cent}_{\mathrm{GL}(n,\mathbb{Q})}(M) \;\simeq\; K^{*}$, *where* $K^{*} = K \setminus \{0\}$.

(c) $\mathrm{cent}_{\mathrm{Mat}(n,\mathbb{Z})}(M) \;\simeq\; \mathcal{O}$, *where $\mathcal{O}$ is an order in K.*

(d) $\mathrm{cent}_{\mathrm{GL}(n,\mathbb{Z})}(M) \;\simeq\; \mathcal{O}^{\times}$. □

Here, $\mathrm{cent}_{\mathrm{GL}(n,\mathbb{Z})}(M) = \mathcal{S}(M)$ from above, even though M itself need not be an element of $\mathrm{GL}(n, \mathbb{Z})$. The proof is a slight variation of what we did for Fact 6 and Lemma 1, and need not be spelled out again. It is important to note that the order $\mathcal{O}$ appearing here, as mentioned before, in general is *not* the maximal order of K, though it contains $\mathbb{Z}[\lambda]$. The following is now an immediate consequence.

Proposition 5 *Let M be an integer matrix with irreducible characteristic polynomial $P(x)$. Let λ be a root of $P(x)$, and let $\mathcal{O}_{\max}$ be the maximal order in $\mathbb{Q}(\lambda)$. Then, $\mathcal{S}(M)$ is both a $\mathbb{Z}$-module and a ring, and isomorphic to an order $\mathcal{O}$ that satisfies $\mathbb{Z}[\lambda] \subset \mathcal{O} \subset \mathcal{O}_{\max}$.* □

Note that there is now also a natural extension to the case of simple matrices M, compare Theorem 1 and Eq. (20), but we omit further details here. Also, from Fact 6 it is clear that $\mathcal{S}(M)$ is Abelian if and only if the minimal polynomial of M has degree n.

As to reversibility, this new point of view requires some thought. By Corollary 4, M reversible implies $\det(M) = \pm 1$, so reversible integer matrices are restricted to $\mathrm{GL}(n, \mathbb{Z})$. It would then not be unnatural to also insist on the existence of at least one unimodular matrix G with $M^{-1} = GMG^{-1}$, and reversibility is basically as above, except that, if we enlarge the symmetries of M from subgroups of $\mathrm{GL}(n, \mathbb{Z})$ to subrings of $\mathrm{Mat}(n, \mathbb{Z})$, reversing symmetries get enlarged accordingly. Note, however, that the ring structure is lost: the sum of a symmetry and a reversing symmetry is not a meaningful operation in this context. Together, they only form a monoid, i.e. a semi-group (under matrix multiplication) with unit element.

To go one step further, one could then also rewrite the reversibility condition as

$$G \;=\; MGM \tag{36}$$

and only demand that G is non-singular, to avoid pathologies with projections to subspaces and to keep the statement of Corollary 4. Note that this is a slightly weaker form of reversibility, as one does not assume that G^{-1} is a meaningful mapping in this context. In particular, it is clear that there is then no need any more to restrict G to unimodular integer matrices, so that now $G \in \mathrm{GL}(n, \mathbb{Q})$. Reversibility in $\mathrm{GL}(n, \mathbb{Q})$ is solved by our Theorem 2 of Section 2.3. It is clear that, whenever $M \in \mathrm{GL}(n, \mathbb{Z})$ is reversible in $\mathrm{GL}(n, \mathbb{Q})$ with reversing symmetry G, then M also has a reversing symmetry $G' = qG$ which is an integer matrix (q is the least common multiple of the denominators of G). The inverse of G' is in $\mathrm{GL}(n, \mathbb{Q})$, but need not be in $\mathrm{GL}(n, \mathbb{Z})$. So, reversibility in $\mathrm{GL}(n, \mathbb{Q})$, but not in $\mathrm{GL}(n, \mathbb{Z})$, always leads to new cases of the weaker reversibility described by (36).

To give a concrete example, consider the matrices

$$M = \begin{pmatrix} 4 & 9 \\ 7 & 16 \end{pmatrix} \qquad \text{and} \qquad G = \begin{pmatrix} 3 & 0 \\ 4 & -3 \end{pmatrix}. \tag{37}$$

Then M is the matrix from [12, Ex. 2] that was shown to be irreversible in $\mathrm{GL}(2, \mathbb{Z})$. In fact, the automorphism of $\mathbb{T}^2$ induced by M is irreversible even in the larger group of homeomorphisms of the 2-torus, see Fact 1 above (and [4] and [3, p. 9] for more details on the connection between general and linear homeomorphisms). Nevertheless, one can check that $G = MGM$, where $\det(G) = -9$. In other words, M is reversible in $\mathrm{GL}(2, \mathbb{Q})$, as are *all* elements of $\mathrm{SL}(2, \mathbb{Z})$ by our previous discussion following Corollary 5.

Note that G does *not* induce a homeomorphism of the 2-torus because G^{-1} is not an integer matrix. However, G does induce an automorphism on any lattice of the torus of the form

$$\Lambda_q := \{ (\tfrac{m}{q}, \tfrac{n}{q})^t \mid 0 \le m, n < q \}$$

for which $\det(G) \neq 0 \pmod{q}$. This is relevant as a recent study [24] shows: the quantum map which corresponds to M (which, in turn, corresponds to the action of M on a (Wigner) lattice of the torus) showed an eigenvalue statistics according to the circular orthogonal ensemble (COE) rather than the unitary one (CUE). So, even though M does not have a reversing symmetry in the sense of Section 2.3, the presence of a "pseudo-symmetry" such as G still leaves its mark!

Acknowledgements

The authors would like to thank Peter A. B. Pleasants, Alfred Weiss and Benjamin Weiss for clarifying discussions, Gabriele Nebe for helpful advice on the literature, and Wilhelm Plesken for suggesting a number of improvements. This work was supported by the German and Australian Research Councils (DFG and ARC).

References

[1] R. L. Adler, "Symbolic dynamics and Markov partitions", *Bull. Amer. Math. Soc.* **35** (1998) 1–56.

[2] R. Adler, C. Tresser and P. A. Worfolk, "Topological conjugacy of linear endomorphisms of the 2-torus", *Trans. Amer. Math. Soc.* **349** (1997) 1633–1652.

[3] R. L. Adler and B. Weiss, *Similarity of Automorphisms of the Torus*, Memoirs of the AMS, vol. 98, AMS, Providence, RI (1970).

[4] R. L. Adler, and R. Palais, "Homeomorphic conjugacy of automorphisms of the torus", *Proc. Amer. Math. Soc.* **16** (1965) 1222–5.

[5] W. A. Adkins and S. H. Weintraub, *Algebra: An Approach via Module Theory*, Springer, New York (1992).

[6] V. I. Arnold and A. Avez, *Ergodic Problems of Classical Mechanics*, Benjamin, New York (1968); reprint: Addison-Wesley, Redwood City, CA (1989).

[7] M. Baake, "Reversing symmetry groups of cat maps", in: *Group 21*, vol. II, eds. H.-D. Doebner, W. Scherer and C. Schulte, World Scientific, Singapore (1997), pp. 860–4; math.DS/9911061.

[8] M. Baake, "A Guide to Mathematical Quasicrystals", in: *Quasicrystals*, eds. J.-B. Suck, M. Schreiber and P. Häußler, Springer, Berlin (2001), in press; preprint math-ph/9901014.

[9] M. Baake, U. Grimm and D. Joseph, "Trace maps, invariants, and some of their applications", *Int. J. Mod. Phys.* **B 7** (1993) 1527–50; math-ph/9904025.

[10] M. Baake, J. Hermisson and P. A. B. Pleasants, "The torus parametrization of quasiperiodic LI-classes", *J. Phys.* **A 30** (1997) 3029–56.

[11] M. Baake and J. A. G. Roberts, "Symmetries and reversing symmetries of trace maps", written for: *Proceedings of the 3rd International Wigner Symposium*, Oxford (1993), unpublished; preprint math.DS/9901124.

[12] M. Baake and J. A. G. Roberts, "Reversing symmetry group of $\mathrm{GL}(2,\mathbb{Z})$ and $\mathrm{PGL}(2,\mathbb{Z})$ matrices with connections to cat maps and trace maps", *J. Phys.* **A 30** (1997) 1549–73.

[13] Z. I. Borevich and I. R. Shafarevich, *Number Theory*, Academic Press, New York (1966).

[14] R. Bowen, "Markov partitions for Axiom A diffeomorphisms", *Amer. J. Math.* **92** (1970) 725–747.

[15] H. Brown, R. Bülow, J. Neubüser, H. Wondratschek and H. Zassenhaus, *Crystallographic Groups of Four-Dimensional Space*, Wiley, New York (1978).

[16] H. Cohn, *A Classical Invitation to Algebraic Numbers and Class Fields*, 2nd printing, Springer, New York (1988).

[17] D. Damanik, "Gordon-type arguments in the spectral theory of one-dimensional quasicrystals", in: *Directions in Mathematical Quasicrystals*, eds. M. Baake and R. V. Moody, CRM Monograph Series, Amer. Math. Soc., Providence, RI (2000), pp. 277–305; preprint math-ph/9912005.

[18] M. Degli Esposti and S. Isola, "Distribution of closed orbits for linear automorphisms of tori", *Nonlinearity* **8** (1995) 827–42.

[19] G. R. Goodson, "Inverse conjugacies and reversing symmetry groups", *Amer. Math. Monthly* **106** (1999) 19–26.

[20] H. Hasse, *Über die Klassenzahl abelscher Zahlkörper*, Akademie-Verlag, Berlin (1952); corr. reprint, Springer, Berlin (1985).

[21] N. Jacobson, *Lectures in Abstract Algebra II: Linear Algebra*, van Nostrand, Princeton, NJ (1953); reprint: Springer, New York (1975).

[22] A. Katok, S. Katok and K. Schmidt, "Rigidity of measurable structure for $\mathbb{Z}^d$-action by automorphisms of a torus", preprint math.DS/0003032.

[23] A. Katok and B. Hasselblatt, *Introduction to the modern theory of dynamical systems*, Cambridge University Press, Cambridge (1995).

[24] J. P. Keating and F. Mezzadri, "Pseudo-symmetries of Anosov maps and spectral statistics", *Nonlinearity* **13** (2000) 747–76.

[25] J. P. Keating and F. Mezzadri, "Torus maps, symmetries and spectral statistics", preprint HPL-BRIMS-1999-11.

[26] J. S. W. Lamb, "Reversing symmetries in dynamical systems", *J. Phys.* **A 25** (1992) 925–37; and: *Reversing Symmetries in Dynamical Systems*, PhD-thesis, Univ. Amsterdam (1994).

[27] J. S. W. Lamb and G. R. W. Quispel, "Reversing k-symmetries in dynamical systems", *Physica* **D 73** (1994) 277–304; and: "Cyclic reversing k-symmetry groups", *Nonlinearity* **8** (1995) 1005–26.

[28] J. S. W. Lamb and J. A. G. Roberts, "Time-reversal symmetry in dynamical systems: A survey", *Physica* **D 112** (1998) 1–39.

[29] S. Lang, *Algebra*, 3rd ed., Addison Wesley, Reading, MA (1993).

[30] J. M. Luck, C. Godrèche, A. Janner and T. Janssen, "The nature of the atomic surfaces of quasiperiodic self-similar structures", *J. Phys.* **A 26** (1993) 1951–99.

[31] J. Neukirch, *Algebraische Zahlentheorie*, Springer, Berlin (1992); English ed.: *Algebraic Number Theory*, Springer, Berlin (1999).

[32] J. Opgenorth, W. Plesken and T. Schulz, "Crystallographic algorithms and tables", *Acta Cryst.* **A 54** (1998) 517–31.

[33] J. Palis and J. C. Yoccoz, "Centralizers of Anosov diffeomorphisms on tori", *Ann. Sci. Ecole Norm. Sup.(4)* **22** (1989) 99–108.

[34] K. Petersen, *Ergodic Theory*, Cambridge University Press, Cambridge (1983); corr. reprint (1989).

[35] W. Plesken, "Kristallographische Gruppen", in: *Group Theory, Algebra, and Number Theory*, ed. H. G. Zimmer, de Gruyter, Berlin (1996), pp. 75–96.

[36] M. Pohst and H. Zassenhaus, *Algorithmic Algebraic Number Theory*, Cambridge University Press, Cambridge (1989).

[37] A. M. F. Rivas, M. Saraceno and A. M. Ozorio de Almeida, "Quantization of multidimensional cat maps", *Nonlinearity* **13** (2000) 341–76.

[38] J. A. G. Roberts and M. Baake, "Trace maps as 3D reversible dynamical systems with an invariant", *J. Stat. Phys.* **74** (1994) 829–88.

[39] J. A. G. Roberts and M. Baake, "Symmetries and reversing symmetries of area-preserving polynomial mappings in generalised standard form", La Trobe University preprint (2000).

[40] J. A. G. Roberts and G. R. W. Quispel, "Chaos and time-reversal symmetry. Order and chaos in reversible dynamical systems", *Phys. Rep.* **216** (1992) 63–177.

[41] J. A. G. Roberts and R. S. Wilson, "Reversibility of orientation-reversing cat maps and the amalgamated free product structure of PGL(2,$\mathbb{Z}$)", LaTrobe preprint (1999).

[42] R. Salem, *Algebraic Numbers and Fourier Analysis*, Heath Math. Monographs, Boston, MA (1963).

[43] M. B. Sevryuk, *Reversible Systems*, LNM 1211, Springer, Berlin (1986).

[44] O. Taussky, "Introduction into connections between algebraic number theory and integral matrices", appendix 2 of [16], pp. 305–21.

[45] L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd ed., Springer, New York (1996).