Reversing symmetry group of $Gl(2,\mathbb{Z})$ and $PGl(2,\mathbb{Z})$ matrices with connections to cat maps and trace maps

1997 J. Phys. A: Math. Gen. 30 1549

(http://iopscience.iop.org/0305-4470/30/5/020)

J. Phys. A: Math. Gen. **30** (1997) 1549–1573. Printed in the UK PII: S0305-4470(97)77054-9

Reversing symmetry group of $Gl(2,\mathbb{Z})$ and $PGl(2,\mathbb{Z})$ matrices with connections to cat maps and trace maps

Michael Baake† and John A G Roberts‡§

† Institut für Theoretische Physik, Universität Tübingen, Auf der Morgenstelle 14, D-72076 Tübingen, Germany

‡ Department of Mathematics, The University of Melbourne, Parkville, Victoria 3052, Australia

§ Department of Mathematics, LaTrobe University, Bundoora, Victoria 3083, Australia‖

Received 9 August 1996

Abstract. Dynamical systems can have both symmetries and time-reversing symmetries. Together these two types of symmetries form a group called the reversing symmetry group $\mathcal{R}$ with the symmetries forming a normal subgroup $\mathcal{S}$ of $\mathcal{R}$. We give a complete characterization of $\mathcal{R}$ (and hence $\mathcal{S}$) in the dynamical systems associated with the groups of integral matrices $Gl(2,\mathbb{Z})$ and $PGl(2,\mathbb{Z})$. To do this, we use well known methods of number theory, such as Dirichlet's unit theorem for quadratic fields and Gauß' results on the equivalence of integer quadratic forms, and employ the algebraic structure of the modular group $PSl(2,\mathbb{Z})$ as a free product. We show how some recently discussed generalizations of the reversing symmetry group are also nicely illustrated when we consider affine extensions of these matrix groups. Our results are applicable to hyperbolic toral automorphisms (Anosov or *cat* maps), pseudo-Anosov maps, and the group of three-dimensional (3D) trace maps that preserve the Fricke–Vogt invariant.

0. Introduction

Symmetry is a much studied concept in both group theory and dynamical systems. This paper combines algebraic and group theoretic notions with those of dynamical systems, in a spirit similar to several recent papers [3, 16, 18, 19, 25, 26], in order to classify symmetries and reversing symmetries of two important classes of dynamical systems.

In the context of group theory, we will be interested in finding those elements S of a group $\mathcal{G}$ which conjugate a given element F into itself (and hence commute with it), and those elements R which conjugate F into its inverse. The set of elements S is well known in group theory as the *centralizer* of F (in $\mathcal{G}$), and is always non-empty because it at least contains F and its powers (including $F^0 = Id$). It is interesting to know whether it contains other elements. On the other hand, the existence of *any* R which makes F and F^{-1} conjugate is not obvious and depends on the particular choice of F.

The application of these group-theoretic structures to dynamical systems is our main concern. If we think now of F, S and R as automorphisms of some topological space of some manifold to itself, then S is called a *symmetry* of F, and R a *reversing symmetry* (because it relates F to its time-reversed version F^{-1}). Symmetries of dynamical systems have been studied for quite some time. Since they form a group $\mathcal{S}(F)$, group theory has helped in obtaining and understanding results. Time-reversing symmetries have received much less attention, although symmetries and time-reversing symmetries of a given F may be investigated systematically [16], as together they form the so-called *reversing symmetry*

‖ Permanent address.

0305-4470/97/051549+25\$19.50

group $\mathcal{R}(F)$, with the symmetries $\mathcal{S}(F)$ as a normal subgroup. Knowledge of $\mathcal{R}$ and its structure helps to understand the dynamics (as summarized, for instance, in its phase portrait), see [17–19, 27] for a detailed discussion.

The purpose of this paper is to show that the possible structure of $\mathcal{R}(F)$ is completely resolvable when we confine F, S and R to the groups $Gl(2,\mathbb{Z})$ and $PGl(2,\mathbb{Z})$. These groups (or their index-2 subgroups of elements of positive determinant) are much studied and feature in many contexts. For example, $Gl(2,\mathbb{Z})$ is well known as the group of two-dimensional (2D) toral automorphisms or, in crystallography, as the group of lattice automorphisms in 2D, whereas $PSl(2,\mathbb{Z})$ (the well known modular group) is isomorphic to the group of biholomorphic transformations of the Riemann sphere. Much is also known about the structure of $Gl(2,\mathbb{Z})$, $PGl(2,\mathbb{Z})$ and their subgroups. For example, $PSl(2,\mathbb{Z})$ is known to be the *free product* of a cyclic group of order 2 with one of order 3, a property that will prove useful in our analysis.

On the other hand, $Gl(2,\mathbb{Z})$ and $PGl(2,\mathbb{Z})$ and their subgroups are associated with important classes of dynamical systems. The maps induced on the torus by the elements of $Gl(2,\mathbb{Z})$ are the toral automorphisms. The hyperbolic ones out of the latter are chaotic on the entire torus, with the orientation-preserving ones being the only structurally-stable symplectic maps of the torus. The most famous example is the 'cat map' of Arnold and Avez [1], induced by

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

Hyperbolic toral automorphisms, or *cat maps* as we more loosely call them, have received much attention as chaotic, yet solvable, systems [9, 22]

The set $PGl(2,\mathbb{Z})$ arises naturally in the group theory context as the quotient of $Gl(2,\mathbb{Z})$ by its centre. In geometric terms, the quotient of the 2-torus by the reflection in the origin ($\boldsymbol{x} \mapsto -\boldsymbol{x}$) produces the 2-sphere with four punctures. Consequently, each element of $PGl(2,\mathbb{Z})$ induces a mapping of this sphere to itself. In particular, the hyperbolic elements of $PGl(2,\mathbb{Z})$ induce chaotic automorphisms of the punctured sphere, which are examples of *pseudo-Anosov* mappings [5, 20].

Our interest in $PGl(2,\mathbb{Z})$ also arises in another way. This group is isomorphic to the group $\mathcal{G}$ of 3D invertible polynomial *trace maps* which preserve the Fricke–Vogt invariant

$$I(x, y, z) = x^2 + y^2 + z^2 - 2xyz - 1 \tag{2}$$

and fix the point $(1, 1, 1)$. Such mappings arise very naturally in physics from applications of transfer matrix techniques to phenomena displaying non-periodicity in space or time, e.g. cf [2, 23, 25, 30] and references therein. The canonical example is the Fibonacci trace map $F_1 : (x, y, z) \mapsto (y, z, 2yz - x)$ which, via the above-mentioned isomorphism between these polynomial mappings and $PGl(2,\mathbb{Z})$, can be associated with the matrix $R_1 = \pm \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$. We see that the structure of the reversing symmetry group of, for example, F_1 within the group $\mathcal{G}$ of polynomial mappings is simply a manifestation of that of R_1 in $PGl(2,\mathbb{Z})$.

In view of the many applications, we found it remarkable that the groups $Gl(2,\mathbb{Z})$ and $PGl(2,\mathbb{Z})$ appear to have enough structure to allow a calculation of the reversing symmetry group $\mathcal{R}$ within them, while at the same time the hyperbolic elements of these groups lead to non-trivial and interesting dynamical systems on compact manifolds, including the ones on the torus and the punctured sphere†.

† Up to now, most of the study of symmetries and reversing symmetries of automorphisms of 2D surfaces has been confined to automorphisms of the plane.

Searching for (reversing) symmetries inside a group also means to restrict them to a certain (natural) set. Though this might be necessary in one application, it might be too restrictive in another. For example, a linear mapping of the plane which is volume and orientation preserving (i.e. represented by an $Sl(2, \mathbb{Z})$ matrix) is conjugate both to itself (trivial) and to its inverse (obvious from its Jordan normal form). However, when we restrict ourselves to homeomorphisms of the torus induced by $Gl(2, \mathbb{Z})$ matrices, we need to look for homeomorphisms of the torus that can act as (reversing) symmetries. One important result for *hyperbolic* elements of $Gl(2, \mathbb{Z})$ follows from lemma 4 of [12]:

Lemma 1. Suppose two hyperbolic toral automorphisms (i.e. two hyperbolic elements of $Gl(2, \mathbb{Z})$) are conjugate to one another via a homeomorphism of the torus. Then this homeomorphism corresponds to the action of an element of $Gl(2, \mathbb{Z})$, or to the affine extension (with a rational translation) of such an element.

Furthermore, it is easy to show that an affine mapping of this type can only be a (reversing) symmetry if its linear part already is one itself (cf section 4 below). Consequently, for hyperbolic toral automorphisms, the existence of (reversing) symmetries amounts to searching essentially only in $Gl(2, \mathbb{Z})$ (this is not so for other toral automorphisms, e.g. the finite-order ones). It turns out that the consideration of *affine* transformations as (reversing) symmetries is also of independent interest. This is because it gives rise to the possibility that a power of a mapping F possesses additional (reversing) symmetries, a question that has attracted some attention recently [18, 19].

Let us, at this point, briefly describe how the paper is organized. After some preliminaries in section 1, we first discuss the case of $Gl(2, \mathbb{Z})$ in section 2. Here, we focus more on symmetries than on reversing symmetries, and employ some standard results from algebraic number theory to derive a complete classification. Then, in section 3 on $PGl(2, \mathbb{Z})$, we emphasize reversing symmetries and use the free product structure of $PSl(2, \mathbb{Z})$ to get everything as explicit as possible. This way we actually obtain a rather complete picture for both cases. While we proceed, we keep an open eye on (reversing) symmetries of powers of a given matrix which we can also completely classify. In section 4, we discuss the extension to affine symmetries and reversing symmetries, where we also re-derive (as a by-product) the set of polynomial mappings of 3-space that leave $I(x, y, z)$ of equation (2) invariant. This is followed by some concluding remarks.

1. Preliminaries

1.1. Symmetries and reversing symmetries

We have to introduce the concept of symmetry and reversing symmetry. Consider some (topological) space Ω, its automorphism group $\mathrm{Aut}(\Omega)$ and an element $F \in \mathrm{Aut}(\Omega)$ which, by definition, is invertible. Then, the group

$$\mathcal{S}(F) := \{G \in \mathrm{Aut}(\Omega) \mid G \circ F = F \circ G\} \tag{3}$$

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

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

$$R \circ F \circ R^{-1} = F^{-1}. \tag{4}$$

Such R is called a *reversing symmetry* of F, and when such an R exists, we call F reversible. We will, in general, not use different symbols for symmetries and reversing symmetries from now on, because together they form a group [16],

$$\mathcal{R}(F) := \{G \in \mathrm{Aut}(\Omega) | G \circ F \circ G^{-1} = F^{\pm 1}\} \tag{5}$$

the so-called *reversing symmetry group* of F. It is a subgroup of the *normalizer* of $\langle\langle F \rangle\rangle$ (the group generated by F) 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

$$\mathcal{R}(F)/\mathcal{S}(F) \simeq C_2. \tag{6}$$

The underlying algebraic structure has fairly strong consequences. One is that reversing symmetries cannot be of odd order [16], another one is

Lemma 2. If F (with $F^2 \neq Id$) has an involutory reversing symmetry R, the reversing symmetry group of F is a semi-direct product†:

$$\mathcal{R}(F) = \mathcal{S}(F) \times_{\mathrm{s}} C_2.$$

Proof. Certainly, $\{Id, R\} \simeq C_2$ is a subgroup of $\mathcal{R}(F)$, and $\mathcal{S}(F) \cap C_2 = \{Id\}$ by assumption. As the representation of *any* $T \in \mathcal{R}(F)$ in the form $T = G \circ H$ with $G \in \mathcal{S}(F)$ (the normal subgroup) and $H \in C_2$ is unique, the statement follows. □

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 $\mathrm{Aut}(\Omega)$. 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 [18] and, in particular, [17]. 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 $\mathcal{R}(F)$. If such a situation occurs, we say that F possesses additional k-symmetries, respectively reversing k-symmetries. Let us make this a little more precise.

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. To analyse the structure a bit further, let us therefore restrict to mappings $F \in \mathrm{Aut}(\Omega)$ of *infinite* order. Let us introduce

$$\mathcal{S}_\infty(F) := \bigcup_{k=1}^{\infty} \mathcal{S}(F^k) \tag{7}$$

which is clearly a subgroup of $\mathrm{Aut}(\Omega)$. Let us also introduce the automorphism induced by F

$$\phi_F(G) := F \circ G \circ F^{-1}. \tag{8}$$

One can then easily see that $G \in \mathcal{S}_\infty(F)$ if and only if $\phi_F^n(G) = G$ for some $n \in \mathbb{N}$. Now, we actually want to know the minimal such order n, wherefore we introduce

$$\#_F(G) := \min\{n \in \mathbb{N} | \phi_F^n(G) = G\} \tag{9}$$

which is finite on $\mathcal{S}_\infty(F)$ and infinite otherwise. Consequently, we have

$$\mathcal{S}_\infty(F) = \{G \in \mathrm{Aut}(\Omega) | \#_F(G) < \infty\}. \tag{10}$$

† We use $N \times_{\mathrm{s}} H$ for the semi-direct product of two groups N and H, with N being the normal subgroup.

Of course, it can 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, $\#_F(G) = k$ might be larger than one in which case we call G a genuine or true k-symmetry. G is a true† k-symmetry of F if and only if the iterates of G under ϕ_F generate a proper k-cycle. It will be part of our classification later on to determine $\mathcal{S}_\infty$ and $\#_F$ for an interesting class of examples.

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

2. Matrices in $Gl(2,\mathbb{Z})$ and toral automorphisms

Toral automorphisms, in particular hyperbolic ones (cat maps), play an important role in the theory of dynamical systems, especially in connection with symbolic dynamics [9]. The toral automorphisms of the 2-torus $\mathbb{T} = \mathbb{R}^2/\mathbb{Z}^2$ can be described as the unimodular 2×2-matrices with integer coefficients which form the group $Gl(2,\mathbb{Z})$.

2.1. Symmetries

It is certainly an interesting and important question to know, for a given M, its symmetries, i.e. the set of mappings that commute with it—where one has to specify a class of mappings to consider. So, determining the symmetries of a mapping means to find its centralizer inside some 'natural' set. In the setting of toral automorphisms, one very obvious choice is the entire set of them, i.e. $Gl(2,\mathbb{Z})$. The centralizer is then a group, and we have, for $M \in Gl(2,\mathbb{Z})$,

$$\mathcal{S}_{Gl(2,\mathbb{Z})}(M) = \mathrm{cent}_{Gl(2,\mathbb{Z})}(M) = \{G \in Gl(2,\mathbb{Z}) | MG = GM\}. \tag{11}$$

This is precisely what we want to determine now. To be more precise, we are only interested in the structure of the symmetry group as this 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 PMP^{-1} because

$$\mathcal{S}(PMP^{-1}) = P\mathcal{S}(M)P^{-1} \tag{12}$$

where we have suppressed the index $Gl(2,\mathbb{Z})$ because it will not change until the end of this section.

When we work along the various possibilities, we shall encounter two principal situations. A given M determines its characteristic polynomial which is monic and has only integer coefficients, so its roots are algebraic integers. Furthermore, it is either *reducible* over $\mathbb{Z}$ (which happens if and only if the eigenvalues of M are elements of $\{1, -1\}$) or it is *irreducible*. In the latter case we know that M is diagonalizable (over $\mathbb{C}$) and its two eigenvalues are different. This simplifies the problem considerably, as we will see from the next lemma, while the reducible case has to be treated separately and explicitly. Now, for the irreducible case we formulate

Lemma 3. Let $M \in Gl(2,\mathbb{Z})$ 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 $Gl(2,\mathbb{Z})$ is isomorphic with a subgroup of the group of units in the maximal order of the quadratic field $\mathbb{Q}(\lambda)$.

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

Proof. It is clear that irreducibility of $P(x)$ implies that M must have two different eigenvalues, λ and $\det(M)/\lambda$ in fact. We then know that diagonalization can be performed not only in $\mathbb{C}$ but also in $\mathbb{Q}(\lambda)$ because this is the quadratic field generated by λ and we can solve the linear equations for the eigenvectors within $\mathbb{Q}(\lambda)$ (see chapter XIV of [15] for details), i.e. there is a matrix U with elements in $\mathbb{Q}(\lambda)$ such that

$$U\,M\,U^{-1} = \mathrm{diag}(\lambda, \det(M)/\lambda). \tag{13}$$

Now, only diagonal matrices can commute with a diagonal matrix with pairwise different diagonal elements. To find the centralizer of M, we have to determine all other matrices $A \in Gl(2,\mathbb{Z})$ which are also diagonalized by U. But if α is an eigenvalue of A, it must be an element of $\mathbb{Q}(\lambda)$. Since A is an integer matrix, α is an algebraic integer, hence an element of $\mathcal{O}$, the maximal order of $\mathbb{Q}(\lambda)$ ($\mathcal{O}$ is the intersection of $\mathbb{Q}(\lambda)$ with the set of algebraic integers). Finally, as A has determinant ± 1, α must be a *unit* in $\mathcal{O}$. Though the group property of matrices commuting with M is obvious, we do not know whether *all* units appear this way. So, we only know that the centralizer is isomorphic with a subgroup of the unit group of $\mathcal{O}$ which was the statement. □

It is clear that the centralizer is isomorphic with the entire unit group if λ itself (or its conjugate) is a fundamental unit (i.e. a generator of the unit group). This happens for the finite-order elements with irreducible $P(x)$, as we shall see.

Now, we will proceed in three steps, discussing the situation for elements of finite-order (*elliptic* case), for elements with non-trivial Jordan normal form (*parabolic* case), and finally for all other elements of infinite order (*hyperbolic* case), and then summarize the findings in theorem 1.

2.1.1. Elements of finite order (elliptic case). It is a well known fact that any element of finite order in $Gl(2,\mathbb{Z})$ can only have order 1, 2, 3, 4 or 6—the proof is the same as that for the crystallographic restriction in 2D [28]. Finite order for $M \in Gl(2,\mathbb{Z})$ means that M has its eigenvalues on the unit circle, but as M is real and has determinant ± 1, they must be complex conjugates of one another with their product being the determinant. But since $\mathrm{tr}(M) \in \mathbb{Z}$, we have only finitely many possibilities, namely those mentioned.

Now, to start with the trivial cases: $\{\pm \mathbb{1}\}$ is the centre of $Gl(2,\mathbb{Z})$, i.e. $M = \pm \mathbb{1}$ are the only matrices in $Gl(2,\mathbb{Z})$ to commute with every element of the group, so we have

$$\mathcal{S}(\pm\mathbb{1}) = Gl(2,\mathbb{Z}). \tag{14}$$

Here, $-\mathbb{1}$ is an involution, but a trivial one. There are more elements of second order, namely those M with eigenvalues 1 and -1. The Cayley–Hamilton theorem [15] for 2×2 matrices tells us that this happens if and only if $\mathrm{tr}(M) = 0$ and $\det(M) = -1$:

$$M^2 = \mathrm{tr}(M) \cdot M - \det(M) \cdot \mathbb{1} \tag{15}$$

from which one can derive the statement. (The other solutions of $M^2 = \mathbb{1}$, with different eigenvalues of course, are $M = \pm \mathbb{1}$ given above.) As the characteristic polynomial in this case is reducible, we cannot apply lemma 3 and have to treat it explicitly. The involutions under consideration thus have the form

$$M = \begin{pmatrix} a & b \\ c & -a \end{pmatrix} \qquad \text{with } a^2 + bc = 1. \tag{16}$$

Such matrices commute with $\pm M$ and with $\pm \mathbb{1}$, but with nothing else, as is easy to check explicitly. To proceed, we take advantage of the following.

Lemma 4. There are precisely two conjugacy classes of $Gl(2, \mathbb{Z})$-matrices M with $\mathrm{tr}(M) = 0$ and $\det(M) = -1$. They are faithfully represented by the two involutions

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \tag{17}$$

Proof. It is easy to check that these two matrices must be in different conjugacy classes of $Gl(2, \mathbb{Z})$. So we have to show that they are sufficient. From lemma 5.5 on p 166 of [10] we know that *any* involution $M \in Gl(2, \mathbb{Z})$ with negative determinant is conjugate to either $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ or $\begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}$. The second matrix in turn is conjugate to $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ which completes the proof. □

For the non-trivial involutions $M^2 = \mathbb{1} \neq \pm M$ we thus have

$$\mathcal{S}(M) = \{\pm M, \pm \mathbb{1}\} \simeq C_2 \times C_2 \tag{18}$$

where here and in the following we use the symbol C_n for the cyclic group of order n and $\times$ for the direct product of groups. We shall write groups multiplicatively throughout even though most of them will be Abelian.

Because it is closely related, let us next consider the case of matrices M of fourth order. Again, we are interested in those cases where no smaller power of M gives $\mathbb{1}$ as we have treated those already. So, we must have a *primitive* fourth root of unity and its complex conjugate as eigenvalues, which means $\pm \mathrm{i}$. So, M is truly of fourth order if and only if $\mathrm{tr}(M) = 0$ and $\det(M) = 1$. Such matrices have the form

$$M = \begin{pmatrix} a & b \\ c & -a \end{pmatrix} \qquad \text{with } a^2 + bc = -1 \tag{19}$$

and (again!) commute with $\pm M$ and $\pm \mathbb{1}$. Can we have more? The characteristic polynomial is irreducible over $\mathbb{Z}$, so we know from lemma 3 above that we have an isomorphism with a subgroup of the unit group of $\mathbb{Z}[\mathrm{i}]$, the maximal order in $\mathbb{Q}(\mathrm{i})$. This unit group is known to be $\{1, \mathrm{i}, -1, -\mathrm{i}\} \simeq C_4$ [7], which we have already exhausted wherefore we cannot find further symmetries. The difference to the previous case is that, as $M^2 = -\mathbb{1}$, the four elements form a group isomorphic with C_4 (rather than $C_2 \times C_2$) and we obtain

$$\mathcal{S}(M) = \{\pm M, \pm \mathbb{1}\} \simeq C_4. \tag{20}$$

Next, consider elements of third order, i.e. $M^3 = \mathbb{1}$, but $M \neq \mathbb{1}$. So, we need a primitive third root of unity and its complex conjugate as eigenvalues which is unique: $(-1 \pm \mathrm{i}\sqrt{3})/2$. Consequently, we must have $\mathrm{tr}(M) = -1$ and $\det(M) = 1$, and the matrices are of the form

$$M = \begin{pmatrix} a-1 & b \\ c & -a \end{pmatrix} \qquad \text{with } a(a-1) + bc = -1. \tag{21}$$

They commute with $\mathbb{1}, M, M^2$, but also with $-\mathbb{1}, -M, -M^2$, hence

$$\mathcal{S}(M) = \{\pm \mathbb{1}, \pm M, \pm M^2\} \simeq C_2 \times C_3 \simeq C_6. \tag{22}$$

In fact, this symmetry group can be generated by $-M^2$ which happens to be a root of M in $Gl(2, \mathbb{Z})$. That there are no more elements can again be derived from lemma 3, as the characterisic polynomial is irreducible, the quadratic field is $\mathbb{Q}(\mathrm{e}^{2\pi \mathrm{i}/3})$ with maximal order $\mathbb{Z}[\varrho]$ where $\varrho = \mathrm{e}^{2\pi \mathrm{i}/6}$ (!) and the unit group [7] is $\{1, \varrho, \varrho^2, \ldots, \varrho^5\} \simeq C_6$.

Finally, the genuine order 6 case has to exclude order 2 and 3 (both treated already), so we need a complex conjugate pair of primitive sixth roots of unity here—which again is unique: $(1 \pm \mathrm{i}\sqrt{3})/2$. So, we must have $\mathrm{tr}(M) = 1$ and $\det(M) = 1$ (hence $M^3 = -\mathbb{1}$), and matrices of the form

$$M = \begin{pmatrix} a+1 & b \\ c & -a \end{pmatrix} \qquad \text{with } a(a+1) + bc = -1. \tag{23}$$

Certainly, they commute with M and its powers, but with nothing else—wherefore we here obtain the answer

$$\mathcal{S}(M) = \{\pm\mathbb{1}, \pm M, \pm M^2\} \simeq C_6. \tag{24}$$

The reason is as in the previous case, because we have to deal with $\mathbb{Q}(\mathrm{e}^{2\pi\mathrm{i}/6})$ which coincides with $\mathbb{Q}(e^{2\pi\mathrm{i}/3})$. Consequently, we have the same maximal order, $\mathbb{Z}[\varrho]$, with unit group isomorphic to C_6.

At this point, the discussion of elements of finite order is complete. An alternative derivation of the results could use a faithful set of representatives of the various conjugacy classes, which is given in table 1 (it is possible to determine the number of conjugacy classes, see theorem 2 below, and to calculate suitable representatives).

2.1.2. Parabolic elements. Since $|\,\mathrm{tr}(M)| > 2$ is sufficient for hyperbolicity, we have here to consider the cases with $\mathrm{tr}(M) = \pm 2$ and $\det(M) = 1$, i.e. both eigenvalues being 1 or -1, but *excluding* the cases $M = \pm\mathbb{1}$ which are of finite order. (The remaining case with $\det(M) = -1$ and $\mathrm{tr}(M) = \pm 1$ is also hyperbolic and therefore treated in the next section.)

The only possibilities to be considered are thus

$$M = \pm\begin{pmatrix} 1-a & b \\ -c & 1+a \end{pmatrix} \qquad \text{where } a^2 = bc. \tag{25}$$

One way to proceed is to find a good set of representatives of the conjugacy classes in $Gl(2, \mathbb{Z})$ with $\det = 1$ and $\mathrm{tr} = \pm 2$. To this end, we define (for $m \in \mathbb{Z}$)

$$T_m := \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \tag{26}$$

which certainly is of that type. It is easy to check that any such T_m is conjugate to its transpose: $T_m \sim (T_m)^t$, and also that $T_m \sim T_n$ if and only if $m = \pm n$.

Furthermore:

Lemma 5. The conjugacy classes of $Gl(2, \mathbb{Z})$ matrices with $\mathrm{tr}(M) = 2$ and $\det(M) = 1$ are faithfully represented by the matrices T_m of equation (26) with $m \in \mathbb{N}_0$. Out of those, only $T_0 = \mathbb{1}$ is of finite order.

Proof. The last statement of the lemma is obvious. Also, a matrix $M \in Gl(2, \mathbb{Z})$ with $\mathrm{tr}(M) = 2$ and $\det(M) = 1$ must have the form (25). Here, we can further assume that $a \neq 0$ and hence $bc \neq 0$, because $a = 0$ brings us back to the case of T_m or its transpose which has been discussed already. Consider now the equation

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}^{-1} = \begin{pmatrix} 1 - m\alpha\gamma\Delta & m\alpha^2\Delta \\ -m\gamma^2\Delta & 1 + m\alpha\gamma\Delta \end{pmatrix} \tag{27}$$

where $\Delta = \alpha\delta - \beta\gamma = \pm 1$. Let us now compare (25), with positive sign, and the right-hand side of (27). Write $b = r^2 b_0$ and $c = s^2 c_0$, $r, s > 0$, with b_0 and c_0 square-free (i.e. not divisible by any square except 1). But $bc = a^2$ then implies $b_0 = c_0$. Let $t = \gcd(r, s)$ and define r', s' through $r = tr'$ and $s = ts'$ where now $\gcd(r', s') = 1$. We then have to show the solvability of the set of equations

$$m\alpha\gamma\Delta = a \qquad m\alpha^2\Delta = t^2(r')^2 b_0 \qquad m\gamma^2\Delta = t^2(s')^2 b_0.$$

To achieve this, choose $\Delta = \text{sgn}(b_0)$, $\alpha = r'$, $\gamma = \text{sgn}(ab_0)\cdot s'$ and $m = t^2|b_0| = \gcd(b, c)$. But then we clearly solve the second and third equation and also have $m\alpha\gamma\Delta = \text{sgn}(ab_0)\cdot t^2|b_0|r's'\cdot\text{sgn}(b_0) = \text{sgn}(a)\cdot\sqrt{|bc|} = a$. Finally, since $\gcd(\alpha, \gamma) = 1$, we can always find $\beta, \delta \in \mathbb{Z}$ so that $\alpha\delta - \beta\gamma = \Delta = \text{sgn}(b_0)$. As, on the other hand, the matrices T_m with $m \in \mathbb{N}_0$ are pairwise inequivalent, the assertion follows. □

We have treated the case $\text{tr}(M) = 2$ here, but the rest is trivial:

Corollary 1. The conjugacy classes with $\text{tr} = -2$ and $\det = 1$ are faithfully represented by the matrices $-T_m$ with $m \in \mathbb{N}_0$.

Proof. Observe $\text{tr}(-M) = -\text{tr}(M)$ but $\det(-M) = \det(M)$. Since $-\mathbb{1}$ commutes with all matrices, the statement follows from the previous lemma. □

There is a reason why we called these special representing matrices T_m: they are a 2D representation of the 1D translation group, $\mathbb{Z}$, which is Abelian. In particular,

$$T_m \cdot T_n = T_{m+n} \tag{28}$$

and thus also $T_m = (T_1)^m$. This also implies $T_{-m} = (T_m)^{-1}$. Now, it is easy to check that T_m ($m \neq 0$) commutes only with the powers of T_1 and with their negatives—i.e. precisely with all matrices $\{\pm T_k | k \in \mathbb{Z}\} \simeq C_2 \times \mathbb{Z} \simeq C_2 \times C_\infty$.

Finally, we get the result for the symmetry group of any parabolic M ($M \neq \pm\mathbb{1}$) as

$$\mathcal{S}(M) \simeq C_2 \times \mathbb{Z} \tag{29}$$

where the infinite cyclic group is always generated by T_1 or one of its conjugates, i.e. in general by a root of M in $Gl(2,\mathbb{Z})$.

2.1.3. Elements of infinite order: hyperbolic case. One case with $|\text{tr}(M)| < 2$ did not appear above: $\text{tr}(M) = \pm 1$ with $\det(M) = -1$. This gives eigenvalues $\pm(\tau, -1/\tau)$ with $\tau = (1 + \sqrt{5})/2$ the golden ratio, so these M are hyperbolic. Furthermore, we have to discuss the case $|\text{tr}(M)| > 2$ where both eigenvalues of M must be real and, due to $|\det(M)| = 1$, one, λ say, must lie strictly outside the interval $[-1, 1]$ and the other strictly inside. Consequently, the larger eigenvalue is a Pisot–Vijayaraghavan number [6].

To solve the question for the symmetry group here, we may employ Dirichlet's unit theorem. It is clear that λ is a quadratic irrational and real, and its algebraic conjugate (the other solution of the characteristic polynomial) is different from it. So, from lemma 3 we know that the centralizer must be a subgroup of the unit group of the maximal order in $\mathbb{Q}(\lambda)$. Here, we have a quadratic field with *real* irrationality, so we know from Dirichlet's unit theorem [7] that the unit group is $\{\pm u^k | k \in \mathbb{Z}\} \simeq C_2 \times \mathbb{Z}$, where u is the fundamental unit, and $C_2 = \{\pm 1\}$ is the unit group of $\mathbb{Z}$. In particular, M corresponds to some power of u, u^m say, but need not have an mth root inside $Gl(2,\mathbb{Z})$. However, M certainly commutes with $\pm M^n$ for any $n \in \mathbb{Z}$. So we have the C_2 part of the unit group. On the other hand, any non-trivial subgroup of $\mathbb{Z} \simeq C_\infty$ is isomorphic with C_∞ again!

So, for any hyperbolic toral automorphism M we now know that its symmetry group is given by

$$\mathcal{S}(M) \simeq C_2 \times \mathbb{Z}. \tag{30}$$

Now, there is still the question for the proper generator of the infinite cyclic group. As already mentioned, this need not be a matrix that corresponds to the fundamental unit, but can be some power of it—and this has to be calculated for each special M. This can be done for each given M in finitely many steps because there is a finite algorithm to determine the fundamental root u, see [4], and the eigenvalues of M correspond (up to a sign) to powers of u.

2.1.4. Symmetries summarized. Let us summarize our findings in the following theorem.

Theorem 1. The structure of the centralizer of an element $M \in Gl(2, \mathbb{Z})$ (i.e. the structure of the symmetry group $\mathcal{S}(M) \subset Gl(2, \mathbb{Z})$) has precisely one of the following forms:

(1) $\mathcal{S}(M) = Gl(2, \mathbb{Z})$ if and only if $M = \pm \mathbb{1}$;

(2) $\mathcal{S}(M) = \{\pm\mathbb{1}, \pm M\} \simeq C_2 \times C_2$ if and only if $\mathrm{tr}(M) = 0$ and $\det(M) = -1$ (i.e. $M^2 = \mathbb{1} \neq \pm M$);

(3) $\mathcal{S}(M) = \{\pm\mathbb{1}, \pm M\} \simeq C_4$ if and only if $\mathrm{tr}(M) = 0$ and $\det(M) = 1$ (i.e. $M^4 = -M^2 = \mathbb{1}$);

(4) $\mathcal{S}(M) = \{\pm\mathbb{1}, \pm M, \pm M^2\} \simeq C_6$ if and only if $\mathrm{tr}(M) = \pm 1$ and $\det(M) = 1$ (i.e. $M^6 = \mathbb{1} \neq M^2$); or

(5) $\mathcal{S}(M) \simeq C_2 \times C_\infty$ if and only if M is not of finite order.

2.2. Reversing symmetries

Now, for various reasons (some mentioned in the introduction) one is not only interested in the symmetries of a mapping M, but also in its so-called *reversing symmetries*, i.e. in such mappings G that conjugate M into its inverse

$$GMG^{-1} = M^{-1}. \tag{31}$$

All such elements, together with the symmetries of M, form the so-called reversing symmetry group of M, abbreviated as $\mathcal{R}(M)$. It contains the symmetry group $\mathcal{S}(M)$ as a normal subgroup. There are precisely two possibilities: either $\mathcal{R}(M) = \mathcal{S}(M)$ or $\mathcal{R}(M)$ is a group extension of $\mathcal{S}(M)$ of index 2. We will meet both cases later. The property of being reversible is again an invariant of the conjugacy classes, and a matrix M is reversible if and only if the class represented by M is ambivalent, i.e. contains the inverses of its members.

Let us consider this for the case of $Gl(2, \mathbb{Z})$-matrices. For invertible 2×2 matrices one has a simple relation between the trace of a matrix and that of its inverse

$$\mathrm{tr}(M^{-1}) = \det(M) \cdot \mathrm{tr}(M) \tag{32}$$

which has the rather strong consequence that we can exclude all matrices M with $\det(M) = -1$ and $\mathrm{tr}(M) \neq 0$ from any further discussion in this section: they cannot be reversible because reversibility (31) would imply the *same* trace for M and M^{-1}, but from (32) we know that they have different sign. On the other hand, we can only escape this argument through $\mathrm{tr}(M) = 0$ which then means $M^2 = \pm \mathbb{1}$ if $\det(M) = \mp 1$. We have thus settled

Lemma 6. A matrix $M \in Gl(2, \mathbb{Z})$ with $\mathrm{tr}(M) \neq 0$ and $\det(M) = -1$ is not reversible. The only reversible orientation-reversing matrices in $Gl(2, \mathbb{Z})$ are involutions. In both cases $\mathcal{R}(M) = \mathcal{S}(M)$.

On the other hand, $M = \pm\mathbb{1}$ and any involution $M^2 = \mathbb{1}$ is trivially reversible, as $M = M^{-1}$, again with $\mathcal{R}(M) = \mathcal{S}(M)$. It will now be our task to find out the situation for the other elements. To this end, the following result from [29] will be helpful

Theorem 2. Let $M \in Gl(2, \mathbb{Z})$ be a matrix with a characteristic polynomial $P(x)$ that is irreducible over $\mathbb{Z}$. Let λ be a root of P. Then the number of conjugacy classes of $Gl(2, \mathbb{Z})$-matrices A for which $P(A) = 0$ is finite and equals the number of ideal classes in the ring $\mathbb{Z}[\lambda]$.

This is a specialization of theorem 5 in [29] where one can also find the proof. We only remark that it is rather natural to relate to this result since the investigation of the equivalence of two given matrices (unless in trivial cases) reduces more or less automatically to the question of the representability of certain numbers by a quadratic form—and hence to the class number of its discriminant. There are two class numbers frequently found in the literature, one corresponding to $Gl(2, \mathbb{Z})$ conjugacy (which is what we need here, see [4] for a table), and another one corresponding to $Sl(2, \mathbb{Z})$ conjugacy—so some care is needed when looking them up.

2.2.1. Elements of finite order and parabolic case. We know the answer already for all involutions. Let us, therefore, continue with the elements of (true) order 3,4,6. In all three cases, we have the situation of theorem 2, and in all three cases we have class number 1—which means one conjugacy class each. As the inverse elements have the same order here, the classes must contain them, and thus the elements of order 3,4,6 must be conjugate to their inverses within $Gl(2, \mathbb{Z})$, hence reversible. There are many different ways to look at this result. Here, we just use the fact and refer to table 1 for a choice of representatives. The additional reversing symmetries enlarge the cyclic groups C_4 and C_6 to the dihedral groups D_4 and D_6, respectively.

Also the case of parabolic matrices is easy to settle, as we know the answer already. The matrices T_m of equation (26) are our representatives of the conjugacy classes, and we know that $(T_m)^{-1} = T_{-m}$ from equation (28). But we know also that $T_m \sim T_{-m}$, explicitly

$$\mathrm{diag}(1, -1) \cdot T_m \cdot \mathrm{diag}(1, -1) = T_{-m}. \tag{33}$$

So, the matrices T_m are reversible, with an involution that is *not* in their symmetry group, and we thus get (by lemma 5) for any parabolic M ($M \neq \pm \mathbb{1}$):

$$\mathcal{R}(M) = \mathcal{S}(M) \times_{\mathrm{s}} C_2 \simeq (C_2 \times \mathbb{Z}) \times_{\mathrm{s}} C_2 \simeq C_2 \times D_\infty. \tag{34}$$

We now have to consider the hyperbolic matrices M with $\det(M) = 1$.

2.2.2. Hyperbolic elements. To begin with one result: it is *not* true that all hyperbolic elements M with $\det(M) = 1$ are reversible, and this is related to the class number problem again. In cases where the ring $\mathbb{Z}[\lambda]$ has class number one, we know from theorem 2 without any further work that there is also only one conjugacy class of matrices with eigenvalue λ, hence these matrices are conjugate to their inverses and thus reversible. This is so because M^{-1} leads to the ring $\mathbb{Z}[\lambda^{-1}]$ which is identical with $\mathbb{Z}[\lambda]$, since λ is a unit.

A nice general result, particularly relevant to the hyperbolic elements, is the nature of the possible reversing symmetries. If we consider $M \in Gl(2, \mathbb{Z})$ ($M \neq \pm \mathbb{1}$), the equation $GMG^{-1} = M^{-1}$ for a reversing symmetry $G \in Gl(2, \mathbb{Z})$ directly leads to

Lemma 7. Let $M, G \in Gl(2, \mathbb{Z})$, $M \neq \pm \mathbb{1}$. If G is a reversing symmetry of M, it is of finite order, namely $G^4 = \mathbb{1}$.

Proof. If $\mathrm{tr}(M) = 0$, M itself is an involution or an element of fourth order, and the statement follows, e.g., from direct calculation with the representatives of table 1. If

$\mathrm{tr}(M) \neq 0$, we must have $\det(M) = 1$ from lemma 6. If now the two diagonal entries of M are not equal, we immediately get $\mathrm{tr}(G) = 0$ from the matrix equation $GMG^{-1} = M^{-1}$ and hence the statement. If finally the two diagonal entries of M are equal, not both off-diagonal elements can vanish, and we get again $\mathrm{tr}(G) = 0$. □

Let us briefly comment on this. Clearly, the search for reversing symmetries is considerably simplified if we only have to search among involutions and anti-involutions ($G^2 = -\mathbb{1}$). From our previous classification we know that given a reversing symmetry G, all other reversing symmetries are obtained as HG with $H \neq \pm\mathbb{1}$ a symmetry of M, and either $H = \pm M^k$ for some k or at least some power of H has this form. In both cases, HG is again an involution or an anti-involution, because of lemma 7. This entire structure is particularly helpful if we switch from the matrix picture to the algebraic picture where we approach $Gl(2, \mathbb{Z})$ through generators and reformulate reversibility in terms of the word problem. We shall come back to this a little later. Let us illustrate the situation here with two examples.

Example 1. The canonical cat map (1) has the order 4 reversing symmetry $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, as well as the involutory reversing symmetry $\begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}$.

Example 2. The hyperbolic element $M = \begin{pmatrix} 4 & 9 \\ 7 & 16 \end{pmatrix}$ has no reversing symmetry in $Gl(2, \mathbb{Z})$. Note that $\mathrm{tr}(M) = 20$. This is the minimum value of $|\mathrm{tr}(M)|$ for M a hyperbolic element of $Sl(2, \mathbb{Z})$ for which irreversibility in $Gl(2, \mathbb{Z})$ occurs.

Let us also remark here that a hyperbolic element M of $Sl(2, \mathbb{Z})$ has a reversing symmetry $G \in Gl(2, \mathbb{Z})$ if and only if the corresponding element of $PSl(2, \mathbb{Z})$ has a reversing symmetry in $PGl(2, \mathbb{Z})$. This will be discussed in section 3.1, where we also give algorithms to decide *in finitely many steps* reversibility of elements of $PSl(2, \mathbb{Z})$ in $PGl(2, \mathbb{Z})$. For the moment, we just distinguish between the two possibilities, reversible and irreversible. We note, with respect to the latter possibility and example 2 above, that it follows from lemma 1 and the remarks following it that irreversibility of a hyperbolic $Gl(2, \mathbb{Z})$ element within $Gl(2, \mathbb{Z})$ finally implies irreversibility within the (much larger) group of homeomorphisms of the torus. Since the hyperbolic toral automorphisms are structurally stable, example 1 (respectively example 2) show that irreversibility (respectively reversibility) are non-generic properties among C^1 area-preserving toral diffeomorphisms, see [24] for details.

2.2.3. *Reversing symmetries summarized.*

Let us summarize our findings in the following theorem.

Theorem 3. The structure of the reversing symmetry group $\mathcal{R}(M) \subset Gl(2, \mathbb{Z})$ of a matrix $M \in Gl(2, \mathbb{Z})$ has precisely one of the following forms:

(1) $\mathcal{R}(M) = Gl(2, \mathbb{Z})$ if and only if $M = \pm\mathbb{1}$;

(2) $\mathcal{R}(M) \simeq D_2$ if and only if $\mathrm{tr}(M) = 0$ and $\det(M) = -1$ (i.e. $M^2 = \mathbb{1} \neq \pm M$);

(3) $\mathcal{R}(M) \simeq D_4$ if and only if $\mathrm{tr}(M) = 0$ and $\det(M) = 1$ (i.e. $M^4 = -M^2 = \mathbb{1}$);

(4) $\mathcal{R}(M) \simeq D_6$ if and only if $\mathrm{tr}(M) = \pm 1$ and $\det(M) = 1$ (i.e. $M^6 = \mathbb{1} \neq M^2$);

(5) $\mathcal{R}(M) \simeq D_\infty \times C_2$ if and only if M is of infinite order and possesses a reversing symmetry of order 2;

(6) $\mathcal{R}(M) \simeq C_\infty \times_s C_4$ if and only if M is of infinite order and possesses a reversing symmetry of order 4, but none of order 2; or

(7) $\mathcal{R}(M) \simeq C_\infty \times C_2$ if and only if M is of infinite order but irreversible.

Here, $D_n \simeq C_n \times_s C_2$ is the dihedral group. Let us add a comment on the structure of the reversing symmetry group in case (6) of the last theorem. It may look a bit astonishing that $\mathcal{R}$ can still be written as a semi-direct product (cf lemma 2), but the reason for it is that the fourth-order reversing symmetry G fulfils $G^2 = -\mathbb{1}$, so by absorbing the C_2-part of the symmetry group $\mathcal{S}$ we can find a subgroup of $\mathcal{R}$ isomorphic to C_4 that conjugates the C_∞-part into itself but has only the unit matrix in common with it.

2.3. Extension to (reversing) k-symmetries

Above, we have classified the possible symmetry and reversing symmetry groups. As explained in the introduction, powers of a matrix M could, in principle, have additional (reversing) symmetries, and we now want to know whether that situation really occurs. As we shall show, it is impossible within $Gl(2, \mathbb{Z})$ in most cases, the only non-trivial cases being orientation-reversing irreversible matrices with a reversible square (the square root of M of equation (1) within $Gl(2, \mathbb{Z})$ is an example of this).

2.3.1. Elliptic and parabolic cases. Clearly, an elliptic element M is of finite order, wherefore we certainly encounter the trivial case of (reversing) k-symmetries: whenever $M^k = \pm\mathbb{1}$, we get $\mathcal{S}(M^k) = \mathcal{R}(M^k) = Gl(2, \mathbb{Z})$. Apart from that, no other (reversing) k-symmetries occur for elements of finite order as can easily be checked, e.g. from table 1.

Parabolic elements in turn are conjugate to $\pm T_m$ for some $m \in \mathbb{N}$. However, since $(T_m)^k = T_{km}$ and $\mathcal{S}(T_\ell) = \mathcal{S}(T_1)$ for all $\ell \in \mathbb{N}$, we cannot have k-symmetries other than symmetries. From $\mathcal{R}(T_\ell) = \mathcal{R}(T_1)$ we see that the same holds for the reversing symmetries. We have thus established

Proposition 1. Elliptic elements M of $Gl(2, \mathbb{Z})$ do not possess any true (reversing) k-symmetries unless $M^k = \pm\mathbb{1}$ where the (reversing) symmetries add up to the entire group $Gl(2, \mathbb{Z})$. Parabolic elements do not possess any true (reversing) k-symmetries at all for $k > 1$.

2.3.2. Hyperbolic elements. From theorem 1, it is clear that hyperbolic elements cannot have k-symmetries for $k > 1$ because the generator of the C_∞-part of $\mathcal{S}(M)$ is the 'maximal' root of M in $Gl(2, \mathbb{Z})$, so $\mathcal{S}(M^k) = \mathcal{S}(M)$ for all $k \in \mathbb{N}$. Similarly, if M is reversible, no power of it can have additional reversing symmetries which follows from theorems 1 and 3: an additional reversing symmetry would also imply an additional symmetry which cannot exist.

The situation is different, however, if M has $\det(M) = -1$ (and $\mathrm{tr}(M) \neq 0$). Such an M cannot be reversible as explained earlier, but its square can.

Example 3. The matrix $M = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ is orientation-reversing with $\mathrm{tr}(M) \neq 0$ and thus irreversible. Its square, however, is the cat map of equation (1) and reversible, see example 1 above. This is a case of a true reversing 2-symmetry.

Can we have other situations? For the answer, we need the following.

Table 1. Representatives of all elliptic and parabolic conjugacy classes.

tr	det(M)	order	M	$\mathcal{S}(M)$	$\mathcal{R}(M)$
2	1	1	$\mathbb{1}$	$Gl(2,\mathbb{Z})$	$Gl(2,\mathbb{Z})$
−2	1	1	$-\mathbb{1}$	$Gl(2,\mathbb{Z})$	$Gl(2,\mathbb{Z})$
0	−1	2	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$(C_2 \times C_2)$	$(C_2 \times C_2)$
0	1	4	$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$	C_4	D_4
−1	1	3	$\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$	C_6	D_6
1	1	6	$\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$	C_6	D_6
2	1	∞	$\begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}$ $m \in \mathbb{N}$	$C_2 \times C_\infty$	$C_2 \times D_\infty$
−2	1	∞	$\begin{pmatrix} -1 & -m \\ 0 & -1 \end{pmatrix}$ $m \in \mathbb{N}$	$C_2 \times C_\infty$	$C_2 \times D_\infty$

Lemma 8. Let $A, B \in Sl(2,\mathbb{Z})$ be of infinite order. If $\mathrm{tr}(A) = \mathrm{tr}(B)$ and $A^n = B^n$ for some $n \geqslant 1$, then $A = B$.

Proof. Let $x = \mathrm{tr}(A)/2 = \mathrm{tr}(B)/2$. Infinite order in $Sl(2,\mathbb{Z})$ then means $|x| \geqslant 1$. By induction, one obtains [2] from the Cayley–Hamilton theorem that

$$A^n = U_{n-1}(x) \cdot A - U_{n-2}(x) \cdot \mathbb{1}$$
$$B^n = U_{n-1}(x) \cdot B - U_{n-2}(x) \cdot \mathbb{1}$$

where the $U_m(y)$ denote Chebyshev's polynomials of the second kind†. Then, $A^n = B^n$ if and only if $U_{n-1}(x) \cdot (A - B) = 0$. But all roots of Chebyshev's polynomials are real and strictly inside the interval $[-1, 1]$, so $U_{n-1}(x) \neq 0$ and we must have $A = B$. □

This indeed helps, as we can now show.

Lemma 9. Let $M \in Sl(2,\mathbb{Z})$ be of infinite order with $\mathrm{tr}(M) \neq 0$. If M is irreversible, the same is true of all powers M^k with $k \neq 0$. What is more, G is a reversing symmetry of M if and only if it is one of M^k.

Proof. To prove the first assertion, let us assume the contrary, i.e. M^k reversible ($k \neq 0$), but M itself not. This means there is a $G \in Gl(2,\mathbb{Z})$ with

$$(M^{-1})^k = M^{-k} = GM^kG^{-1} = (GMG^{-1})^k.$$

So, from the first and the last expression, we have two $Sl(2,\mathbb{Z})$-matrices, M^{-1} and GMG^{-1}, both of infinite order, with the same kth power and the same trace. By the previous lemma, they must be equal and M itself is reversible—a contradiction.

† They are defined by $U_{-1} \equiv 0$, $U_0 \equiv 1$, and the recursion $U_{n+1}(y) = 2yU_n(y) - U_{n-1}(y)$.

So, M is reversible if and only if M^k is, $k \neq 0$. Clearly, a reversing symmetry of M must be one of M^k, too, but also the converse holds here: if G were a reversing symmetry of M^k, but not of M, the corresponding symmetry groups would be different—another impossibility. □

To summarize:

Proposition 2. Hyperbolic elements cannot have any k-symmetries for $k > 1$. If they have $\det(M) = 1$, they cannot have reversing k-symmetries either. If, however, $\det(M) = -1$, M can possess a true reversing 2-symmetry, but none of higher order.

3. Matrices in $PGl(2,\mathbb{Z})$ and Nielsen trace maps

Let us now proceed to the second part of our paper, where we shift from the linear group $Gl(2,\mathbb{Z})$ to its projective counterpart, $PGl(2,\mathbb{Z})$. This step is made by identifying a matrix M with $-M$, i.e. we have

$$PGl(2,\mathbb{Z}) \simeq Gl(2,\mathbb{Z})/\{\pm\mathbb{1}\}. \tag{35}$$

This looks as if it makes life more complicated, but the opposite is the case. To distinguish elements of $Gl(2,\mathbb{Z})$ (i.e. matrices) from those of $PGl(2,\mathbb{Z})$ (pairs of matrices) we write round brackets for the former and square brackets for the latter. We deal firstly (and easily) with symmetries, and then move on to reversing symmetries.

3.0.1. Elements of finite order. The first observation here is that we can no longer have elements of order 4 or 6 (since such elements fulfil $M^2 = -\mathbb{1}$ or $M^3 = -\mathbb{1}$), but remain only with order 1, 2 or 3—just consider the results of the previous classification. We then notice that all symmetry groups derived above shrink to half their size due to the identification of M with $-M$. On the other hand, we now have to check whether the equation $GM = -MG$ has any solution (where then $\mathrm{tr}(GM) = 0$), which is indeed the case for order 2, but not for order 3. This means that we get $C_2 \times C_2$ again for elements of second order, but C_3 for third order.

3.0.2. Elements not of finite order. Consider first the case of parabolic matrices. Here, we have essentially to check what happens with the matrix

$$M = T_1 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \tag{36}$$

where it is easy to calculate that no new solutions appear, so that we find directly

$$\mathcal{S}(M) \simeq \mathbb{Z}. \tag{37}$$

The same situation applies to hyperbolic elements, where no new solutions exist and the centralizer of M in $PGl(2,\mathbb{Z})$ is the previous one shrunk by the C_2-part.

3.0.3. Summary of symmetries. We can summarize this situation by the following theorem previously given in [3, 30].

Theorem 4. The symmetry group $\mathcal{S}(M) \subset PGl(2,\mathbb{Z})$ for $M \in PGl(2,\mathbb{Z})$ is:
(1) $PGl(2,\mathbb{Z})$ if and only if $M = [\mathbb{1}]$;
(2) $C_2 \times C_2$ if and only if $M^2 = [\mathbb{1}] \neq M$;
(3) C_3 if and only if $M^3 = [\mathbb{1}] \neq M$;
(4) C_∞ in all remaining cases, i.e. whenever M is not of finite order.

Let us add a comment here. It is well known that every Abelian subgroup of the modular group $PSl(2,\mathbb{Z})$ is cyclic, cf [29], which has a nice connection with part (2) of theorem 4. There, the symmetry group is $C_2 \times C_2$ which is Abelian but *not* cyclic. It turns out that its intersection with $PSl(2,\mathbb{Z})$ is C_2 and hence cyclic as it must be. This way we see

Corollary 2. The possible Abelian subgroups of $PSl(2,\mathbb{Z})$ are C_2, C_3 and $\mathbb{Z} \simeq C_\infty$.

This matches well with the fact that $PSl(2,\mathbb{Z})$ is isomorphic with the free product of C_2 and C_3 [14, 21]

$$PSl(2,\mathbb{Z}) = C_2 * C_3 \tag{38}$$

which will be helpful in what follows. Let us pause to explore this a little. Equation (38) means that we can write $C_2 * C_3$ as a quotient [21] of the free group F_2 of two generators, v, q say, after the relations $R = \{v^2 = e, q^3 = e\}$ where e is the neutral element (i.e. empty word) in F_2,

$$C_2 * C_3 \simeq F_2/R. \tag{39}$$

This implies immediately that we have precisely one conjugacy class of involutions in $PSl(2,\mathbb{Z})$, represented by v, and precisely two classes of elements of order 3, namely those represented by q and $q^2 = q^{-1}$ (they become conjugate only in $PGl(2,\mathbb{Z})$). This structure will prove useful in a moment.

3.1. Reversing symmetries

First of all, the restriction encountered previously in the $Gl(2,\mathbb{Z})$ case does not apply here, as we have to calculate always mod $\pm\mathbb{1}$. This means in particular that many orientation-reversing matrices actually are reversible [3, 25, 26]. Let us state the result as follows.

Theorem 5. The reversing symmetry group $\mathcal{R}(M) \subset PGl(2,\mathbb{Z})$ of $M \in PGl(2,\mathbb{Z})$ is:
(1) C_∞ if and only if M is not reversible;
(2) $PGl(2,\mathbb{Z})$ if and only if $M = [\mathbb{1}]$;
(3) $D_2 \simeq C_2 \times C_2$ if and only if $M^2 = [\mathbb{1}] \neq M$;
(4) D_3 if and only if $M^3 = [\mathbb{1}] \neq M$; or
(5) D_∞, if M is reversible but not of finite order.

At this point, we know the complete answer for elliptic and parabolic elements (which all are reversible), but still have to decide between possibilities (1) and (5) of theorem 5. This requires a bit more algebra which we will now explain.

3.1.1. Reversibility and the word problem in $PSl(2,\mathbb{Z})$. Let us describe how to decide whether an infinite-order element $M \in PGl(2,\mathbb{Z})$ is reversible or not. We do this mainly by converting the reversibility issue into a conjugacy problem within the group $PSl(2,\mathbb{Z})$ of (38). This is advantageous because conjugacy of any two elements in a free product is decidable via a finite algorithm (for a full discussion, see [14, 21]; also cf [23] for a summary and another application of this property). Practically speaking, (38) means that any element M of $PSl(2,\mathbb{Z})$ can be written uniquely as a finite word in v, q and q^{-1}, namely

$$M \in PSl(2,\mathbb{Z}) \to M = v^{\alpha} q^{\pm 1} v q^{\pm 1} \dots v q^{\pm 1} v^{\beta} \tag{40}$$

where $\alpha, \beta \in \{0, 1\}$, and the so-called *reduced* representation (40) is unique. The term *reduced* refers to the fact that the relations $R = \{v^2 = q^3 = e\}$ are used to ensure that each consecutive element of the word alternatingly belongs to the subgroup $C_2 = \langle\langle v\rangle\rangle$ or to $C_3 = \langle\langle q\rangle\rangle$, and is different from the unit element. For an explicit algorithm to find this word, see the appendix in [14].

To make things explicit, we use the matrix representatives

$$v = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \qquad \text{and} \qquad q = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}. \tag{41}$$

As an example, we have, for $\ell \in \mathbb{Z}$,

$$\begin{bmatrix} 1 & \ell \\ \ell & 1+\ell^2 \end{bmatrix} = (vq^{-1})^{\ell}(vq)^{\ell}. \tag{42}$$

Note that $\ell = 1$ gives the $PSl(2,\mathbb{Z})$ element corresponding to the cat map (1).

Two elements of $PSl(2,\mathbb{Z})$ are conjugate if and only if they have the same *cyclically reduced* word. The latter is found by wrapping the word (40) on the circle with the first and last letters adjacent, and then reducing if necessary to ensure adjacent letters are from different subgroups. The process of finding the cyclically reduced word, or comparing two such words up to cyclic permutation, in general involves moving parts of the original word (40) from its beginning to its end or *vice versa*. This establishes the conjugating element linking the two words. For example, qvq is conjugate to vq^{-1} because they share the same cyclically reduced word. As a more pertinent example, observe

$$\begin{bmatrix} 1 & \ell \\ \ell & 1+\ell^2 \end{bmatrix}^{-1} = (q^{-1}v)^{\ell}(qv)^{\ell} = q^{-1}(vq^{-1})^{\ell-1}(vq)^{\ell}v = v(vq^{-1})^{\ell}(vq)^{\ell}v. \tag{43}$$

Comparing (43) and (42), we find the words to be cyclic permutations of one another, hence conjugate (by v). This shows that (42) is reversible in $PSl(2,\mathbb{Z})$ with v as involutory reversing symmetry.

It is not hard to see that the set of cyclically reduced words consists of v, q, q^{-1}, together with certain mixed words. The latter can be taken, without loss of generality, to be $(vq)^j$ or $(vq^{-1})^j$, $j \in \mathbb{N}$ (where $\mathbb{N} = \{1, 2, 3, \dots\}$), or words containing at least one copy of both vq and vq^{-1}, i.e. of the form

$$(vq^{-1})^{j_1}(vq)^{k_1} \dots (vq^{-1})^{j_n}(vq)^{k_n} \qquad n \geqslant 1,\ j_i, k_i \in \mathbb{N}. \tag{44}$$

Noting that

$$vq = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \qquad \text{and} \qquad vq^{-1} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \tag{45}$$

so that any product of them has trace exceeding 2, we see that any $M \in PSl(2,\mathbb{Z})$ which is hyperbolic has a cyclically reduced word of the form (44) (and hence is conjugate to such a word). We can encode this cyclically reduced word for hyperbolic M by the integer sequence of powers of the vq and vq^{-1} blocks

$$\{M\} := \{-j_1, k_1, \dots, -j_n, k_n\} \qquad n \geqslant 1,\ j_i, k_i \in \mathbb{N}. \tag{46}$$

The sequence $\{M\}$ is to be understood with periodic boundary conditions.

It follows from the other cyclically reduced words given above that we have the following situation in $PSl(2,\mathbb{Z})$: (i) there are infinitely many conjugacy classes of parabolic matrices, with representatives $(vq)^m$ and $(vq^{-1})^m$, $m \in \mathbb{N}$; (ii) there are two conjugacy classes of order 3, with representatives q and q^{-1}; and (iii) one conjugacy class of involutions, represented by v. It is easy to see the reversibility within $PGl(2, \mathbb{Z})$ of the finite-order and parabolic elements from their representatives. The involution v is reversible with itself as the reversing symmetry. The parabolic matrix vq has inverse $q^{-1}v$. As these two words have different cyclic reductions, they cannot be conjugate in $PSl(2, \mathbb{Z})$. However, we have

$$vq = s(q^{-1}v)s \tag{47}$$

where the involution s is given by

$$s := \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}. \tag{48}$$

Thus vq is reversible in $PGl(2, \mathbb{Z})$, while irreversible in $PSl(2, \mathbb{Z})$. A similar statement is true of vq^{-1}, and also of the powers of these elements. This follows because $vq^{-1} = sv(vq)sv$ from sandwiching (47) by sv and noting that s and v commute. That is, vq and vq^{-1} are not conjugate in $PSl(2, \mathbb{Z})$, while they are in $PGl(2, \mathbb{Z})$ (and similarly for the powers). Finally, we also know from above that, in contrast to the case of $PSl(2, \mathbb{Z})$, there is only one conjugacy class of third-order elements in $PGl(2, \mathbb{Z})$. Whence q and q^{-1} are conjugate (and reversible) in $PGl(2, \mathbb{Z})$, as distinct from $PSl(2, \mathbb{Z})$. The reversing symmetry is again sv.

It remains to consider the reversibility or irreversibility of a hyperbolic element $M \in PSl(2, \mathbb{Z})$. In what follows, we show that this can be decided via symmetry properties of the sequence $\{M\}$ of (46). We know already from lemma 7 that possible reversing symmetries are involutions in $PGl(2, \mathbb{Z})$. We consider firstly the case that the involution is orientation-preserving (and so also in $PSl(2, \mathbb{Z})$), and then the case that it is orientation-reversing (and thus in $PGl(2, \mathbb{Z}) \backslash PSl(2, \mathbb{Z})$).

Proposition 3. Let $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ be a hyperbolic element of $PSl(2, \mathbb{Z})$. Then M is reversible in $PSl(2, \mathbb{Z})$, i.e. $GMG^{-1} = M^{-1}$ with $G \in PSl(2, \mathbb{Z})$, if and only if:

(1) G is conjugate to v of (41) in $PSl(2, \mathbb{Z})$;
(2) $b = c$ in M, or M is conjugate to such a matrix;
(3) the sequence $\{M\}$ of (46) is invariant under reversal followed by a change of sign.

Proof. (1) follows from the fact that all involutions in $PSl(2, \mathbb{Z})$ are conjugate to v. For (2), a straightforward calculation shows that $vMv = M^{-1}$ implies $b = c$. If $G = PvP^{-1}$ with $P \in PSl(2, \mathbb{Z})$, then $M' = P^{-1}MP$ has $b' = c'$. For (3), it follows that since M is conjugate to a word of the form (44), then M^{-1} is conjugate to the inverse of (44). The inverse of (44) is $(q^{-1}v)^{k_n}(qv)^{j_n} \ldots (q^{-1}v)^{k_1}(qv)^{j_1}$, which is conjugate via v to $(vq^{-1})^{k_n}(vq)^{j_n} \ldots (vq^{-1})^{k_1}(vq)^{j_1}$. This shows that $\{M^{-1}\} = \{-k_n, j_n, \ldots, -k_1, j_1\}$. From the standard theory, M^{-1} and M are conjugate if and only if $\{M^{-1}\} = \{M\}$. □

We next consider the case of an involutory reversing symmmetry G with $\det(G) = -1$, i.e. $G \in PGl(2, \mathbb{Z}) \backslash PSl(2, \mathbb{Z})$. We can then write $G = sG'$, with s the orientation-reversing involution of (48) and $G' \in PSl(2, \mathbb{Z})$. We then have

$$GMG^{-1} = M^{-1} \Leftrightarrow sG'MG'^{-1}s = M^{-1} \Leftrightarrow G'MG'^{-1} = sM^{-1}s. \tag{49}$$

Since $sM^{-1}s \in PSl(2, \mathbb{Z})$, this shows that reversibility with a reversing symmetry of negative determinant can still be related to a conjugacy problem in $PSl(2, \mathbb{Z})$. We find

Proposition 4. Let $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ be a hyperbolic element of $PSl(2,\mathbb{Z})$. Then M has a reversing symmetry $G \in (PGl(2,\mathbb{Z})\backslash PSl(2,\mathbb{Z}))$, i.e. $GMG^{-1} = M^{-1}$ with $G = sG'$ and $G' \in PSl(2,\mathbb{Z})$, if and only if:

(1) G is conjugate to $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$, or $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$; in $PGl(2,\mathbb{Z})$;

(2) $a = d$, or $b = -c$ (e.g. $b|(d-a)$ or $c|(d-a)$); in M, or M is conjugate to such a matrix;

(3) the sequence $\{M\}$ of (46) is invariant under reversal.

Proof. For (1) and (2), we refer to lemma 4 and to [12, 25]. To show (3), we use the fact that M is reversible with reversing symmetry of negative determinant if and only if its cyclically reduced word is reversible with such a reversing symmetry. Similar to (49), the latter is true if and only if the word of the form (44) to which M is conjugate, denoted $w(M)$, is conjugate in $PSl(2,\mathbb{Z})$ to $sw(M)^{-1}s$. Using (44), and (47) to move one s through $w(M)^{-1}$ and cancel it with the other, one deduces that $\{sw(M)^{-1}s\} = \{k_n, -j_n, \ldots, k_1, -j_1\}$. This sequence equals that of $\{w(M)\} = \{M\}$ of (46) if and only if the latter is invariant under reversal. □

Let us now give some examples of how the previous propositions can be used to decide reversibility of hyperbolic elements of $PSl(2,\mathbb{Z})$ in $PGl(2,\mathbb{Z})$. This also decides reversibility of corresponding hyperbolic elements of $Sl(2,\mathbb{Z})$ in $Gl(2,\mathbb{Z})$, since the following is easily proved.

Proposition 5. Let $M \in Sl(2,\mathbb{Z})$ with $\mathrm{tr}(M) \neq 0$. Then M has a reversing symmetry $G \in Gl(2,\mathbb{Z})$ if and only if $[G][M][G]^{-1} = [M]^{-1}$, where $[M]$, respectively $[G]$, stand for the corresponding elements of $PSl(2,\mathbb{Z})$, respectively $PGl(2,\mathbb{Z})$.

There is only one thing to note when considering reversibility and working between corresponding hyperbolic elements of $Sl(2,\mathbb{Z})$ and $PSl(2,\mathbb{Z})$. This is that the reversibility described in proposition 3 via an orientation-preserving involution in $PSl(2,\mathbb{Z})$, becomes reversibility via an order 4 element in $Sl(2,\mathbb{Z})$.

Example 4. If we take $n = 1$ in (46) and the normal form (44), we observe that $(vq^{-1})^{j_1}(vq)^{k_1}$ always has an orientation-reversing involutory reversing symmetry because $\{-j_1, k_1\}$ is equivalent to $\{k_1, -j_1\}$ (cf proposition 4). On the other hand, $(vq^{-1})^{j_1}(vq)^{k_1}$ only has an orientation-preserving involutory reversing symmetry if $j_1 = k_1$, because this is needed for $\{-j_1, k_1\}$ to equal $\{-k_1, j_1\}$ (cf proposition 3). The element (42) is precisely this example (cf also (43)).

Example 5. Once we take $n = 2$ in (46) and consider sequences $\{-j_1, k_1, -j_2, k_2\}$, we can avoid *both* possibilities for reversibility in $PGl(2,\mathbb{Z})$ as described in propositions 3 and 4. This becomes increasingly easy with higher n (e.g. a necessary condition for proposition 4 is that the subsequences of j_i's and k_i's are each symmetric). For $n = 2$, we have

$$(vq^{-1})^{j_1}(vq)^{k_1}(vq^{-1})^{j_2}(vq)^{k_2} = \begin{bmatrix} 1 + k_1 j_2 & k_1 + k_2(1 + k_1 j_2) \\ j_2 + j_1(1 + k_1 j_2) & 1 + j_1 k_1 + j_2 k_2 + j_1 k_2 (1 + k_1 j_2) \end{bmatrix}.$$

The sequence $\{-j_1, k_1, -j_2, k_2\} = \{-1, 1, -3, 2\}$ corresponds to a hyperbolic element of $PSl(2,\mathbb{Z})$ which is irreversible in $PGl(2,\mathbb{Z})$. This provides the corresponding $Sl(2,\mathbb{Z})$ element in example 2 of section 2.2.

For hyperbolic elements of $PSl(2,\mathbb{Z})$ with small trace, the conditions (2) of propositions 3 and 4 are particularly useful. Firstly, the conjugacy representatives (44), together with (45), show that every hyperbolic element of $PSl(2,\mathbb{Z})$ is conjugate to one with positive integer entries (for a geometric, rather than algebraic, proof of this result, cf [20]). Secondly, conjugacy by $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ can always be used to interchange the diagonal elements. Consequently, it is not hard to write out the matrices $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$, with $a, b, c, d \in \mathbb{N}$ and $a \geqslant d$, for small values of $a+d$ and verify they satisfy the above-mentioned conditions (or obvious transformed versions of them). Doing so, we find:

Example 6. All hyperbolic elements of $PSl(2,\mathbb{Z})$ with $3 \leqslant \mathrm{tr}(M) \leqslant 19$ are reversible.

We now complete the analysis of reversibility in $PGl(2,\mathbb{Z})$ by considering the reversibility of an element $M \in PGl(2,\mathbb{Z})$ with $\det(M) = -1$. If $\mathrm{tr}(M) = 0$, we know M is an involution and is reversible. If $\mathrm{tr}(M) > 0$, then M is hyperbolic and so is $M^2 \in PSl(2,\mathbb{Z})$. If M is reversible, we again know that its reversing symmetries are involutions. Hence, from standard results [27], M can be written as the product of two involutions. So, $\det(M) = -1$ implies that one involution has negative and the other positive determinant. Since a power of a reversible mapping certainly possesses any reversing symmetry of the mapping itself, it follows that M^2 has an involutory reversing symmetry with $\det = -1$ and another one with $\det = 1$, so satisfies the conditions of both proposition 3 and proposition 4. Conversely, we can show for hyperbolic $M \in PGl(2,\mathbb{Z})$ with $\det(M) = -1$, that when M^2 satisfies one of proposition 3 or proposition 4, it must satisfy both and M is reversible. This uses:

Lemma 10. Let A, $B \in PGl(2,\mathbb{Z})$ with $\det(A) = \det(B) = -1$ and $\mathrm{tr}(A), \mathrm{tr}(B) \neq 0$. If $A^2 = B^2$ in $PSl(2,\mathbb{Z})$, then $A = B$.

Proof. From the Cayley–Hamilton theorem, we have

$$A^2 - \mathrm{tr}(A) \cdot A - \mathbb{1} = B^2 - \mathrm{tr}(B) \cdot B - \mathbb{1} = 0.$$

From the assumptions, this implies $A = \gamma B$ where $\gamma = \mathrm{tr}(B)/\mathrm{tr}(A)$. However, taking traces of both sides of $A = \gamma B$ shows $\gamma^2 = 1$, whence $A = B$ as we can ignore a possible minus sign. □

It follows from lemma 10 that $M^{-2} = GM^2G^{-1} = (GMG^{-1})^2$ implies $M^{-1} = GMG^{-1}$ for hyperbolic $M \in PGl(2,\mathbb{Z})$ with $\det(M) = -1$. In summary, we have shown

Proposition 6. Let $M \in PGl(2,\mathbb{Z})$ with $\det(M) = -1$ and $\mathrm{tr}(M) > 0$. Then M is reversible in $PGl(2,\mathbb{Z})$ if and only if the hyperbolic element $M^2 \in PSl(2,\mathbb{Z})$ is reversible in both $PSl(2,\mathbb{Z})$ and $PGl(2,\mathbb{Z})\backslash PSl(2,\mathbb{Z})$. M and M^2 share the same reversing symmetries. M is reversible if and only if the sequence $\{M^2\}$ is invariant under *both* a change of sign and reversal.

The canonical illustration of proposition 6 is the orientation-reversing hyperbolic element $\begin{bmatrix} 0 & 1 \\ 1 & \ell \end{bmatrix}$. Its square is the $PSl(2,\mathbb{Z})$ element (42). Proposition 6 also shows that we cannot have true reversing 2-symmetries in $PGl(2,\mathbb{Z})$ (cf proposition 2).

3.1.2. Alternative approach via quadratic forms. We finish this section with a short description of a number-theoretic way of deciding reversibility in $PGl(2, \mathbb{Z})$. Though this does not give any essential new insight, it has the advantage that it allows for a generalization to matrices of larger dimension.

It was shown in proposition 17 of [25] via direct calculation that $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in PGl(2, \mathbb{Z})$ has a reversing symmetry in $PGl(2, \mathbb{Z})$ if and only if there exists $\alpha, \beta, \gamma \in \mathbb{Z}$ satisfying

$$(a - d)\alpha + c\beta + b\gamma = 0 \tag{50}$$

together with

$$\alpha^2 + \beta\gamma = \pm 1. \tag{51}$$

The corresponding reversing symmetry G reads $\begin{bmatrix} \alpha & \beta \\ \gamma & -\alpha \end{bmatrix}$, with (51) being the determinant condition.

Now the linear diophantine equation (50) always has an infinity of solutions for $(\alpha, \beta, \gamma) \in \mathbb{Z}^3$, which can be found using standard number-theoretic methods. To describe this, let us assume $a \neq d$ ($a = d$ is trivial) and $c \neq 0$ (this is no restriction as $b = c = 0$ is again trivial, and $c = 0$ but $b \neq 0$ would result in an analogous chain of arguments). Then, we define $r = \gcd(a - d, b, c)$, and $s = \gcd(a - d, c)$. Clearly, $r \mid s$ and we write $s = \mu r$. Then, $(a - d)/r$, b/r and c/r as well as $(a - d)/s$ and c/s are again integers and the equation

$$\frac{a - d}{s}\alpha + \frac{c}{s}\beta = 1 \tag{52}$$

has integer solutions because $\gcd((a - d)/s, c/s) = 1$. Let (α_0, β_0) be one such solution (which then also fulfils $\gcd(\alpha_0, \beta_0) = 1$). The general solution of (50) can then be written as follows:

$$\alpha = \frac{b}{r}\ell\alpha_0 - \frac{c}{s}k \qquad \beta = \frac{b}{r}\ell\beta_0 + \frac{a - d}{s}k \qquad \gamma = -\mu\ell \tag{53}$$

where ℓ and k are arbitrary integers.

It is now condition (51) that places a possible restriction on ℓ and k. Substituting (53) in (51) yields

$$P\ell^2 + Qk\ell + Rk^2 = \pm 1 \tag{54}$$

where

$$P = \alpha_0^2\frac{b^2}{r^2} - \mu\beta_0\frac{b}{r} \qquad Q = -\left(\frac{a - d}{r} + 2\alpha_0\frac{b}{r}\frac{c}{s}\right) \qquad R = \frac{c^2}{s^2}. \tag{55}$$

The left-hand side of (54) is an integer binary quadratic form in ℓ and k. In the language of binary quadratic forms, (54) asks whether ± 1 can be *represented* by this form, i.e. whether integers ℓ and k satisfying (54) can be found. This is a solvable problem, using techniques dating back to Gauß (cf [10] for an overview). Thus, in this description, reversibility is equivalent to a representation problem by binary quadratic forms.

To decide the problem for a given M, one uses the notion of *equivalent* binary quadratic forms. Two forms are said to be equivalent if one is converted into the other via a unimodular transformation. A number N is represented by a form $Ax^2 + Bxy + Cy^2$ if and only if the given form is equivalent to one with leading coefficient N, i.e. $NX^2 + B'XY + C'Y^2$ with $(X, Y) \in \mathbb{Z}^2$ and $(x, y) \in \mathbb{Z}^2$ linked by an element of $Gl(2, \mathbb{Z})$ (note that we are *not* using the restricted form of equivalence with only orientation-preserving matrices here). An algorithm for deciding equivalence of forms was derived by Gauß.

In our case (54)–(55), having solved the problem for elliptic and parabolic matrices by other means, we are dealing with *indefinite* forms because the *discriminant*

$$D = Q^2 - 4PR = (\mathrm{tr}(M)^2 - 4\det(M))/r^2 \tag{56}$$

which follows by inserting (55) and observing the relations $s = \mu r$ and (52), is clearly positive for hyperbolic M. An indefinite form can always be transformed (via an algorithmic use of a *finite number* of unimodular transformations) to one of the so-called *reduced* forms [10]. There are also only finitely many of those, which divide into a number h of *cycles* of equivalent reduced forms. Finally, two indefinite forms are equivalent if and only if they reduce into the *same* cycle. In this respect, h is the *class number* for equivalence classes of forms and is a function of the discriminant D. Of course, when $h(D) = 1$, all forms with that particular discriminant are equivalent. A conjecture due to Gauß (and still unproved, as far as we are aware) is that $h(D) = 1$ occurs for infinitely many values of the discriminant D. In our context, from (56), this would imply infinitely many values of $\mathrm{tr}(M)$ for which all matrices with that trace are reversible—a rather unexpected outcome.

4. Extension to affine transformations

So far, we have mainly discussed linear transformations, but it is an interesting question (e.g. cf lemma 1 for cat maps) what happens if one extends the search for (reversing) symmetries to the group of *affine* transformations.

Let us start with the plane, where affine transformations can be written as (t, M) with $t \in \mathbb{R}^2$ and $M \in Gl(2, \mathbb{R})$. The action on a point of the plane is $(t, M)x := Mx + t$ and the product reads

$$(t, M) \cdot (t', M') = (t + Mt', MM'). \tag{57}$$

From this equation it is immediate that the affine transformations of the plane form a group which is a semi-direct product

$$\mathcal{G}_a = \mathbb{R}^2 \times_s Gl(2, \mathbb{R}) \tag{58}$$

with neutral element $(0, \mathbb{1})$ and $(t, M)^{-1} = (-M^{-1}t, M^{-1})$. $\mathbb{R}^2$ is a normal subgroup of $\mathcal{G}_a$ since

$$(t, M) \cdot (s, \mathbb{1}) \cdot (t, M)^{-1} = (Ms, \mathbb{1}) \tag{59}$$

and $s' = Ms$ is again a valid translation.

4.1. Toral automorphisms

Now, we are not primarily interested in the plane, but in the torus $\mathbb{T}$ defined through

$$\mathbb{T} := \{(x, y)^t | 0 \leqslant x, y < 1\}. \tag{60}$$

This is still an Abelian group if we define the addition of vectors now mod. 1 componentwise, and the affine transformations of $\mathbb{T}$ form the group

$$\mathcal{G}_a^{\mathbb{T}} = \mathbb{T} \times_s Gl(2, \mathbb{Z}) \tag{61}$$

which is still a semi-direct product.

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

Lemma 11. The affine transformation (t, G) is a (reversing) symmetry of the toral automorphism $(0, M)$ if and only if G is a (reversing) symmetry of M in $Gl(2,\mathbb{Z})$ and $Mt = t$ (mod 1).

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

From this it is clear that we need not consider all translations in $\mathbb{T}$ but only those with *rational* components, which we denote as

$$\Lambda_\infty := \{(x, y)^t \in \mathbb{T} | x, y \in \mathbb{Q}\}. \tag{62}$$

For many purposes, we can also consider discrete sublattices Λ_q of Λ_∞ on $\mathbb{T}$ ($q \in \mathbb{N}$):

$$\Lambda_q := \left\{ \left(\frac{m}{q}, \frac{n}{q}\right)^t | 0 \leqslant m, n < q \right\}. \tag{63}$$

All these Λ_q (including $q = \infty$) form Abelian groups with respect to addition mod 1,

$$\Lambda_q \simeq C_q \times C_q \tag{64}$$

and all of them give rise to affine subgroups of $\mathcal{G}_a^{\mathbb{T}}$ that are semi-direct products

$$\mathcal{G}_q = \Lambda_q \times_{\mathrm{s}} Gl(2,\mathbb{Z}) \tag{65}$$

as can easily be checked from equation (59). Furthermore, we have $\mathcal{G}_1 \simeq Gl(2,\mathbb{Z})$ and $\Lambda_\infty = \cup_{q \geqslant 1} \Lambda_q$.

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

$$a_k = \sum_{\ell | k} \ell \cdot p_\ell \tag{66}$$

where p_ℓ counts the true orbits of length ℓ, and the Möbius inversion formula [13] gives

$$p_k = \frac{1}{k} \sum_{\ell | k} \mu(k/\ell) \cdot a_\ell \tag{67}$$

with the Möbius function $\mu(m)$ [13]. If p_k is positive for some k, we get a k-symmetry (and, hence, eventually a reversing k-symmetry) of M. This can easily be calculated explicitly, where a very natural tool is provided by the so-called dynamical or Artin–Mazur ζ-functions [8]. Here, the a_k's can be extracted from the series expansion of the logarithm of the ζ-function, while the p_k's appear as exponents of the factors of the Euler product expansion of the ζ-function itself.

On the other hand, suppose we restrict our search for (reversing) k-symmetries to a particular $\mathcal{G}_q$ of (65) arising from the lattice Λ_q of (63) for definite q. Then the existence and distribution (in k) of (reversing) k-symmetries in this set is equivalent to the problem of the existence and distribution of periodic orbits induced by M on Λ_q. Quite a bit of work has been done on the latter problem for hyperbolic M when q is prime [22, 11].

4.2. The case of $\boldsymbol{PGl}(2,\mathbb{Z})$.

It is an obvious question to ask what happens in the $PGl(2,\mathbb{Z})$ case which could be considered as quotienting with respect to $\pm\mathbb{1}$, i.e. $PGl(2,\mathbb{Z}) \simeq Gl(2,\mathbb{Z})/\{\pm\mathbb{1}\}$. This is then the group of linear transformations of $\mathbb{T}/\sim$ where the equivalence relation

$$x \sim y \qquad :\Leftrightarrow \qquad y = -x \tag{68}$$

preserves the linear structure. This allows the determination of the affine transformations of $\mathbb{T}/\sim$ from those of $\mathbb{T}$. We have to determine the normalizer of the quotienting group $\{\pm\mathbb{1}\} \simeq C_2$ in $\mathcal{G}_a^{\mathbb{T}}$ from which we obtain $\mathcal{G}_a^{\mathbb{T}/\sim}$ as a factor group

$$\mathcal{G}_a^{\mathbb{T}/\sim} \simeq \mathrm{norm}_{\mathcal{G}_a^{\mathbb{T}}}(\{\pm\mathbb{1}\})/(\{\pm\mathbb{1}\}). \tag{69}$$

Since $(0,\mathbb{1})$ is the neutral element in $\mathcal{G}_a^{\mathbb{T}}$, we actually have to determine all affine transformations (t, M) of the torus that commute with $(0,-\mathbb{1})$ which gives the condition

$$t = -t \qquad (\mathrm{mod}\ 1). \tag{70}$$

This equation has precisely four solutions on $\mathbb{T}$, namely the elements of Λ_2 (the so-called 2-division points). We can now calculate the factor group of equation (69) and get

$$\mathcal{G}_a^{\mathbb{T}/\sim} \simeq \Lambda_2 \times_{\mathrm{s}} PGl(2,\mathbb{Z}) \tag{71}$$

which is, since $\Lambda_2 \simeq C_2 \times C_2$, isomorphic with the group $\mathcal{A}$ of polynomial mappings that preserve the Fricke–Vogt invariant (2)! In view of the relation of $PGl(2,\mathbb{Z})$ to Nielsen trace maps and their affine extensions to other polynomial mappings which preserve the Fricke–Vogt invariant, compare [25, 26], and in view of lemma 1, this provides an independent derivation of the structure of the group $\mathcal{A}$ to that of [31].

5. Concluding remarks

In this paper, we have discussed the symmetries and reversing symmetries of 2D unimodular matrices. By means of algebraic and number theoretic techniques, it was possible to classify the (reversing) symmetry groups of such matrices. We also described how to calculate the (reversing) symmetries of a given matrix explicitly, and how to deal with the extension to affine symmetries and to (reversing) k-symmetries. The integral 2×2 matrices thus provide a nice example where the structure of symmetry and reversing symmetry can be exploited completely, without approximative methods.

It is clear that this is somewhat exceptional, and mainly the consequence of the linear structure—even if the answer in detail required various discrete methods. To some extent, the analysis can be generalized to $Gl(n,\mathbb{Z})$, but with increasing complication from matrices with characteristic polynomials that are reducible over $\mathbb{Z}$. Still rather interesting will be the case of $Gl(3,\mathbb{Z})$ due to its relation to lattice symmetries in three dimensions and the appearance of more complicated symmetry groups. We hope to report on this in more detail soon.

Acknowledgments

It is a pleasure to thank G Cairns, E Ghys and J S W Lamb for various useful discussions. JAGR gratefully acknowledges partial support from the Australian Research Council through its Fellowship Scheme.

References

[1] Arnold V I and Avez A 1968 *Ergodic Problems of Classical Mechanics* (New York: Benjamin) (reprint: 1989 Redwood City: Addison Wesley)
[2] Baake M, Grimm U and Joseph D 1993 Trace maps, invariants, and some of their applications *Int. J. Mod. Phys.* B **7** 1527–50
[3] Baake M and Roberts J A G 1993 Symmetries and reversing symmetries of trace maps *Proc. 3rd Int. Wigner Symp. (Oxford 1993)* (Singapore: World Scientific) at press
[4] Borevich Z I and Shafarevich I R 1966 *Number Theory* (New York: Academic)
[5] Cairns G and Jessup B 1996 Linear dynamics on quotients of tori *La Trobe University Preprint*
[6] Cassels J S W 1965 *An Introduction to Diophantine Approximation* (Cambridge: Cambridge University Press)
[7] Cohn H 1980 *Advanced Number Theory* 2nd edn (New York: Dover)
[8] Degli Esposti M and Isola S 1995 Distribution of closed orbits for linear automorphisms of tori *Nonlinearity* **8** 827–42
[9] Devaney R V 1989 *An Introduction to Chaotic Dynamical Systems* 2nd edn (Redwood City: Addison Wesley)
[10] Flath D E 1989 *Introduction to Number Theory* (New York: Wiley)
[11] Gaspari G 1994 The Arnold cat map on prime lattices *Physica* **73D** 352–72
[12] Ghys E and Sergiescu V 1980 Stabilite et conjugaison differentiable pour certains feuilletages *Topology* **19** 179–97
[13] Hardy G H and Wright E M 1979 *An Introduction to the Theory of Numbers* 5th edn (Oxford: Clarendon)
[14] Kurosh A G 1960 *The Theory of Groups* vol 2 2nd edn (New York: Chelsea)
[15] Lang S 1993 *Algebra* 3rd edn (Reading, MA: Addison Wesley)
[16] Lamb J S W 1992 Reversing symmetries in dynamical systems *J. Phys. A: Math. Gen.* **25** 925–37
[17] Lamb J S W 1994 *Reversing Symmetries in Dynamical Systems PhD thesis* University of Amsterdam
[18] Lamb J S W and Quispel G R W 1994 Reversing k-symmetries in dynamical systems *Physica* **73D** 277–304
[19] Lamb J S W and Quispel G R W 1995 Cyclic reversing k-symmetry groups *Nonlinearity* **8** 1005–26
[20] Llibre J and McKay R S 1992 Pseudo-Anosov homeomorphisms on a sphere with four punctures have all periods *Math. Proc. Cambridge Phil. Soc.* **112** 539–49
[21] Magnus W, Karrass A and Solitar D 1976 *Combinatorial Group Theory* 2nd edn (New York: Dover)
[22] Percival I and Vivaldi F 1987 Arithmetical properties of strongly chaotic motions *Physica* **25D** 105–30
[23] Roberts J A G 1996 Escaping orbits in trace maps *Physica* **228A** 295–325
[24] Roberts J A G 1997 Some characterisations of low-dimensional dynamical systems with time-reversal symmetry *Control and Chaos* ed K Judd (New York: Birkhäuser) to appear
[25] Roberts J A G and Baake M 1994 Trace maps as 3D reversible dynamical systems with an invariant *J. Stat. Phys.* **74** 829–88
[26] Roberts J A G and Baake M 1994 The dynamics of trace maps *Hamiltonian Mechanics: Integrability and Chaotic Behaviour (NATO ASI Series B: Physics)* ed J Seimenis (New York: Plenum) p 275–85
[27] Roberts J A G and Quispel G R W 1992 Chaos and time-reversal symmetry. Order and chaos in reversible dynamical systems *Phys. Rep.* **216** 63–177
[28] Schwarzenberger R L E 1980 *N-dimensional crystallography* (London: Pitman)
[29] Taussky O 1988 Introduction into connections between algebraic number theory and integral matrices *A Classical Invitation to Algebraic Numbers and Class Fields* 2nd edn, ed H Cohn (New York: Springer) Appendix 2, pp 305–21
[30] Wagner H, Baake M and Roberts J A G 1995 Trace maps and dynamical systems *Proc. 5th Int. Conf. on Quasicrystals* ed C Janot and R Mosseri (Singapore: World Scientific) pp 104–7
[31] Wen Z-X and Wen Z-Y 1992 Algebraic properties of trace mappings associated with sustitutive sequences *Modern Mathem. (China)* to appear
Peyrière J, Wen Z-X and Wen Z-Y 1993 Polynômes Associés aux Endomorphisms de Groupes Libres *L'Enseignement Mathem.* **39** 153–75