THE STRUCTURE OF REVERSING SYMMETRY GROUPS

MICHAEL BAAKE AND JOHN A.G. ROBERTS

We present some of the group theoretic properties of reversing symmetry groups, and classify their structure in simple cases that occur frequently in several well-known groups of dynamical systems.

1. INTRODUCTION

Let X be some space, with automorphism group $G := \mathrm{Aut}(X)$. An element $L \in G$ is said to have a *symmetry* if there exists an automorphism $S \in G$ that satisfies $L \circ S = S \circ L$ or, equivalently, $S \circ L \circ S^{-1} = L$, and a *reversing symmetry*, or *reversor*, if there exists an automorphism $R \in G$ so that $R \circ L \circ R^{-1} = L^{-1}$. The set of symmetries is non-empty (it certainly contains all powers of L) and forms a group, the *symmetry group* $S(L)$. On the other hand, the existence *a priori* of any reversing symmetries for a particular L is unclear. When L has a reversing symmetry, L is called *reversible*, and *irreversible* otherwise. The set $\mathcal{R}(L)$ of all symmetries and reversing symmetries of L is a group, too, called the *reversing symmetry group* ([17]) of L (see also [10]).

The simultaneous consideration of ordinary and reversing symmetries of reversible automorphisms (which may arise as the time-one maps of reversible flows) is known to provide some powerful algebraic insights. As the results of [17, 10] illustrate, the knowledge of $S(L)$ has several implications on the nature of possible reversing symmetries in $\mathcal{R}(L)$. The power of this group theoretic setting has recently been realised in cases where one has access to the structure of the symmetry group $S(L)$, as in the case of toral automorphisms ([1, 2]) (via Dirichlet's unit theorem [13, Chapter 15.5]) or polynomial automorphisms of the plane ([25, 3, 8, 9]) (via the classification of Abelian subgroups according to [31]).

In many cases of reversible automorphisms (and also in the analogous continuous-time case of reversible flows), it is in fact found that all its reversing symmetries R are involutions or elements of small even order. Whenever an involutory reversor exists, the automorphism L can be written as the composition of two involutions, for example, $L \circ R$

and R, or R and $R \circ L$, an observation that goes back to Birkhoff [4]. References [26] and [20] include reviews of the properties and applications of reversible automorphisms and flows.

The goal of the present paper is to analyze the general structure of $\mathcal{R}(L)$, distilling and extending some theoretical insights from specific cases already considered in [1, 2, 3, 25]. Most of the algebraic methods we use below are standard. Nevertheless, in view of the applications to dynamical systems, we try to make the text self-contained as far as algebraic methods are concerned (also giving references for further background material).

2. MATHEMATICAL SETTING

From now on, we shall work within a given group G, for example, the automorphism group of some space X. Elements of G will be denoted by f, g et cetera, with 1 being the neutral element. Motivated by the dynamical systems context, we define the following subgroups of G. The *symmetry group* of an element $f \in G$ is the centraliser of this element within G, that is,

$$(1) \qquad \mathcal{S}(f) := \mathrm{cent}_G(f) = \{g \in G \mid fg = gf\} = \{g \in G \mid gfg^{-1} = f\}.$$

The *reversing symmetry group* $\mathcal{R}(f)$ is defined as

$$(2) \qquad \mathcal{R}(f) := \{h \in G \mid hfh^{-1} = f^{\pm 1}\}.$$

There are well-known facts about the groups $\mathcal{S}(f)$ and $\mathcal{R}(f)$, not all of which are easy to locate in the literature. In this section, we recall and extend some results that are relevant to our later discussion, providing short proofs.

Clearly, $\mathcal{R}(f)$ is a subgroup of G that contains $\mathcal{S}(f)$, and one has, compare [17, 1]:

FACT 1. $\mathcal{S}(f)$ is a normal subgroup of $\mathcal{R}(f)$, with the factor group $\mathcal{R}(f)/\mathcal{S}(f)$ either being the trivial group or C_2, the cyclic group of order 2.

PROOF: If $\mathcal{R}(f) = \mathcal{S}(f)$, which happens if $f^2 = 1$ or if f is irreversible, the statement is trivial. So, assume that there is an $r \in \mathcal{R}(f)$ with $rfr^{-1} = f^{-1} \neq f$. Define a binary *grading* $\Sigma : \mathcal{R}(f) \longrightarrow C_2 = (\{\pm 1\}, \cdot)$ by $\Sigma(h) := \varepsilon$ when $hfh^{-1} = f^\varepsilon$. This grading is a group homomorphism with $\ker(\Sigma) = \mathcal{S}(f)$ (hence $\mathcal{S}(f)$ is a normal subgroup) and $\mathrm{im}(\Sigma) = C_2$ (thus $\mathcal{R}(f)/\mathcal{S}(f) \simeq C_2$), which establishes the claim. The grading highlights the fact that the composition of two reversors is a symmetry. $\qquad\qquad\square$

The case that $f^2 = 1$ is not of particular interest, as this always gives $\mathcal{R}(f) = \mathcal{S}(f)$, due to $f^{-1} = f$. So, from now on, we shall always assume

> The element $f \in G$ satisfies $f^2 \neq 1$, that is, it is neither 1 nor an involution.

This has an immediate consequence [17, Proposition 5] that we shall need a number of times below:

FACT 2. If f is reversible, with $f^2 \neq 1$, no reversor of f can be of odd order.

PROOF: If r is any reversor of f, we have $rfr^{-1} = f^{-1}$. This implies $rf^{-1}r^{-1} = f$ (using $1 = rr^{-1} = rfr^{-1}rf^{-1}r^{-1} = f^{-1}rf^{-1}r^{-1}$), hence also $r^{\ell}fr^{-\ell} = f^{(-1)^{\ell}}$. Then, $r^{2m+1} = 1$ would give $f = f^{-1}$, contradicting the assumption. $\Box$

REMARK 1.   For most applications in dynamical systems, one is mainly interested in the situation that f is not of finite order, so that

$$\langle f \rangle := \left\{ f^n \mid n \in \mathbb{Z} \right\} \simeq C_{\infty}.$$

In this case, the reversing symmetry group $\mathcal{R}(f)$ of (2) can also be formulated as

$$(3) \qquad\qquad\qquad \mathcal{R}(f) = \mathrm{norm}_G\big(\langle f \rangle\big)$$

because $h\langle f \rangle h^{-1} = \langle f \rangle$ is only possible here if f (as a generator of $\langle f \rangle$) is conjugated into a generator, hence into either f or f^{-1}. Equation (3) should then be compared with $\mathcal{S}(f) = \mathrm{cent}_G\big(\langle f \rangle\big)$, the latter being an obvious reformulation of Equation (1).

If f is of *finite* order, $\mathrm{norm}_G\big(\langle f \rangle\big)$ contains $\mathcal{R}(f)$ as a subgroup, but possibly further elements, for example, elements h with $hfh^{-1} = f^2$. It might then be advantageous, also in view of questions discussed in [11], to consider this extension.

Let us recall another classic result on the order of reversing symmetries, see [18, Theorem 1.1.5], with a considerably simplified proof.

FACT 3.   Let $f \in G$, with $f^2 \neq 1$, have a reversor r of finite order. Then, this order is $\mathrm{ord}(r) = 2^{\ell}(2m + 1)$ for some $\ell \geqslant 1$, and f also has a reversor r' of order 2^{ℓ}. The set of all reversors of f, within G, is thus given by $r'\mathcal{S}(f)$.

PROOF: Clearly, the order of r is even, by Fact 2, and hence of the form stated. Define $r' = r^{2m+1}$, which is a reversor of f because $2m + 1$ is odd. Clearly, r' has order 2^{ℓ}. Fact 1 implies that we can use 1 and r' as the coset representatives of $\mathcal{S}(f)$ in $\mathcal{R}(f)$, so that we get $\mathcal{R}(f) = \mathcal{S}(f) \, \dot{\cup} \, r'\mathcal{S}(f)$. $\Box$

An important consequence of Fact 3 is that we may restrict the search for reversing symmetries to elements of order 2^{ℓ}, $\ell \geqslant 1$, provided there is a finite order reversor at all.

As mentioned in the Introduction, a particularly frequent case in applications is that of an involutory reversor. To formulate the corresponding result ([1]), we write $N \rtimes G$ for the semi-direct product of the groups N and G, with N the normal subgroup.

LEMMA 1.   *Let $f \in G$ be a mapping with $f^2 \neq 1$ and symmetry group $\mathcal{S}(f)$. If f has an involutory reversor r, the reversing symmetry group is $\mathcal{R}(f) = \mathcal{S}(f) \rtimes C_2$, with $C_2 = \langle r \rangle$.*

PROOF: Once again by Fact 1, we know that 1 and r can be used as the coset representatives, that is, $\mathcal{R}(f) = \mathcal{S}(f) \, \dot{\cup} \, r\mathcal{S}(f)$, all seen as subgroups or subsets of G. As r is an involution, $\mathcal{R}(f)/\mathcal{S}(f) \simeq \langle r \rangle = C_2$, thus establishing the semi-direct product. $\Box$

Let us give an important example where *all* reversors are involutions, irrespective of the structure of $\mathcal{S}(f)$.

EXAMPLE 1. ([**16**, **15**]) Let E be an elliptic curve defined over a field $\mathbb{K}$. It is birationally conjugate to a Weierstrass form $W\colon y^2 = x^3 + Ax + B$, with $A, B \in \mathbb{K}$. It is well known, see [**30**], that the points $W(\mathbb{K})$ on the curve W (or $E(\mathbb{K})$ on the curve E) with coordinates in $\mathbb{K}$ form an Abelian group with associated group law "+". Let G be the group of birational transformations over $\mathbb{K}$ that map E to itself. Then, in the typical case (that is, when the curve does not permit complex multiplication, which can be worked out using the so-called j-invariant), G has the form

$$(4) \qquad\qquad G \simeq \mathcal{T} \rtimes \{\pm \mathbb{1}\},$$

where $\mathcal{T}$ is the group of translations on W, $P \mapsto P + \Omega$ with $\Omega \in W(\mathbb{K})$, and $\pm\mathbb{1}$ stands for $P \mapsto \pm P$. Clearly, any $f \in \mathcal{T}$, with $f^2 \neq \mathbb{1}$, has $\mathcal{S}(f) = \mathcal{T} \simeq W(\mathbb{K})$, that is, $\mathcal{S}(f)$ is Abelian. The reversors of $f \in G$ are always involutions, $P \mapsto -P + S$, for some $S \in W(\mathbb{K})$.

The structure of $W(\mathbb{K})$, and hence of $\mathcal{S}(f)$, is quite general, depending on the field $\mathbb{K}$. In particular, $W(\mathbb{R})$ is a one-dimensional compact Lie group, while $W(\mathbb{C}) \simeq \mathbb{T}^2$, the 2-torus. Moreover, $W(\mathbb{Q})$ is a finitely generated Abelian group, hence, by [**21**, Theorem I.8.5],

$$W(\mathbb{Q}) \simeq F \times (C_\infty)^{r_W},$$

where r_W is the rank of the curve and F is the finite torsion group.

Looking more closely at this example, one realises that the extra structure, in comparison to Lemma 1, is that any involutory reversor r of f actually conjugates *all* elements of the group $\mathcal{S}(f)$ into their inverses, not just f. This is a situation that is not a priori restricted to a translation group structure as in (4). An important part of the semi-direct product structure $\mathcal{R}(f) = \mathcal{S}(f) \rtimes \langle r \rangle$ in Lemma 1 is the induced automorphism σ on the normal subgroup,

$$(5) \qquad\qquad \sigma(g) := rgr^{-1} = rgr,$$

for all $g \in \mathcal{S}(f)$. Given an involutory reversor r, the interplay between the nature of σ and the structure of $\mathcal{S}(f)$ can be used effectively to determine the detailed structure of the group $\mathcal{R}(f)$, as we shall see below in Theorem 2. In particular, given an involutory reversor r, the order of any other reversor rg with $g \in \mathcal{S}(f)$, necessarily of this form by Fact 1 and of even order by Fact 2, follows from the equations

$$(6) \qquad\qquad (rg)^{2k} = (rgr^{-1}g)^k = (\sigma(g)\,g)^k, \quad \text{for } k \in \mathbb{Z}.$$

This has the following simple consequences (compare Example 1).

PROPOSITION 1. *Consider the element $f \in G$ of Lemma 1 with an involutory reversor r, an element $g \in \mathcal{S}(f)$ and σ as in (5). Then, one has:*

(1) $\sigma(g) = g^{-1}$ if and only if the reversor rg is an involution. Consequently, r is a simultaneous reversor for all elements of the group $\mathcal{S}(f)$ if and only if all reversors of f are involutions;

(2)   any finite order reversor of f must have order 2ℓ, where ℓ is the order of some finite order symmetry of f. So, if no non-trivial symmetry of finite order exists, there can only be reversors that are involutions or of infinite order. In this case, if $\sigma(g') \neq (g')^{-1}$ for some $g' \in \mathcal{S}(f)$, the reversor rg' is of infinite order.

PROOF: The first claim is obvious from Equation (6), used with $k = 1$. The second claim follows from the observation that $(rg)^2 = \sigma(g)\, g$ is a symmetry, hence either trivial or not of finite order under the assumptions made.   ☐

COROLLARY 1.   If all reversors of f are involutions, the symmetry group $\mathcal{S}(f)$ is Abelian.

PROOF: By part (1) of Proposition 1, a reversor r of f is a simultaneous reversor for all elements of $\mathcal{S}(f)$. So, if $a, b \in \mathcal{S}(f)$, we have $rar = a^{-1}$, $rbr = b^{-1}$ and $r(ab)r = (ab)^{-1}$. Consequently,

$$a^{-1}b^{-1} = rabr = (ab)^{-1} = b^{-1}a^{-1}$$

which gives $ab = ba$.   ☐

That the converse of Corollary 1 is not true is illustrated below in Theorem 2 and the associated examples.

3. IMPLICATIONS FROM THE SYMMETRY GROUP

To further explore the group theoretic concequences, let us recall the concept of a group extension, compare [12, Theorem 15.3.1] or [14, Section I.14]. Fact 1 shows that we need to look at cyclic C_2-extensions of the symmetry group, but not all such extensions will give reversing symmetry groups. It is thus a natural task to select and classify those that do. We now present first steps in this direction, building on previous work by various authors [17, 10, 20].

The main point in using the group theoretic setting comes from the consequences of the structure of $\mathcal{S}(f)$ to that of $\mathcal{R}(f)$. Classifying the structure of (non-trivial) reversing symmetry groups then means:

(1)   Start from groups of the form $N = \mathrm{cent}_G(f)$, for some f with $f^2 \neq 1$;

(2)   Search for an $h \in G \setminus N$ with $hfh^{-1} = f^{-1}$;

(3)   Classify $H = N \,\dot\cup\, hN$, a C_2-extension of N, according to its group structure.

Our point here is that such a classification is a purely group theoretic problem. In concrete examples and applications, special conditions can then lead to further restrictions.

REMARK 2.   It can also become meaningful, or even necessary, to consider the equation $hfh^{-1} = f^{-1}$ only *up to symmetries*, that is, to look for solutions of $hfh^{-1} = sf^{-1}$ with $s \in \mathcal{S}(f)$. If s is of finite order, some power of f, f^k say, is reversible in the usual sense. This is the basic mechanism of reversing k-symmetries, compare [**18, 19**] for details. A similar remark applies to k-symmetries in comparison to ordinary symmetries. Conversely, a reversible element $f \in G$ might have a *root* in G that is not reversible itself, but satisfies such a more general equation. We shall meet this situation below, in part (3) of Theorem 2.

Let us continue with a general observation, which is a rather direct consequence of a result of Goodson, see [**10**, Proposition 2] and the generalisation mentioned afterwards, and [**2**, Fact 11].

PROPOSITION 2.   Let $f \in G$ be an element of infinite order, and assume that $\mathcal{S}(f) = \mathcal{F} \times \langle g \rangle$ where $\mathcal{F}$ is some finite group of order $N \geqslant 1$ (not necessarily Abelian), and g is some generator (then necessarily of infinite order). If r is a reversor of f, r is an element of finite order. Its order is even and divides $2N$.

PROOF: If r is a reversor, r^2 is a symmetry, hence $r^2 = sg^m$, for some $s \in \mathcal{F}$ and some integer m. Note that, due to the assumption of the direct product structure, we always have $sg = gs$, even if $\mathcal{F}$ itself is not Abelian. Since the group $\mathcal{F}$ is finite and of order N, we know that $s^n = 1$ for some $n \geqslant 1$ that divides N. This implies that $r^{2n} = g^{mn}$.

As f is not of finite order, but clearly an element of $\mathcal{S}(f)$, we may assume $f^N = g^k$ for some (positive) integer k without loss of generality, modifying the argument just used (in particular, $k \neq 0$, while $k > 0$ might require to replace g by g^{-1}).

Since $rf = f^{-1}r$ by assumption (hence also $rf^\ell = f^{-\ell}r$, for all $\ell \in \mathbb{Z}$), we choose $\ell = mnN$ and obtain $rg^{kmn} = g^{-kmn}r$. Since $g^{kmn} = r^{2nk}$, this implies $r\, r^{2nk} = r^{-2nk}r$ and thus $r^{4nk} = 1$, that is, r is of finite order. Since $r^{2n} = g^{mn}$, this is only possible for $mn = 0$, hence $m = 0$. This implies $r^{2n} = 1$, so the order of r divides $2N$. If f is not of finite order, it is not an involution, and r can then not be of odd order by Fact 2 (hence also $r \neq 1$).   ☐

REMARK 3.   An alternative way to state the result of Proposition 2 is the following. If f is an element of infinite order, such that the factor group $\mathcal{S}(f)/\langle f \rangle$ is finite, any reversor r of f must be of finite order. In particular, $r^{2k} = 1$ for some integer $k \geqslant 1$ that divides the order of the factor group.

THEOREM 1.   Let $f \in G$ be an element of infinite order, with $\mathcal{S}(f) \simeq C_\infty$. If f is reversible, one has $\mathcal{R}(f) = \mathcal{S}(f) \rtimes C_2 \simeq D_\infty$, and all reversors of f are involutions.

PROOF: If $\mathcal{S}(f) = \langle g \rangle \simeq C_\infty$, we must have $f = g^m$ for some $0 \neq m \in \mathbb{Z}$. Let r be any reversor of f, which must then be an involution by Proposition 2. This gives the general structure of $\mathcal{R}(f)$ as a semi-direct product by Lemma 1.

In view of Proposition 1, we now have to look at $\sigma(g) = rgr^{-1}$. By the previous argument, all reversors of f are involutions, hence necessarily $rgr^{-1} = g^{-1}$, and

$$\mathcal{R}(f) = \langle g \rangle \rtimes \langle r \rangle \simeq D_\infty$$

is clear.   ☐

The situation of Theorem 1 looks rather special, but actually occurs in some important dynamical contexts.

EXAMPLE 2.   Let G be the space group of the integer lattice $\mathbb{Z}$ in dimension one, which is $G = \mathbb{Z} \rtimes O(1) = \mathbb{Z} \rtimes \{\pm 1\}$, compare [6]. So, G contains all Euclidean transformations that map $\mathbb{Z}$ onto itself, and it has the structure (4) with

$$\mathcal{T} = \{T_m : x \mapsto x + m \mid m \in \mathbb{Z}\} \simeq \mathbb{Z}.$$

Now, take $f = T_n$ (with $n \neq 0$) as our mapping, the n-fold shift. This is a standard mapping considered in symbolic dynamics, compare [22], and G is a very natural group to embed it in. Clearly, $\mathcal{S}(T_n) = \text{cent}_G(T_n) = \mathcal{T} \simeq C_\infty$, while the map $x \mapsto -x$ is an involutory reversor for T_n, noting that $(T_n)^{-1} = T_{-n}$. Consequently, we have $\mathcal{R}(T_n) \simeq C_\infty \rtimes C_2$, as in Theorem 1.

Note that all involutions in G are of the form $x \mapsto -x + m$, with $m \in \mathbb{Z}$, and are always conjugate, within G, to either $x \mapsto -x$ or $x \mapsto -x + 1$. The latter are conjugate via a half-integer shift, hence not within G, but within some larger group.

REMARK 4.   In the previous example, we could replace $\mathbb{Z}$ by $\mathbb{Q}$ or $\mathbb{R}$, with obvious changes to the symmetry group, though the latter is no longer isomorphic with C_∞. Also, if Γ is the generic lattice in $\mathbb{R}^d$, its space group [6] is $G = \Gamma \rtimes \{\pm 1\}$, as inversion is then the only isometry of the lattice. The previous example can now easily be extended to an arbitrary translation $f \colon x \mapsto x + a$ with $0 \neq a \in \Gamma$.

EXAMPLE 3.   Consider $G = \text{PGL}(2, \mathbb{Z})$, the group of integer matrices with determinant ± 1, identified up to an overall sign, that is, $\text{PGL}(2, \mathbb{Z}) = \text{GL}(2, \mathbb{Z})/\{\pm \mathbb{1}\}$. By Dirichlet's unit theorem, one can show [2] that, if $M \in \text{PGL}(2, \mathbb{Z})$ is not of finite order, its symmetry group is $\mathcal{S}(M) = \text{cent}_G(M) \simeq C_\infty$. A concrete example, even with $C_\infty = \langle M \rangle$, is

$$(7) \quad M = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \quad \text{with reversors } R = \begin{bmatrix} 1 & 0 \\ 1 & -1 \end{bmatrix} \text{ and } R' = RM = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix},$$

where we write $[M]$ for a matrix up to overall sign. Note that both R and R' are involutions in $\text{PGL}(2, \mathbb{Z})$, but they are not conjugate within this group.

In other examples, M need not be a generator of C_∞, as, in general, such a matrix can have roots in G. Note that the spectrum of M in (7) is only self-reciprocal up to an overall factor of -1, thus M is not reversible in $\text{GL}(2, \mathbb{Z})$, though its square is (see below).

REMARK 5.   Two groups of dynamical systems isomorphic to $\mathrm{PGL}(2, \mathbb{Z})$ are:

   (1)   The group of 3-dimensional invertible polynomial maps which preserve the Fricke–Vogt invariant

$$I(x, y, z) = x^2 + y^2 + z^2 - 2xyz - 1$$

and fix the point $(1, 1, 1)$. Corresponding to M, R and R' above are, respectively, the Fibonacci trace map $(x, y, z) \mapsto (y, z, 2yz - x)$ and its reversors $(x, y, z) \mapsto (z, y, x)$ and $(x, y, z) \mapsto (2yz - x, z, y)$, see [24] and references therein for details.

   (2)   The group of homeomorphisms of the 2-sphere $\mathbb{S}^2$ that are induced by taking the quotient of the action of a $\mathrm{GL}(2, \mathbb{Z})$ matrix on $\mathbb{T}^2$ by the reflection in the origin. Whenever the $\mathrm{GL}(2, \mathbb{Z})$ matrix is hyperbolic, this yields a so-called pseudo-Anosov map of $\mathbb{S}^2$, see [5, 23] for details.

THEOREM 2.   *If $f \in G$ is a reversible element of infinite order with symmetry group $\mathcal{S}(f) \simeq C_2 \times C_\infty$, all reversors must be involutions or elements of order 4. In particular, one finds precisely one of the following three situations.*

   (1) $\mathcal{R}(f) \simeq C_2 \times D_\infty$, *if and only if all reversors of f are involutions.*

   (2) $\mathcal{R}(f) \simeq C_\infty \rtimes C_4$, *if and only if all reversors of f are elements of order 4.*

   (3) $\mathcal{R}(f) \simeq (C_2 \times C_\infty) \rtimes C_2$, *if and only if there are reversors both of order 2 and 4.*

PROOF: By assumption and Proposition 2, we know that a reversor in this setting must be an involution or an order 4 element.

Let $\mathcal{S}(f) \simeq C_2 \times C_\infty$ with $C_\infty = \langle g \rangle$ and an involutory symmetry s, which is then unique by the structure of the group. If the reversor r is an involution, one has $\mathcal{R}(f) \simeq \mathcal{S}(f) \rtimes C_2$. Since rsr is also an involutory symmetry, we get $rsr = s$ by uniqueness, and r and s commute. Since $r \neq s$, this gives $\mathcal{R}(f) \simeq (C_2 \times C_\infty) \rtimes C_2$, with either $rgr^{-1} = g^{-1}$ (then simplifying to $\mathcal{R}(f) \simeq C_2 \times D_\infty$) or $rgr^{-1} = sg^{-1}$ (in which case f must be an even power of g). Note that, in the latter case, $\varrho = gr$ is an element of order 4, and a reversor of f.

If $\mathcal{R}(f) = C_2 \times D_\infty$, we are in the situation of part (1) of Proposition 1, as r conjugates all generators of $\mathcal{S}(f)$ into their inverses. Consequently, all reversors of f are involutions then.

If f has a reversor r of order 4, $r^2 = s$ is the unique involutory symmetry of f, and $f = r^{2\varepsilon} g^m$ for $\varepsilon \in \{0, 1\}$ and some integer $m \neq 0$. In particular, r^2 and g commute, and rgr^{-1} is a symmetry of f, so that $rgr^{-1} = r^{2k} g^\ell$ for $k \in \{0, 1\}$ and some $\ell \in \mathbb{Z}$. Clearly, in view of $rfr^{-1} = f^{-1}$, this forces $\ell = -1$.

If $k = 0$, r is also a reversor of g, and we have $\mathcal{R}(f) \simeq C_\infty \rtimes C_4$. Reversors are of the form rg^n or $r^3 g^n$, all of which have order 4. This is the only case for m odd, while

for m even also $k = 1$ is possible, that is, $rgr^{-1} = r^2 g^{-1}$. This gives a group with the presentation

$$\mathcal{R}(f) = \langle r, g \mid r^4 = 1, \, rg^{\pm 1} = g^{\mp 1} r^{-1} \rangle$$

which is an index 2 extension of $\mathcal{S}(f) \simeq C_2 \times C_\infty$, but does not look like a simple semi-direct product. However, $\rho = g^{-1} r$ is an involution that satisfies $\rho g \rho = r^2 g^{-1}$, and it is a reversor for f. This brings us back to $\mathcal{R}(f) \simeq (C_2 \times C_\infty) \rtimes C_2$, where the outer C_2 is generated by ρ.

This chain of arguments shows that the 3 cases of the theorem are both (algebraically) possible and exhaustive. □

REMARK 6.   Note that the meaning of the group

$$\big(C_2 \times C_\infty\big) \rtimes C_2 = \big(\langle s \rangle \times \langle g \rangle\big) \rtimes \langle \rho \rangle$$

in case (3) of Theorem 2 includes the induced automorphism $\rho g \rho^{-1} = s g^{-1}$. This is the key difference to case (1), where a different induced automorphism permits the simplification shown.

Examples of all three cases of Theorem 2 appear among hyperbolic toral automorphisms (or cat maps) and polynomial automorphisms of the plane:

EXAMPLE 4.   ([**1, 2, 28**]) Elements M of the matrix group $\mathrm{GL}(2, \mathbb{Z})$ that are not of finite order, including the hyperbolic ones, have $\mathcal{S}(M) \simeq C_2 \times C_\infty$, where $C_2 = \{\pm 1\}$. Reversible elements M, and associated reversors R (with subscripts indicating their order), which illustrate each case of Theorem 2 are:

$$(1): \quad M = \begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix}, \quad R_2 = \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix};$$

$$(2): \quad M = \begin{pmatrix} 5 & 7 \\ 7 & 10 \end{pmatrix}, \quad R_4 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix};$$

$$(3): \quad M = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}, \quad R_2 = \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix} \text{ and } R_4 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Note that the third case is closely related to the previous $\mathrm{PGL}(2, \mathbb{Z})$ matrix in Equation (7).

EXAMPLE 5.   ([**3, 9, 25**]) Consider the case that G is the group of planar polynomial automorphisms with coefficients in the field $\mathbb{K}$, that is, polynomial transformations $x' = P(x, y)$, $y' = Q(x, y)$ that have a polynomial inverse (for ease of notation, we use (x', y') for the image points), see [**7**] for general background material. Utilising the classical result that G is an amalgamated free product of two groups, consequently giving knowledge of the Abelian subgroups within G ([**31**]), it can be shown that $\mathcal{S}(f)$ is

isomorphic to either C_∞ or $C_2 \times C_\infty$, when $\mathbb{K} \in \{\mathbb{Q}, \mathbb{R}\}$ and f is dynamically non-trivial. The latter property means, in the language of [3], that f is a so-called CR element of G, hence neither conjugate to an affine nor to an elementary mapping in G.

Reversible elements (for G with $\mathbb{K} \in \{\mathbb{Q}, \mathbb{R}\}$) illustrating each case of Theorem 2 are:

(1) $f : x' = x + p(y)$, $y' = y + q(x')$, with $p \neq q$ odd polynomials;

$s : x' = -x$, $y' = -y$, an involution;

$r : x' = -x - p(y)$, $y' = y$, an involution;

$\mathcal{S}(f) = \mathrm{cent}_G(f) = \langle s \rangle \times \langle f \rangle \simeq C_2 \times C_\infty$;

$\mathcal{R}(f) = \langle s \rangle \times (\langle f \rangle \rtimes \langle r \rangle) \simeq C_2 \times D_\infty$.

(2) $f : x' = -x + y^3$, $y' = -y - (x')^3$,

involutory symmetry s as in case (1);

$r : x' = -y$, $y' = x$, an order 4 reversor, with $r^2 = s$;

$\mathcal{S}(f) = \mathrm{cent}_G(f) = \langle s \rangle \times \langle f \rangle \simeq C_2 \times C_\infty$;

$\mathcal{R}(f) = \langle f \rangle \rtimes \langle r \rangle \simeq C_\infty \rtimes C_4$.

(3) $f : x' = x + p(y)$, $y' = y + p(x')$, with p an odd polynomial.

involutory symmetry s and reversor r as in case (1);

$t : x' = y$, $y' = x + p(y)$, so that $f = t^2$;

$\mathcal{S}(f) = \mathrm{cent}_G(f) = \langle s \rangle \times \langle t \rangle \simeq C_2 \times C_\infty$;

$\mathcal{R}(f) = (\langle s \rangle \times \langle t \rangle) \rtimes \langle r \rangle \simeq (C_2 \times C_\infty) \rtimes C_2$.

In cases (1) and (2), f has no root in G. In case (3), $r' = tr$ is an order 4 reversor of f.

Note that [27] provides a test for reversibility within the group G, when a reduction of the polynomial maps to finite fields is possible.

Following on from Theorem 2, it would be nice to have some similarly simple classification of the group structure of $\mathcal{R}(f)$ for more general symmetry groups $\mathcal{S}(f)$. However, things quickly become more involved, in particular if f possesses roots in G, which is a situation frequently met in practice. If f has no roots in G, one can go further as follows.

THEOREM 3. *Let $\mathcal{S}(f) \simeq C_p \times C_\infty$ with $C_\infty = \langle f \rangle$ and $C_p = \langle h \rangle$, p an odd prime. If f is reversible, there are always involutory reversors, and one meets precisely one of the following two situations.*

(1) $\mathcal{R}(f) = C_\infty \rtimes C_{2p} = \langle f \rangle \rtimes \langle r \rangle$, *with* $rfr^{-1} = f^{-1}$ *and* $h = r^2$, *if and only if a reversor r of order $2p$ exists;*

(2) $\mathcal{R}(f) = (C_p \times C_\infty) \rtimes C_2$, *with* $C_2 = \langle r \rangle$ *and* $rhr = h^{-1}$, *if and only if all reversors are involutions.*

PROOF: By Proposition 2, any reversor r of f must be of even order that divides $2p$, so either $\mathrm{ord}(r) = 2$ or $\mathrm{ord}(r) = 2p$ because p is prime. In the latter case, in line with

Fact 3, r^p is an involutory reversor, so that $\mathcal{R}(f) = (C_p \times C_\infty) \rtimes C_2$ in both cases, by Lemma 1.

We can thus focus on the equation $qfq^{-1} = f^{-1}$ with $q^2 = 1$, and consider the possible automorphisms induced by q on $\mathcal{S}(f)$. Clearly, $qhq^{-1} = qhq$ is a symmetry of f of order p, so that $qhq = h^m$ for some $1 \leqslant m \leqslant p - 1$. Since $h = q^2 hq^2 = qh^m q = h^{m^2}$, we must have $m^2 = 1 \pmod p$. Since p is a prime (and $\mathbb{F}_p$ thus a finite field), this congruence has precisely two solutions. These are $m = \pm 1 \pmod p$, either giving $qhq = h$ or $qhq = h^{-1}$.

In the first case, h and q commute, and $(qh)^k = q^k h^k$. This shows that $r = qh$, which is also a reversor, has order $2p$, and $r^p = q$. Consequently, the reversing symmetry group becomes $\mathcal{R}(f) = C_\infty \rtimes C_{2p}$ with $C_{2p} = \langle r \rangle$ and $r^2 = h$.

In the second case, q is a reversor also for the finite order element h, and the structure of $\mathcal{R}(f)$ is as claimed. This brings us back to the situation of part (1) of Proposition 1, hence all reversors of f are involutions. □

REMARK 7. If one considers $\mathcal{S}(f) = C_n \times C_\infty = \langle h \rangle \times \langle f \rangle$ for $n > 1$ not a prime, things quickly become more complicated. In the case that n is odd, any reversor r must have order 2ℓ for some $\ell \mid n$, by Proposition 2. But then, $s = r^\ell$ is an involutory reversor, and we can again restrict ourselves to looking at the equation $sfs = f^{-1}$ and the induced automorphism on $\mathcal{S}(f)$. In this case, $shs = h^m$ for some

$$m \in \big\{ 1 \leqslant k \leqslant n \mid \gcd(k, n) = 1 \big\},$$

subject to the additional requirement that $m^2 = 1 \pmod n$. This equation always has the solutions $m = \pm 1 \pmod n$. They are the only ones for $n = p^k$ with $k \geqslant 1$ and p an odd prime, while more solutions exist otherwise, for example, $n = 15$ permits $m = \pm 1$ and $m = \pm 4$. The number of solutions is 2^a, with $a \geqslant 1$ the number of distinct prime divisors of n, see [13, Chapter 6.3]. The result of Theorem 3 has to be extended accordingly.

If n is even, such extra solutions may exist as well (for example, $n = 8$ permits $m = \pm 1$ and $m = \pm 3$, while $n = 12$ is compatible with $m = \pm 1$ and $m = \pm 5$). Here, if we write $n = 2^{k+1}(2\ell + 1)$ with $k \geqslant 0$, the number of solutions is $2^{a + \min\{k, 2\}}$, with $a \geqslant 0$ the number of distinct prime divisors of $2\ell + 1$, compare [13, Chapter 6.3]. In general, it is no longer true that at least one involutory reversor exists, as we already saw in case (2) of Theorem 2.

Next, let us take a closer look at a case where an additional symmetry of infinite order exists. This is motivated both by the structure of (projective) toral automorphisms in dimensions $d > 2$, see [2], and by other examples from algebraic dynamics, see [29] and references therein for an orientation.

THEOREM 4. *Let $\mathcal{S}(f) = \langle t \rangle \times \langle g \rangle \simeq C_\infty \times C_\infty$, with $f = g^n$ for some integer $n \neq 0$. Then, any reversor r of f is either an involution (hence giving $\mathcal{R}(f)$ as in Fact 1) or it is not of finite order.*

Moreover, r is also a reversor for g, and either $\sigma(t) := rtr^{-1} = t^{-1}$ or $\sigma(t) = tg^k$ for some $k \in \mathbb{Z}$. In the latter case, one can change the generators of $\mathcal{S}(f)$ in such a way that the equation is satisfied with either $k = 0$ or $k = 1$.

Finally, the following group structures for a reversible f with involutory reversor r are possible after this reduction.

    (1)   *$\mathcal{R}(f) = \langle t \rangle \times (\langle g \rangle \rtimes \langle r \rangle) \simeq C_\infty \times D_\infty$, if and only if r commutes with t. In this case, also reversors of infinite order exist.*

    (2)   *$\mathcal{R}(f) = (\langle t \rangle \times \langle g \rangle) \rtimes \langle r \rangle \simeq (C_\infty \times C_\infty) \rtimes C_2$, if and only if either $\sigma(t) = t^{-1}$ (which happens if and only if all reversors are involutions) or $\sigma(t) = tg$ (in which case, once again, also reversors of infinite order exist).*

PROOF: Since rgr^{-1} is a non-trivial symmetry of f, we must have $rgr^{-1} = t^\varepsilon g^\ell$ for some $\varepsilon, \ell \in \mathbb{Z}$, not both 0. On the other hand,

$$g^{-n} = f^{-1} = rfr^{-1} = rg^n r^{-1} = (rgr^{-1})^n = t^{n\varepsilon} g^{n\ell},$$

which implies $\varepsilon = 0$ and $\ell = -1$. This shows $rgr^{-1} = g^{-1}$. The statement about the order of r is obvious from the fact that r^2 is a symmetry.

Next, observe that $rtr^{-1} \neq 1$ is a symmetry, so that $rtr^{-1} = t^\varepsilon g^k$ for some $\varepsilon, k \in \mathbb{Z}$, not both 0. Since r^2 commutes with t, one finds

$$t = r^2 t r^{-2} = rt^\varepsilon g^k r^{-1} = (rtr^{-1})^\varepsilon rg^k r^{-1} = (t^\varepsilon g^k)^\varepsilon g^{-k} = t^{\varepsilon^2} g^{k(\varepsilon-1)}.$$

This implies $\varepsilon^2 = 1$ and $k(\varepsilon - 1) = 0$. The solutions are $\varepsilon = -1$ together with $k = 0$, which means that r is also a reversor for t, and $\varepsilon = 1$ together with an arbitrary $k \in \mathbb{Z}$, giving $rtr^{-1} = tg^k$.

In the latter case, one may assume that $k \geqslant 0$ (otherwise, replace the generator g by g^{-1}). If $k > 1$, one can define a new generator $\tilde{t} = tg^{\lfloor k/2 \rfloor}$, so that $\tilde{t}$ and g still generate the same group $\mathcal{S}(f)$. It is easy to check that this results in $r\tilde{t}r^{-1} = \tilde{t}$ (respectively $\tilde{t}g$) depending on whether k was even (respectively odd).

For the final assertion, $\mathcal{R}(f) = \mathcal{S}(f) \rtimes \langle r \rangle$ is clear by Lemma 1, where always $\sigma(g) = g^{-1}$. The three cases now follow from the different possibilities how σ acts on t. If r is a reversor for both t and g, we are again in the situation of part (1) of Proposition 1. Otherwise, non-involutory reversors exist, which must then be of infinite order.   ◻

EXAMPLE 6.   ([2]) Consider the matrices $M, R \in \mathrm{PGL}(4, \mathbb{Z})$ given by

$$M = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 2 & 2 & 2 \end{bmatrix} \quad \text{and} \quad R = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}.$$

It is easy to check that the involution R conjugates M into its inverse. As follows from [2, Corollary 6], M has symmetry group $\mathcal{S}(M) \simeq C_\infty \times C_\infty$ in $\mathrm{PGL}(4, \mathbb{Z})$. One generator is

M itself, as this is a matrix without roots in this matrix group, while the other generator can be either chosen as

$$N = \begin{bmatrix} 1 & 0 & -3 & 1 \\ -1 & 3 & 2 & -1 \\ 1 & -3 & 1 & 0 \\ 0 & 1 & -3 & 1 \end{bmatrix} \quad \text{or as} \quad N' := M\,N = \begin{bmatrix} -1 & 3 & 2 & -1 \\ 1 & -3 & 1 & 0 \\ 0 & 1 & -3 & 1 \\ -1 & 2 & 3 & -1 \end{bmatrix}.$$

Note that N can neither possess a root in $\mathrm{GL}(4,\mathbb{Z})$ nor in $\mathrm{PGL}(4,\mathbb{Z})$ because the sum of the square roots of the eigenvalues of N is not an integer. The characteristic polynomial of N is $Q(x) = x^4 - 6x^3 + 22x^2 - 14x + 1$, which is not self-reciprocal – neither directly nor up to an overall sign. Consequently, N is not reversible within G, and neither within $\mathrm{GL}(4,\mathbb{Q})$, compare [2, Propisition 2], and the same statement applies to N'. In fact, one quickly checks that R and N' commute, thus $R' := RN'$ is a reversor of infinite order. The reversing symmetry group thus has the structure $\mathcal{R}(M) = \langle N' \rangle \times \big(\langle M \rangle \rtimes \langle R \rangle \big) \simeq C_\infty \times D_\infty$, in line with case (1) of Theorem 4

REMARK 8.   The previous example can be considered within $\mathrm{GL}(4,\mathbb{Z})$ as well, that is, as a toral automorphism. Note that the largest eigenvalue of M is a so-called Salem number. The characteristic polynomial of M is $P(x) = x^4 - 2x^3 - 2x^2 - 2x + 1$, which is irreducible over $\mathbb{Z}$ (and hence also over $\mathbb{Q}$). Its roots are $\tau \pm \sqrt{\tau}$ (both real) and $(1-\tau) \pm \sqrt{1-\tau}$ (both on the unit circle), where $\tau = (\sqrt{5}+1)/2$ is the golden ratio. The symmetry is now $\mathcal{S}(M) \simeq C_2 \times C_\infty \times C_\infty$, with $C_2 = \{\pm\mathbb{1}\}$, with the other details to be changed accordingly.

4. COMMENTS AND FURTHER DIRECTIONS

Further extensions of the results along the lines of the previous theorems are possible. In particular, one might want to extend the setting to symmetry groups of the form $\mathcal{S}(f) = C_m \times C_\infty^\ell$, with $\ell \geqslant 1$ and m even, which occur for toral automorphisms ([2]) as a result of Dirichlet's unit theorem. Since the methods should be clear from our above results, we do not go into further detail.

Above, we have looked into the case that $\mathcal{S}(f) = \mathcal{H} \times \langle g \rangle$ where f was a power of g. In general, if $\mathcal{S}(f)$ is a finitely generated Abelian group, it is of the form $\mathcal{S}(f) = \mathcal{F} \times C_\infty^k$ with $\mathcal{F}$ a finite Abelian group, see [21, Theorem I.8.5]. For f not of finite order, we might then also assume that f is an element of one of the C_∞ factors.

However, in general, $\mathcal{S}(f)$ need not be Abelian, hence there is no compelling reason to start from a product structure such as $\mathcal{H} \times C_\infty$ (even with $\mathcal{H}$ non-Abelian), as can be seen from the possibility of k-symmetries. The general setting is then even more involved, but can be handled by a computer assisted approach, for example, as in the classification of crystallographic point and space groups.

REFERENCES

[1] M. Baake and J.A.G. Roberts, 'Reversing symmetry group of $GL(2, \mathbb{Z})$ and $PGL(2, \mathbb{Z})$ matrices with connections to cat maps and trace maps', *J. Phys. A: Math. Gen.* **30** (1997), 1549–1573.

[2] M. Baake and J.A.G. Roberts, 'Symmetries and reversing symmetries of toral automorphisms', *Nonlinearity* **14** (2001), R1–R24; math.DS/0006092.

[3] M. Baake and J.A.G. Roberts, 'Symmetries and reversing symmetries of polynomial automorphisms of the plane', *Nonlinearity* **18** (2005), 791–816; math.DS/0501151.

[4] G.D. Birkhoff, 'The restricted problem of three bodies', *Rend. Circ. Mat. Palermo* **39** (1915), 265–334.

[5] G. Cairns, B. Jessup and M. Nicolau, 'Topologically transitive homeomorphisms of quotients of tori', *J. Discrete Contin. Dynam. Systems* **5** (1999), 291–300.

[6] H.S.M. Coxeter and W.O.J. Moser, *Generators and relations for discrete groups*, (4th edition) (Springer, Berlin, 1980).

[7] A. van den Essen, *Polynomial automorphisms and the Jacobian conjecture* (Birkhäuser, Basel, 2000).

[8] A. Gómez and J.D. Meiss, 'Reversible polynomial automorphisms of the plane: the involutory case', *Phys. Lett. A* **312** (2003), 49–58; nlin.CD/0209055.

[9] A. Gómez and J.D. Meiss, 'Reversors and symmetries for polynomial automorphisms of the complex plane', *Nonlinearity* **17** (2004), 975–1000; nlin.CD/0304035.

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

[11] G.R. Goodson, 'Ergodic dynamical systems conjugate to their composition squares', *Acta Math. Univ. Comenian (N.S.)* **71** (2002), 201–210.

[12] M. Hall, *Group theory*, (2nd edition reprint) (Chelsea, New York, 2002).

[13] H. Hasse, *Vorlesungen über Zahlentheorie*, (2nd edition) (Springer, Berlin, 1964).

[14] B. Huppert, *Endliche Gruppen I* (Springer, Berlin, 1967).

[15] D. Jogia and J.A.G. Roberts, 'Integrable maps: the reversing symmetry group', (UNSW preprint 2006).

[16] D. Jogia, J.A.G. Roberts and F. Vivaldi, 'An algebraic geometric approach to integrable maps of the plane', *J. Phys. A: Math. Gen.* **39** (2006), 1133–1149.

[17] J.S.W. Lamb, 'Reversing symmetries in dynamical systems', *J. Phys. A: Math. Gen.* **25** (1992), 925–937.

[18] J.S.W. Lamb, *Reversing symmetries in dynamical systems*, (Ph.D. Thesis) (Amsterdam, 1994).

[19] J.S.W. Lamb and G.R.W. Quispel, 'Reversing k-symmetries in dynamical systems', *Physica D* **73** (1994), 277–304.

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

[21] S. Lang, *Algebra*, Revised 3rd edition (Springer, New York, 2002).

[22] D. Lind and B. Markus, *An introduction to symbolic dynamics and coding* (Cambridge University Press, Cambridge, 1995).

[23] J. Llibre and R.S. MacKay, 'Pseudo-Anosov homeomorphisms on a sphere with four punctures have all periods', *Math. Proc. Cambridge Philos. Soc.* **112** (1992), 539–549.

[24] J.A.G. Roberts and M. Baake, 'Trace maps as 3D reversible dynamical systems with an invariant', *J. Stat. Phys.* **74** (1994), 829–888.

[25] J.A.G. Roberts and M. Baake, 'Symmetries and reversing symmetries of area-preserving polynomial mappings in generalised standard form', *Physica A* **317** (2003), 95–112 `math.DS/0206096`.

[26] 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.

[27] J.A.G. Roberts and F. Vivaldi, 'Signature of time-reversal symmetry in polynomial automorphisms over finite fields', *Nonlinearity* **18** (2005), 2171–2192.

[28] R.S. Wilson, *Reversibility of cat maps*, M.Sc. minor thesis (Univ. of Melbourne, Victoria, 1997).

[29] K. Schmidt, *Dynamical systems of algebraic origin* (Birkhäuser, Basel, 1995).

[30] J.H. Silverman and J. Tate, *Rational points on elliptic curves* (Springer, New York, 1992).

[31] D. Wright, 'Abelian subgroups of $\mathrm{Aut}_k(k[X,Y])$ and applications to actions on the affine plane', *Illinois J. Math.* **23** (1979), 579–634.

Fakultät für Mathematik   School of Mathematics
Universität Bielefeld   University of New South Wales
33501 Bielefeld   Sydney, NSW 2052
Germany   Australia
e-mail: mbaake@math.uni-bielefeld.de   e-mail: jag.roberts@unsw.edu.au
`http://www.math.uni-bielefeld.de/baake`   `http://www.maths.unsw.edu.au/~jagr`