DISCRETE AND CONTINUOUS
DYNAMICAL SYSTEMS
Volume **33**, Number **2**, February **2013**

doi:10.3934/dcds.2013.33.527

pp. **527–553**

ORBIT STRUCTURE AND (REVERSING) SYMMETRIES OF TORAL ENDOMORPHISMS ON RATIONAL LATTICES

Michael Baake and Natascha Neumärker

Fakultät für Mathematik, Universität Bielefeld
Postfach 100131, 33501 Bielefeld, Germany

John A. G. Roberts

School of Mathematics and Statistics, University of New South Wales
Sydney, NSW 2052, Australia

(Communicated by Bernold Fiedler)

Abstract. We study various aspects of the dynamics induced by integer matrices on the invariant rational lattices of the torus in dimension 2 and greater. Firstly, we investigate the orbit structure when the toral endomorphism is not invertible on the lattice, characterising the *pretails* of eventually periodic orbits. Next we study the nature of the symmetries and reversing symmetries of toral automorphisms on a given lattice, which has particular relevance to (quantum) cat maps.

1. **Introduction.** Toral automorphisms or *cat maps*, by which we mean the action of matrices $M \in \mathrm{GL}(d,\mathbb{Z})$ on the d-torus $\mathbb{T}^d$, are a widely used and versatile class of dynamical systems, see [45, 28] for some classic results in the context of ergodic theory. Of particular interest are the hyperbolic and quasi-hyperbolic ones, which are characterised by having no root of unity among their eigenvalues. All periodic orbits of such automorphisms lie on the rational (or finite) invariant lattices $L_n = \{x \in \mathbb{T}^d \mid nx = 0 \bmod 1\}$, which are also known as the n-division points. One can encode the possible periods of a toral automorphism M on $\mathbb{T}^d$ via the dynamical zeta function in a systematic way, which is always a rational function [8, 18]. The literature on classifying periodic orbits of toral automorphisms when $d = 2$ is vast (compare [21, 25, 37] and references therein). An extension beyond $d = 2$ is difficult due to the fact that the conjugacy problem between integer matrices is then much harder because (unlike $d = 2$) no complete set of conjugacy invariants mod n is known. Therefore, our focus will also be on $d = 2$, with occasional extensions to higher dimensions.

The larger ring $\mathrm{Mat}(d,\mathbb{Z})$ of toral endomorphisms (which includes integer matrices without integer inverses) has received far less attention [2, 14, 8], particularly those in the complement of $\mathrm{GL}(d,\mathbb{Z})$. Note that the resulting dynamics induced by $M \in \mathrm{Mat}(d,\mathbb{Z}) \setminus \mathrm{GL}(d,\mathbb{Z})$ on a finite lattice L_n may or may not be invertible. In the latter case, beyond periodic orbits, there exist *eventually periodic* orbits which possess points that lead into a periodic orbit. We call these points and the periodic

2010 *Mathematics Subject Classification.* 37E30, 37E15.

Key words and phrases. Toral endomorphism, toral automorphism, periodic orbit, orbit structure, symmetry, reversing symmetry.

point to which they attach the 'pretails' to the periodic orbit (see Eq. (15) for a formal definition). The action of M induces a directed graph on L_n (e.g. see our three figures below). Alternatively, the pretails can be combined to form a rooted *tree* which is a characteristic attribute to any pair (M, L_n).

As well as their interest from a mathematical viewpoint, toral automorphisms also have been well-studied from a physics perspective, in particular as quantum cat maps (see [30, 19, 32] and references therein). Here, the action of the integer matrix on a rational lattice L_n, for some n, is all-important as quantum cat maps and their perturbations are built from (classical) cat maps and their perturbations *restricted to a particular rational lattice* (called the Wigner lattice in this instance). There has been recent interest in dealing with so-called pseudo-symmetries of quantum cat maps that are manifestations of local symmetries of cat maps restricted to some rational lattice [30, 19, 32]. Although, in the context of quantisation, matrices from the group $\mathrm{Sp}(2d, \mathbb{Z})$ play the key role, we prefer to work with the larger group of unimodular integer matrices and consider the former as a special case.

The main aims of this paper are twofold: (i) to elucidate the orbit structure of toral endomorphisms on rational lattices, equivalently the periodic orbits together with the related pretail tree structure; (ii) to further characterise the nature of symmetries or (time) reversing symmetries of toral automorphisms, these being automorphisms of the torus (or of a rational lattice) that commute with the cat map, respectively conjugate it into its inverse.

We expand a little on our results, where we refer to the actual formulation below in the paper. The results are readable without the surrounding notational details.

With respect to aim (i), Section 3 characterises the splitting of L_n into periodic and eventually periodic points under a toral endomorphism M. Every periodic point has a pretail graph isomorphic to that of the fixed point 0 (Corollary 1), which is trivial if and only if M is invertible on L_n. In general, the pretail tree codes important information on the action of M. One question in this context is whether all *maximal* pretails have the same length, for which we give a partial answer via a sufficient condition on $\ker(M)$ in Proposition 3. Given M, the lattice L_n can be decomposed into two invariant submodules, one of which captures the invertible part of M and the other the nilpotent part. This way, we are able to characterise the dynamics that is induced by M on L_n in the case of $n = p^r$ with p prime, in Corollary 3 and Lemma 3.

Our contribution towards aim (ii) continues the investigations from [9, 10, 12]. The key quantity for integer matrices of dimension 2 is the mgcd (see Eq. 13 below), and one consequence of [12, Thm. 2] is that $M \in \mathrm{SL}(2, \mathbb{Z})$ is always conjugate to its inverse on L_n, for each $n \in \mathbb{N}$. The conjugating element – called a reversing symmetry or reversor – is an integer matrix that has an integer matrix inverse on L_n, which typically depends on n. In this way, any $\mathrm{SL}(2, \mathbb{Z})$ matrix that fails to be conjugate to its inverse on the torus (e.g. $M = \left(\begin{smallmatrix} 4 & 9 \\ 7 & 16 \end{smallmatrix}\right)$ from [9, Ex. 2]) is still conjugate to its inverse on every rational lattice. In [12], we did not consider the nature of the reversor on the lattice. Theorem 1 of Section 4 establishes that it is an orientation-reversing involution, what is called an anticanonical (time-reversal) symmetry in the language of [30]. Section 4.2 uses normal forms of $\mathrm{GL}(2, \mathbb{F}_p)$ to characterise the symmetries and possible reversing symmetries of such matrices; the underlying structure of the conjugacy classes of $\mathrm{GL}(2, \mathbb{F}_p)$ is summarised in Table 4.2. The symmetry structure has some extensions to higher dimensions (Section

4.3) and to general modulus n (Section 4.4). Section 4.5 presents some results for the case when $M \in \mathrm{GL}(d, \mathbb{F}_p)$ has a root in the same group.

The structure of the paper is as follows. Section 2 summarises some properties of integer matrices that we use later in the paper, with some reformulations or slight generalisations that we find useful. In particular, throughout the paper, we formulate the results for arbitrary dimension whenever it is possible without extra complications, though this is not our main focus. As described, Section 3 addresses aim (i) above, while Section 4 deals with aim (ii). In the Appendix, we briefly discuss two classic examples of toral automorphisms for $d = 2$ and some aspects of their dynamics.

2. **Preliminaries and powers of integer matrices.**

The purpose of this section is to summarise important properties of and around integer matrices that are needed later on, with focus on those that are not standard textbook material. At the same time, we introduce our notation. For general background on integer matrices and their connections to algebraic number theory, we refer to the classic text by Taussky [43].

2.1. **Lattices, rings and groups.**

The most important lattices on the d-torus $\mathbb{T}^d = \mathbb{R}^d/\mathbb{Z}^d$, which is a compact Abelian group, consist of the n-division points

$$\begin{aligned} L_n \, &:= \, \{x \in \mathbb{T}^d \mid nx = 0 \ (\mathrm{mod}\ 1)\} \\ &= \, \bigl\{ \bigl(\tfrac{k_1}{n}, \dots, \tfrac{k_d}{n}\bigr) \mid 0 \le k_i < n \text{ for all } 1 \le i \le d \bigr\}, \end{aligned} \tag{1}$$

with $n \in \mathbb{N}$. Clearly, the L_n are invariant under toral endomorphisms (with the action of the representing matrices taken mod 1). It is sometimes easier to replace L_n by the set $\tilde{L}_n := \{(k_1, \dots, k_d) \mid 0 \le k_i < n\}$, with the equivalent action of M defined mod n. This also applies to various theoretical arguments involving modular arithmetic. Consequently, we use L_n (with action of M mod 1) and $\tilde{L}_n$ (with action mod n) in parallel.

Our discussion will revolve around the residue class ring $\mathbb{Z}/n\mathbb{Z}$ with $n \in \mathbb{N}$, which is a principal ideal ring, but not a domain, unless $n = p$ is a prime. In the latter case, $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ is the finite field with p elements, while the ring has zero divisors otherwise. For general n, the unit group

$$(\mathbb{Z}/n\mathbb{Z})^{\times} \, = \, \{1 \le m \le n \mid \gcd(m,n) = 1\}$$

is an Abelian group (under multiplication) of order $\phi(n)$, where ϕ is Euler's totient function from elementary number theory [26]. In general, it is not a cyclic group.

The integer matrices mod n form the finite ring $\mathrm{Mat}(d, \mathbb{Z}/n\mathbb{Z})$ of order n^{d^2}. The invertible elements in this finite ring form the general linear group $\mathrm{GL}(d, \mathbb{Z}/n\mathbb{Z}) = \{M \in \mathrm{Mat}(d, \mathbb{Z}/n\mathbb{Z}) \mid \det(M) \in (\mathbb{Z}/n\mathbb{Z})^{\times}\}$. If $n = p_1^{r_1} \cdots p_\ell^{r_\ell}$ is the standard prime decomposition, one finds

$$\bigl| \, \mathrm{GL}(d, \mathbb{Z}/n\mathbb{Z}) \bigr| \, = \, n^{d^2} \prod_{j=1}^{\ell} \frac{\bigl| \, \mathrm{GL}(d, \mathbb{F}_{p_j}) \bigr|}{p_j^{d^2}} \, , \tag{2}$$

where

$$\bigl| \, \mathrm{GL}(d, \mathbb{F}_p) \bigr| \, = \, (p^d - 1)(p^d - p) \cdot \ldots \cdot (p^d - p^{d-1}) \tag{3}$$

is well-known from the standard literature [33, 34]. Formula (2) follows from the corresponding one for $n = p^r$ via the Chinese remainder theorem, while the simpler prime power case is a consequence of the observation that each element of a non-singular matrix M over $\mathbb{Z}/p^s\mathbb{Z}$ can be covered (independently of all other matrix elements) by p elements in $\mathbb{Z}/p^{s+1}\mathbb{Z}$ without affecting its non-singularity.

Let us finally mention that $\mathrm{SL}(n,\mathbb{Z}/n\mathbb{Z})$, the subgroup of matrices with determinant 1, is a normal subgroup (it is the kernel of $\det\colon \mathrm{GL}(n,\mathbb{Z}/n\mathbb{Z}) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^{\times}$). The factor group is

$$\mathrm{GL}(n,\mathbb{Z}/n\mathbb{Z})/\,\mathrm{SL}(n,\mathbb{Z}/n\mathbb{Z}) \;\simeq\; (\mathbb{Z}/n\mathbb{Z})^{\times}$$

and thus has order $\phi(n)$.

2.2. **Orbit counts and generating functions.** The orbit statistics of the action of a matrix $M \in \mathrm{Mat}(d,\mathbb{Z})$ on the lattice L_n is encapsulated in the polynomial

$$Z_n(t) \;=\; \prod_{m\in\mathbb{N}} (1-t^m)^{c_m^{(n)}}, \tag{4}$$

where $c_m^{(n)}$ denotes the number of m-cycles of M on L_n. Recall that, if a_m and c_m denote the fixed point and orbit count numbers of M (dropping the upper index for a moment), they are related by

$$a_m \;=\; \sum_{d|m} d\, c_d \quad \text{and} \quad c_m \;=\; \frac{1}{m}\sum_{d|m} \mu\bigl(\tfrac{m}{d}\bigr)\, a_d, \tag{5}$$

where $\mu(k)$ is the Möbius function from elementary number theory [26].

Despite the way it is written, Z_n is a *finite* product and defines a polynomial of degree at most n^d. Note that the degree of Z_n can be smaller than n^d (as the matrix M need not be invertible on L_n), but $Z_n(t)$ is always divisible by $(1-t)$, because 0 is a fixed point of every M. The polynomials Z_n are closely related [12, 36] to the zeta function of toral endomorphisms, which can be calculated systematically; compare [8] and references therein. Dynamical zeta functions give access to the distribution and various asymptotic properties of periodic orbits [18, 40], and also relate to topological questions; compare [23] for a systematic exposition of the latter aspect in a more general setting. Further aspects on the asymptotic distribution of orbit lengths on prime lattices can be found in [29].

2.3. **Matrix order on lattices and plateau phenomenon.** Assume that M is invertible on L_n (hence also on $\tilde{L}_n$). Then, its order is given by

$$\mathrm{ord}(M,n) \;:=\; \gcd\{m \in \mathbb{N}_0 \mid M^m \equiv \mathbb{1} \mod n\}. \tag{6}$$

Clearly, $\mathrm{ord}(M,1)=1$ in this setting. When M is not invertible on L_n, the definition results in $\mathrm{ord}(M,n)=0$; otherwise, $\mathrm{ord}(M,n)$ is the smallest $m\in\mathbb{N}$ with $M^m = \mathbb{1}$ mod n.

Let $M \in \mathrm{GL}(d,\mathbb{Z})$ be arbitrary, but fixed. To determine $\mathrm{ord}(M,n)$ for all $n \geq 2$, it suffices to do so for n an arbitrary prime power, since the Chinese remainder theorem [26] gives

$$\mathrm{ord}(M,n) \;=\; \mathrm{lcm}\bigl(\mathrm{ord}(M,p_1^{r_1}),\ldots,\mathrm{ord}(M,p_\ell^{r_\ell})\bigr) \tag{7}$$

when $n = p_1^{r_1}\cdots p_\ell^{r_\ell}$ is the prime decomposition of n. It is clear that $\mathrm{ord}(M,p^r)$ divides $\mathrm{ord}(M,p^{r+1})$ for all $r\in\mathbb{N}$, see also [14, Lemma 5.2].

Let us now assume that $M \in \mathrm{Mat}(d,\mathbb{Z})$ is *not* of finite order, meaning that $M^k \neq \mathbb{1}$ for all $k\in\mathbb{N}$, which excludes the finite order elements of $\mathrm{GL}(d,\mathbb{Z})$. If p is a prime, we then obtain the unique representation

$$M^{\operatorname{ord}(M,p)} \;=\; \mathbb{1} + p^s B \tag{8}$$

with $s \in \mathbb{N}$ and an integer matrix $B \not\equiv 0 \bmod p$. Starting from this representation, an application of the binomial theorem for powers of it, in conjunction with the properties of the binomial coefficients mod p, gives the following well-known result.

Proposition 1. *Let $M \in \operatorname{Mat}(d,\mathbb{Z})$ be a matrix that is not of finite order. Fix a prime p that does not divide $\det(M)$, and let s be defined as in Eq. (8).*

When p is odd or when $s \geq 2$, one has $\operatorname{ord}(M,p^i) = \operatorname{ord}(M,p)$ for $1 \leq i \leq s$, together with $\operatorname{ord}(M,p^{s+i}) = p^i \operatorname{ord}(M,p^s)$ for all $i \in \mathbb{N}$.

In the remaining case, $p = 2$ and $s = 1$, either $\operatorname{ord}(M,2^r) = 2^{r-1}\operatorname{ord}(M,2)$ for all $r \in \mathbb{N}$, or there is an integer $t \geq 2$ so that $\operatorname{ord}(M,2^i) = 2\operatorname{ord}(M,2)$ for $2 \leq i \leq t$ together with $\operatorname{ord}(M,2^{t+i}) = 2^i \operatorname{ord}(M,4)$ for all $i \in \mathbb{N}$. □

In what follows, we will refer to the structure described in Proposition 1 as the *plateau phenomenon*. Such a plateau can be absent (p odd with $s = 1$, or the first case for $p = 2$), it can be at the beginning (p odd with $s \geq 2$), or it can occur after one step ($p = 2$ when $t \geq 2$ exists as described), but it cannot occur later on.

Proposition 1 is a reformulation of [14, Thms. 5.3 and 5.4], which are originally stated for $M \in \mathrm{GL}(2,\mathbb{Z})$. As one can easily check, the proofs do not depend on the dimension. Similar versions or special cases were also given in [13] and [41] (with focus on $\mathrm{SL}(2,\mathbb{Z})$-matrices), in [37] (for the order of algebraic integers), in [44] (for the Fibonacci sequence), in [15] (for linear quadratic recursions) and in [22] and [46] (for general linear recursions). Let us also mention that, based on the generalised Riemann hypothesis, Kurlberg has determined a lower bound on the order of unimodular matrices mod N for a density 1 subset of integers N in [31].

2.4. **Powers of integer matrices.** Consider a matrix $M \in \operatorname{Mat}(d,\mathbb{Z})$ with $d \geq 2$ and characteristic polynomial $P_M(z) = \det(z\mathbb{1} - M)$, which (following [46]) we write as

$$P_M(z) \;=\; z^d - c_1 z^{d-1} - c_2 z^{d-2} - \ldots - c_{d-1} z - c_d ,$$

so that $c_d = (-1)^{d+1}\det(M)$. Let us define a recursion by $u_0 = u_1 = \ldots = u_{d-2} = 0$ and $u_{d-1} = 1$ together with

$$u_m \;=\; \sum_{i=1}^{d} c_i u_{m-i} \;=\; c_1 u_{m-1} + c_2 u_{m-2} + \ldots + c_d u_{m-d} \tag{9}$$

for $m \geq d$. This results in an integer sequence. Moreover, when $c_d \neq 0$, we also define

$$u_m \;=\; c_d^{-1}\bigl(u_{m+d} - c_1 u_{m+d-1} - \ldots - c_{d-1} u_{m+1}\bigr)$$

for $m \leq -1$. In particular, since $d \geq 2$, one always has $u_{-1} = 1/c_d$ and $u_{-2} = -c_{d-1}/c_d^2$, while the explicit form of u_m with $m < -2$ depends on d. Note that the coefficients with negative index are rational numbers in general, unless $|c_d| = 1$.

The Cayley-Hamilton theorem together with (9) can be used to write down an explicit expansion of powers of the matrix M in terms of M^k with $0 \leq k \leq d-1$,

$$M^m \;=\; \sum_{\ell=0}^{d-1} \gamma_\ell^{(m)} M^\ell , \tag{10}$$

where the coefficients satisfy $\gamma_\ell^{(m)} = \delta_{m,\ell}$ (for $0 \le \ell, m \le d-1$) together with the recursion

$$\gamma_\ell^{(n+1)} = c_{d-\ell}\, \gamma_{d-1}^{(n)} + \gamma_{\ell-1}^{(n)}, \tag{11}$$

for $n \ge d-1$ and $0 \le \ell \le d-1$, where $\gamma_{-1}^{(n)} := 0$. In particular, $\gamma_\ell^{(d)} = c_{d-\ell}$. The coefficients are explicitly given as

$$\gamma_\ell^{(m)} \, = \, \sum_{i=0}^{\ell} c_{d-i} u_{m-\ell-1+i} \, = \, u_{m+d-\ell-1} \, - \sum_{i=1}^{d-\ell-1} c_{d-\ell-i} u_{m-1+i}\,, \tag{12}$$

where $m \ge d$ and the second expression follows from the first by (9). Formulas (10) and (12) can be proved by induction from $M^d = c_1 M^{d-1} + c_2 M^{d-2} + \ldots c_{d-1} M + c_d \mathbb{1}$. Eq. (10) holds for all $m \ge 0$ in this formulation.

When $\det(M) \ne 0$, the representation (12) also holds for $m < d$, as follows from checking the cases $0 \le m < d$ together with a separate induction argument for $m < 0$. In particular, one then has

$$\begin{aligned} M^{-1} = c_d u_{-2} \mathbb{1} + (c_{d-1} u_{-2} + c_d u_{-3}) M + (c_{d-2} u_{-2} + c_{d-1} u_{-3} + c_d u_{-4}) M^2 \\ + \ldots + (c_2 u_{-2} + c_3 u_{-3} + \ldots + c_d u_{-d}) M^{d-2} + u_{-1} M^{d-1}, \end{aligned}$$

which is again an integer matrix when $|c_d| = 1$.

2.5. **Results for $d = 2$.** Let us look at matrices from $\mathrm{Mat}(2,\mathbb{Z})$ more closely, and derive one important result by elementary means. Consider $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, set $D := \det(M)$, $T := \mathrm{tr}(M)$ and define the matrix gcd (or mgcd for short) as

$$\mathrm{mgcd}(M) := \gcd(b, c, d-a), \tag{13}$$

which is another invariant under $\mathrm{GL}(2,\mathbb{Z})$ conjugation. Its special role becomes clear from the following result, which is a reformulation of [12, Lemma 2 and Thm. 2]. This will lead to Corollary 2 below.

Lemma 1. *Two matrices $M, M' \in \mathrm{Mat}(2,\mathbb{Z})$ that are $\mathrm{GL}(2,\mathbb{Z})$-conjugate possess the same mgcd, as defined in Eq. (13). More generally, the reductions modulo n of M and M' are $\mathrm{GL}(2,\mathbb{Z}/n\mathbb{Z})$-conjugate for all $n \ge 2$ if and only if the two matrices share the same trace, determinant and mgcd.* □

Returning to matrix powers, formula (10) simplifies to

$$M^m \, = \, u_m M - D u_{m-1} \mathbb{1}, \tag{14}$$

where now $u_0 = 0$, $u_1 = 1$ and $u_{m+1} = T u_m - D u_{m-1}$ for $m \in \mathbb{N}$; see [12, Sec. 2.3] for details. Let $n \in \mathbb{N}$ and assume $\gcd(n, D) = 1$. This allows us to introduce

$$\kappa(n) \, := \, \text{period of } (u_m)_{m \ge 0} \bmod n$$

which is well-defined, as the sequence mod n is then indeed periodic without 'pre-tail'. Recall that $(u_m)_{m\ge 0}$ mod n must be periodic from a certain index on, as a result of Dirichlet's pigeon hole principle. Since D is a unit in $\mathbb{Z}/n\mathbb{Z}$, the recursion (14) can be reversed, and $(u_m)_{m\ge 0}$ mod n must thus be periodic, with $\kappa(n)$ being the smallest positive integer k such that $u_k = 0$ and $u_{k+1} = 1$ mod n.

One can now relate $\kappa(n)$ and $\mathrm{ord}(M, n)$ as follows, which provides an efficient way to calculate $\mathrm{ord}(M, n)$.

Proposition 2. *Let $M \in \mathrm{Mat}(2,\mathbb{Z})$ be fixed and let $(u_m)_{m\geq 0}$ be the corresponding recursive sequence from (9). If $n \geq 2$ is an integer with $\gcd(n,D)=1$, $\mathrm{ord}(M,n)$ divides $\kappa(n)$. Moreover, with $N_n := n/\gcd\bigl(n,\mathrm{mgcd}(M)\bigr)$, one has*

$$\mathrm{ord}(M,n) \;=\; \kappa(N_n)$$

whenever $N_n > 1$. In particular, this gives $\mathrm{ord}(M,n) = \kappa(n)$ whenever n and $\mathrm{mgcd}(M)$ are coprime.

In the remaining case, $N_n = 1$, the matrix satisfies $M \equiv \alpha\mathbb{1} \bmod n$ with some $\alpha \in (\mathbb{Z}/n\mathbb{Z})^{\times}$, so that $\mathrm{ord}(M,n)$ is the order of α modulo n.

Proof. If $M = \left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right)$, the iteration formula (14) implies that $M^m \equiv \mathbb{1} \bmod n$ if and only if

$$u_m a - D u_{m-1} \equiv 1\,,\quad u_m b \equiv 0\,,\quad u_m c \equiv 0\,,\quad \text{and}\quad u_m d - D u_{m-1} \equiv 1 \quad \bmod n,$$

so that also $u_m(a-d) \equiv 0 \bmod n$. Consequently, n divides $u_m b$, $u_m c$ and $u_m(a-d)$. This implies that u_m is divisible by $\frac{n}{\gcd(n,b)}$, $\frac{n}{\gcd(n,c)}$ and $\frac{n}{\gcd(n,a-d)}$, hence also by the least common multiple of these three numbers, which is the integer

$$N_n \;=\; \frac{n}{\gcd\bigl(n,\gcd(b,c,a-d)\bigr)} \;=\; \frac{n}{\gcd\bigl(n,\mathrm{mgcd}(M)\bigr)}.$$

Since $N_n|n$, we now also have $u_m a - D u_{m-1} \equiv 1 \bmod N_n$. When $u_m \equiv 0 \bmod N_n$, the recursion now gives $u_{m+1} \equiv T u_m - D u_{m-1} \equiv -D u_{m-1} \equiv 1 - u_n a \equiv 1 \bmod N_n$. Consequently, $M^m \equiv \mathbb{1} \bmod n$ is equivalent to $u_m \equiv 0$ and $u_{m+1} \equiv 1 \bmod N_n$. So, for $N_n > 1$, one has

$$\mathrm{ord}(M,n) \;=\; \kappa(N_n),$$

which is the period of the sequence $(u_m)_{m\geq 0}$ modulo N_n. Since $\kappa(N_n)$ clearly divides $\kappa(n)$, one finds $\mathrm{ord}(M,n)\,|\,\kappa(n)$.

Finally, when $N_n = 1$, one has $n|\,\mathrm{mgcd}(M)$, which implies $M \equiv \alpha\mathbb{1} \bmod n$, where we have $\alpha^2 \in (\mathbb{Z}/n\mathbb{Z})^{\times}$ due to $\gcd(n,D)=1$. Since this also implies $\alpha \in (\mathbb{Z}/n\mathbb{Z})^{\times}$, the last claim is clear. $\square$

Remark 1. Instead of the characteristic polynomial P_M, any other monic polynomial that annihilates M can be employed to derive a recursive sequence whose period is a multiple of the matrix order modulo n. For $n = p$ a prime, the unique minimal polynomial Q_M of M suggests itself to be chosen. For $d = 2$, Q_M has smaller degree than P_M precisely when $M = \alpha\mathbb{1}$, whence $\mathrm{mgcd}(M) = 0$ and $Q_M(z) = z - \alpha$. Consequently, $\mathrm{ord}(M,p)$ is then always equal to the order of α modulo p. $\Diamond$

3. **Orbit pretail structure of toral endomorphisms.** In this section, we look at the action of $M \in \mathrm{Mat}(d,\mathbb{Z})$ on a lattice L_n, with special emphasis on the structure of general endomorphisms. When M is not invertible, this manifests itself in the existence of non-trivial 'pretails' to periodic orbits, with rather characteristic properties. More precisely, given a periodic point y of M, a finite set of iterates (or suborbit)

$$O \;=\; \{x, Mx, M^2x, \ldots, M^n x = y\} \tag{15}$$

is called a *pretail* (of y) if y is the only periodic point of M in O.

3.1. **General structure.** Let M and n be fixed, and define $R = \mathbb{Z}/n\mathbb{Z}$. Let $\mathrm{per}(M)$ denote the set of periodic points on the lattice $\tilde{L}_n$, under the action of M mod n. Due to the linear structure of M, $\mathrm{per}(M)$ is an M-invariant submodule of $\tilde{L}_n$. It is the maximal submodule on which the restriction of M acts as an invertible map. The kernel $\ker(M^k) \subset \tilde{L}_n$ denotes the set of points that are mapped to 0 under M^k. One has $\ker(M^k) \subset \ker(M^{k+1})$ for all $k \geq 0$, and this chain stabilises, so that $\bigcup_{k\geq 0} \ker(M^k)$ is another well-defined and M-invariant submodule of $\tilde{L}_n$. This is then the maximal submodule on which the restriction of M acts as a nilpotent map. Note that $\mathrm{per}(M) \cap \ker(M^k) = \{0\}$ for all $k \geq 0$.

Consider an arbitrary $x \in \tilde{L}_n$ and its iteration under M. Since $|\tilde{L}_n| = n^d$ is finite, Dirichlet's pigeon hole principle implies that this orbit must return to one of its points. Consequently, every orbit is a cycle or turns into one after finitely many steps, i.e. it is eventually periodic. By elementary arguments, one then finds the following result.

Fact 1. *There are minimal integers $m \geq 0$ and $k \geq 1$ such that $M^{k+m} \equiv M^m$ mod n. The number k is the least common multiple of all cycle lengths on $\tilde{L}_n$, while m is the maximum of all pretail lengths. Clearly,* $\mathrm{per}(M) = \mathrm{Fix}(M^k)$. □

The lattice $\tilde{L}_n = R^d$ is a free R-module. The modules $\mathrm{per}(M)$ as well as $\mathrm{Fix}(M^j)$ and $\ker(M^j)$ for $j \geq 1$ are submodules of it, with $\mathrm{Fix}(M^i) \cap \ker(M^j) = \{0\}$ for all $i \geq 1$ and $j \geq 0$. Recalling some results on modules from [33, Ch. III] now leads to the following consequences.

Fact 2. *Let m and k be the integers from Fact 1. If $m \geq 1$, one has*

$$\{0\} \subsetneq \ker(M) \subsetneq \ker(M^2) \subsetneq \ldots \subsetneq \ker(M^m) \subseteq \tilde{L}_n,$$

while $\ker(M^{m+j}) = \ker(M^m)$ for all $j \geq 0$. Moreover, one has

$$\tilde{L}_n = \mathrm{Fix}(M^k) \oplus \ker(M^m),$$

which is the direct sum of two M-invariant submodules. Hence, $\mathrm{per}(M)$ and $\ker(M^m)$ are finite projective R-modules. □

In general, the projective summands need not be free. As a simple example, let us consider $\tilde{L}_6$ with $d = 1$ and $M = 2$. Here, $\mathrm{per}(M) = \{0, 2, 4\}$ covers the fixed point 0 and a 2-cycle, while $\ker(M) = \{0, 3\}$. Both are modules (and also principal ideals, hence generated by a single element) over $\mathbb{Z}/6\mathbb{Z}$, but do not have a basis, hence are not free. Nevertheless, one has $\mathbb{Z}/6\mathbb{Z} = \mathrm{per}(M) \oplus \ker(M)$. We will return to this question below.

3.2. **The pretail tree.** Consider the equation $M^\ell x = y$, with $\ell \in \mathbb{N}$, for some arbitrary, but fixed y in $\tilde{L}_n$. In general, this equation need not have any solution $x \in \tilde{L}_n$. On the other hand, when there is a solution $x \in \tilde{L}_n$, the set of all solutions is precisely $x + \ker(M^\ell)$, which has cardinality $|\ker(M^\ell)|$. If y is a periodic point, the first case can never occur, as there is then at least one predecessor of y. Due to the linearity of M, the structure of the set of pretails of a periodic point y must be the same for all $y \in \mathrm{per}(M)$ (note that there is precisely one predecessor of y in the periodic orbit, which might be y itself, while all points of the pretail except y are from the complement of the periodic orbit).

Consequently, we can study the pretail structure for $y = 0$. Let us thus combine all pretails of the fixed point 0 into a (directed) graph, called the *pretail graph* from now on; see [47] for general background on graph theory. A single pretail is called

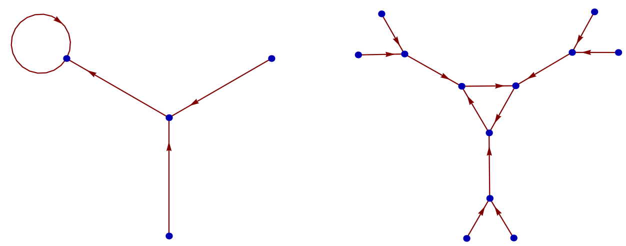

FIGURE 1. The directed graph for the action of $M = \left(\begin{smallmatrix} 4 & 0 \\ 1 & 4 \end{smallmatrix}\right)$ on the lattice $\tilde{L}_6$. The matrix has three fixed points and two 3-cycles (shown once each), while each periodic point has the same binary tree of height 2 as pretail tree.

maximal when it is not contained in any longer one. By construction, there can be no cycle in the pretail graph, while $y = 0$ plays a special role. Viewing each maximal pretail of 0 as an 'ancestral line', we see that this approach defines a rooted tree with root 0. Note that an isomorphic tree also 'sits' at every periodic point y.

Corollary 1. *Every periodic point of M on $\tilde{L}_n$ has a directed pretail graph that is isomorphic to that of the fixed point 0. Up to graph isomorphism, it thus suffices to analyse the latter. By reversing the direction, it is a rooted tree with root 0. This tree is trivial if and only if M is invertible on $\tilde{L}_n$.* □

Two illustrative examples are shown in Figures 1 and 2. Each M defines a unique (rooted) pretail tree on a given lattice. If v_i denotes the number of nodes (or vertices) of this tree with graph distance i from the root, we have $v_0 = 1$ and

$$\left|\ker(M^j)\right| \;=\; v_0 + v_1 + \cdots + v_j \tag{16}$$

for all $j \geq 0$, where $v_i = 0$ for all i larger than the maximal pretail length. Also, one has

$$v_j \;=\; \left|\ker(M^j) \setminus \ker(M^{j-1})\right| \;=\; \left|\ker(M^j)\right| - \left|\ker(M^{j-1})\right| \tag{17}$$

for $j \geq 1$, where the second equality follows from the submodule property. Recall that terminal nodes of a rooted tree (excluding the root in the trivial tree) are called *leaves*. With this definition, the total number of leaves on $\tilde{L}_n$ is $|\tilde{L}_n \setminus M\tilde{L}_n|$. For $i \in \mathbb{N}$, define w_i to be the number of nodes with graph distance i from the root that fail to be leaves, and complete this with $w_0 = 0$ for the trivial tree and $w_0 = 1$ otherwise. It is clear that this leads to

$$v_{i+1} \;=\; w_0\bigl(w_i \left|\ker(M)\right| - \delta_{i,0}\bigr), \tag{18}$$

via the number of solutions to $Mx = 0$ and the special role of the root, and inductively to

$$\left|\ker(M^{i+1})\right| \;=\; (w_0 + w_1 + \cdots + w_i)\left|\ker(M)\right| \tag{19}$$

whenever $w_0 = 1$, with both relations being valid for all $i \geq 0$.

Lemma 2. *If M acts on $\tilde{L}_n$, its uniquely defined pretail tree of the fixed point 0 has height $m \geq 0$, and the following properties are equivalent.*

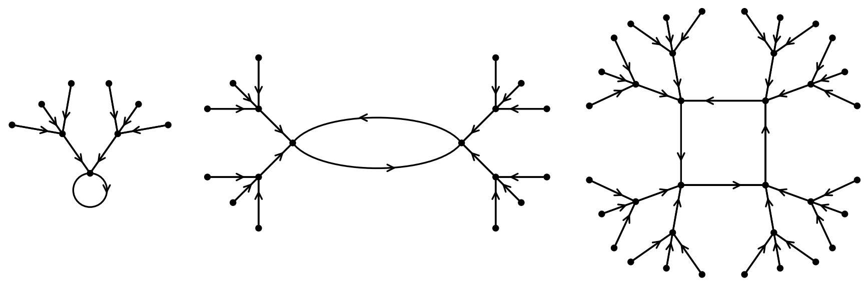

FIGURE 2. The directed graph for the action of $M = \left(\begin{smallmatrix} 0 & 12 \\ 1 & 6 \end{smallmatrix}\right)$ on the lattice $\tilde{L}_{15}$. The only fixed point of M is 0, while it has two 2-cycles and five 4-cycles (shown once each only). All pretail trees have the same height.

(i) *All maximal pretails have the same length* m*;*
(ii) *One has* $v_i = w_i \neq 0$ *for all* $0 \leq i < m$ *and* $w_i = 0$ *for* $i \geq m$*;*
(iii) *One has* $|\ker(M^{i+1})| = |\ker(M)|\,|\ker(M^i)| = |\ker(M)|^{i+1}$ *for all* $0 \leq i < m$*, together with* $|\ker(M^{m+j})| = |\ker(M^m)|$ *for all* $j \geq 0$*.*

In particular, m *is the integer from Fact 1.*

Proof. By Corollary 1, the pretail tree is trivial (hence $w_0 = m = 0$) if and only if M is invertible on $\tilde{L}_n$. Since all claims are clear for this case, let us now assume that M is not invertible on $\tilde{L}_n$.

All maximal pretails have the same length if and only if all leaves of the pretail tree of 0 have the same graph distance from the root 0. Clearly, the latter must be the height m of the tree. When M is not invertible on $\tilde{L}_n$, the tree is not the trivial one, so $m \geq 1$. The equivalence of (i) and (ii) is then clear, since both conditions characterise the fact that all leaves have distance m from the root.

The implication (ii) $\Rightarrow$ (iii) can be seen as follows. The first claim is trivial for $i = 0$, as $\ker(M^0) = \ker(\mathbb{1}) = \{0\}$. Assuming (ii), Eqns. (17) – (19) yield

$$\begin{aligned} \left|\ker(M^{i+1})\right| &= \left|\ker(M^i)\right| + w_i \left|\ker(M)\right| \\ &= \left|\ker(M^i)\right| + \big(|\ker M^i| - |\ker M^{i-1}|\big)\left|\ker M\right| \end{aligned}$$

for $1 \leq i < m$, which (inductively) reduces to the first condition of (iii), while the second is clear from the meaning of m.

Conversely, the second condition of (iii) means $w_{m+j} = 0$ for all $j \geq 0$, while the first condition, together with Eqns. (18) and (19), successively gives $v_i = w_i$ for all $0 \leq i < m$. □

On the lattice $\tilde{L}_{p^r}$, when $|\ker(M)| = p$, one can say more.

Proposition 3. *Consider the action of* M *on the lattice* $\tilde{L}_{p^r}$*. When* $|\ker(M)| = p$*, one has* $|\ker(M^i)| = p^{\min(i,m)}$ *for all* $i \geq 0$*, where* m *is the integer from Fact 1 for* $n = p^r$*. This means* $v_i = p^{i-1}(p-1)$ *for* $1 \leq i \leq m$*, and all maximal pretails share the same length* m*.*

Proof. By assumption, M is not invertible, and the last claim is obvious from Lemma 2 in conjunction with Eq. (16). We thus need to prove the formula for the cardinality of $\ker(M^i)$ for arbitrary $i \geq 0$.

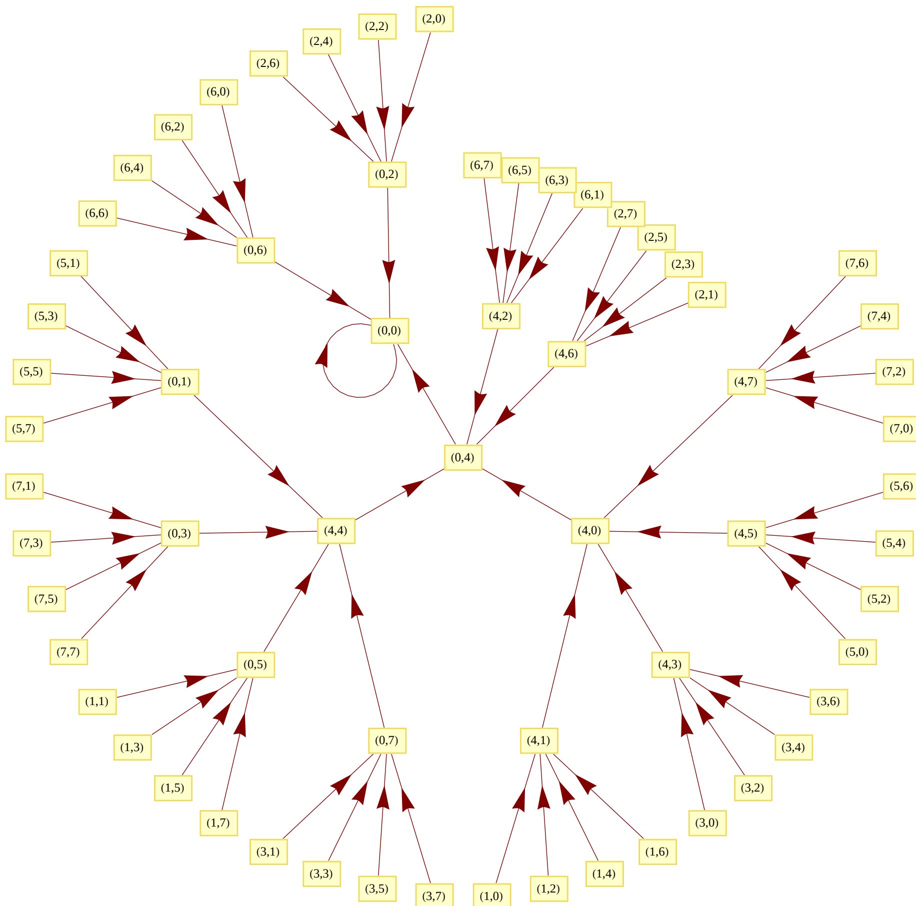

FIGURE 3. The pretail graph for Example 1, with coordinates for the action of the matrix M on $\tilde{L}_8$, where it is nilpotent with nil-degree 4.

Since 0 is a fixed point of M, we clearly have $v_0 = 1$ and $v_1 = p - 1$, together with the inequality $0 \le w_1 \le p - 1$. If $w_1 = 0$, we have $m = 1$ and we are done. Otherwise, $\ker(M) \subsetneq \ker(M^2)$, hence $|\ker(M^2)| = p^j$ for some $j \ge 2$, as the kernel is a subgroup of our lattice (which has cardinality p^{rd}). This forces $w_1 = p - 1$ and $j = 2$. More generally, when $|\ker(M^i)| = p^i$ for some $1 \le i < m$, one cannot have $w_i = 0$, so that $|\ker(M^{i+1})| = p^{i+j}$ for some $j \ge 1$. Since now $0 \le w_i \le p^{i-1}(p-1)$, the only possibility is $j = 1$ together with $w_i = p^{i-1}(p - 1)$. This argument can be repeated inductively until $i = m$ is reached, with $|\ker(M^{m+j})| = |\ker(M^m)|$ for all $j \ge 0$. $\square$

In general, the maximal pretails need not share the same length, which means that we still have to extend our point of view.

Example 1. Consider the matrix $M = \left(\begin{smallmatrix}4&4\\1&4\end{smallmatrix}\right)$ on $\tilde{L}_8$, where it is nilpotent (mod 8) with nil-degree 4. Since $\mathrm{card}(\ker(M)) = 4$, Proposition 3 does not apply. The (directed) pretail graph spans the entire lattice and is shown in Figure 3, together with the loop at 0 that marks this point as the root of the tree (which emerges from the figure by removing this loop and reversing all arrows). ◊

So far, we have looked at a single lattice $\tilde{L}_n$. However, any given matrix M immediately defines a *sequence* of trees via $\tilde{L}_n$ with $n \in \mathbb{N}$. When $d = 2$, the result of [12, Thm. 2] implies the following result.

Corollary 2. *Let $M, M' \in \mathrm{Mat}(2, \mathbb{Z})$ be two matrices with the same trace, determinant and* mgcd*. Then, they have the same sequence of pretail trees on the lattices $\tilde{L}_n$.* □

3.3. **Decomposition on $\tilde{L}_{p^r}$.** When the integers u, v are coprime, one has $L_{uv} \simeq L_u \oplus L_v$, wherefore the action on L_n with $n \in \mathbb{N}$ is completely determined by that on L_{p^r}, for all $p^r || n$. In particular, the pretail orbit structure on an arbitrary L_n can be derived from that on the sublattices associated with the factors in the prime factorisation of n.

Define $R_r = \mathbb{Z}/p^r\mathbb{Z}$, which is a *local* ring, with unique maximal ideal $(p) = pR_r$. The latter contains all zero divisors. By [33, Thm. X.4.4], we then know that the two projective modules $\mathrm{per}(M)$ and $\ker(M^k)$ of Fact 2 are *free*, so each has a basis. Consequently, one knows that the linear map on $\tilde{L}_{p^r}$ defined by M induces unique linear maps on $\mathrm{Fix}(M^{k(r)})$ and $\ker(M^{m(r)})$, and M is conjugate to the direct sum of these maps, compare [1, Prop. 4.3.28]. Each of the latter, in turn, admits a matrix representation with respect to any chosen basis of the corresponding submodule. Different choices of bases lead to conjugate matrices, by an application of [1, Prop. 4.3.23].

Corollary 3. *On $\tilde{L}_{p^r}$, M is similar to a block diagonal matrix $\left(\begin{smallmatrix} A & 0 \\ 0 & B \end{smallmatrix}\right)$ over R_r, where A is invertible and B is nilpotent, the latter of nil-degree $n(B)$ say. The block matrices A and B are unique up to similarity. The direct sum from Fact 2 now reads*

$$\tilde{L}_{p^r} = \mathrm{Fix}(M^{\mathrm{ord}(A,p^r)}) \oplus \ker(M^{n(B)}),$$

where the concrete form of the exponents k and m of Fact 2 follows from the block diagonal structure of M chosen. Here, $\mathrm{Fix}(M^{\mathrm{ord}(A,p^r)}) \simeq R_r^{d'}$ and $\ker(M^{n(B)}) \simeq R_r^{d-d'}$, where one has $d' = \mathrm{rank}\,(\mathrm{per}(M)) \le d$.

Furthermore, d' is independent of r. When comparing the above objects as modules over the ring R_s for different s, one has

$$\mathrm{rank}_1(\mathrm{per}_1(M)) = \mathrm{rank}_r(\mathrm{per}_r(M)) = d' \quad \textit{and}$$

$$\mathrm{rank}_1(\ker_1(M^{m(1)})) = \mathrm{rank}_r(\ker_r(M^{m(r)})) = d - d',$$

where an index s at per, ker *or* rank *refers to R_s as the underlying ring.*

Proof. The diagonal block-matrix structure is clear from [1, Props. 4.3.28 and 4.3.23], while the isomorphism claim follows from [33, Cor. III.4.3].

For the last claim, observe that A and B can be viewed as integer matrices acting on $R_r^{d'}$ and $R_r^{d-d'}$, respectively. Here, $B^s = 0 \bmod p^r$ for some $s \in \mathbb{N}$ and $\gcd(\det(A), p) = 1$, because A is invertible mod p^r and $\det(A)$ must be a unit in R_r. But this means that the reduction of $A \bmod p$ is also invertible over $R_1 = \mathbb{Z}/p\mathbb{Z}$, while the reduction of $B \bmod p$ is still nilpotent. Consequently, these reductions provide the blocks for the direct sum over $\tilde{L}_p$, and the claim is obvious. □

Since two free modules of the same rank are isomorphic [33, Cor. III.4.3], we also have the following consequence.

Corollary 4. *One has the following isomorphisms of R_1-modules (as $\mathbb{F}_p$-vector spaces),*

$$\mathrm{per}_r(M)/p\ \mathrm{per}_r(M) \simeq \mathrm{per}_1(M) \quad \textit{and} \quad \ker_r(M^{m(r)})/p \ker_r(M^{m(r)}) \simeq \ker_1^{(d)}(M^{m(1)}).$$

This implies

$$\big|\,\mathrm{per}_r(M)\big| = p^{rd'} = \big|\,\mathrm{per}_1(M)\big|^r \quad \textit{and} \quad \big|\ker_r(M^{m(r)})\big| = p^{r(d-d')} = \big|\ker_1(M^{m(1)})\big|^r$$

for the cardinalities of the finite modules. □

At this point, it is reasonable to link the properties of M on $\tilde{L}_{p^r}$ to its minimal polynomial over $\mathbb{F}_p$.

Lemma 3. *If M is similar mod p to the block diagonal matrix of Corollary 3, its minimal polynomial over $\mathbb{F}_p$ is $\mu_M(x) = x^s f(x)$, where f is a monic polynomial of order k over $\mathbb{F}_p$ with $f(0) \neq 0$. When M is invertible, one has $s = 0$ and $k = \gcd\{\ell \in \mathbb{N} \mid M^\ell \equiv \mathbb{1} \bmod p\}$. When M is nilpotent, one has $f = 1$ together with $s = \gcd\{t \in \mathbb{N} \mid M^t \equiv 0 \bmod p\}$. In all remaining cases, s and k are the smallest positive integers such that $B^s \equiv 0$ and $A^k \equiv \mathbb{1} \bmod p$.*

Proof. Recall from [34, Def. 3.3.2] that the order of a polynomial $f \in \mathbb{F}_p[x]$ with $f(0) \neq 0$, denoted by $\mathrm{ord}(f,p)$, is the smallest integer $\ell > 0$ such that $f(x)|(x^\ell - 1)$. When M is invertible and k as claimed, the polynomial $x^k - 1$ annihilates M. Since $\mu_M(0) \neq 0$ in our case, we have $\mu_M = f$ with $f(x)|(x^k - 1)$, so that $\mathrm{ord}(f,p)|k$ by [34, Lemma 3.3.6]. By construction, k is also the minimal positive integer such that $x^k - 1$ annihilates M, hence $k = \mathrm{ord}(f,p)$.

When M is nilpotent, the claim is obvious, because 0 is then the only possible root of the minimal polynomial over $\mathbb{F}_p$, as all other elements of the splitting field of f are units.

In all remaining cases, M is similar to $A \oplus B$ with A invertible and B nilpotent, by Corollary 3. We thus know that $\mu_M(x)|x^s(x^k - 1)$ with s and k as claimed, since the latter annihilates both A and B. Observe that $B^s(B^k - \mathbb{1}) \equiv 0 \bmod p$ means $B^{k+s} \equiv B^s \bmod p$. Since B is nilpotent, its powers cannot return to a non-zero matrix, hence $B^s \equiv 0 \mod p$. Similarly, $A^{s+k} \equiv A^s \bmod p$ is equivalent with $A^k \equiv \mathbb{1} \bmod p$, as A is invertible. This shows that we must indeed have $\mu_M(x) = x^s f(x)$ with $\mathrm{ord}(f,p) = k$. □

3.4. **Classification on $\tilde{L}_p$.** When we consider $n = p$, we can go one step further, because $\mathbb{F}_p$ is a field and one can classify nilpotent matrices via their Jordan normal form. This follows from the observation that 0 is the only possible eigenvalue. Recall that an *elementary shift matrix* is an upper triangular matrix with entries 1 on the upper super-diagonal and 0 everywhere else (this includes the 0-matrix in one dimension). An elementary shift matrix is nilpotent, with nil-degree equal to its dimension. The following result is now a standard consequence of the Jordan normal form over fields [27, 33].

Fact 3. *The nilpotent matrices in $\mathrm{Mat}(d, \mathbb{F}_p)$ are conjugate to block-diagonal matrices, where each block is an elementary shift matrix.* □

Some of this structure survives also for general n. For instance, the 0-matrix in dimension $d \geq 1$ leads to the regular $(n^d - 1)$-star as its pretail tree on $\tilde{L}_n$. When $d \geq 2$, the d-dimensional elementary shift matrix, on $\tilde{L}_n$, results in a semi-regular tree with $w_0 = 1$, $w_1 = n - 1$ and $w_i = n$ for $2 \leq i \leq d - 1$, while $w_j = 0$

for all $j \geq d$. These trees have the property that all maximal pretails share the same length, which is the nil-degree of the matrix. One can now go through all possible block-diagonal combinations of such elementary shift matrices. This is a combinatorial problem and gives the possible pretail trees over $\mathbb{F}_p$.

As already suggested by Proposition 3, the structure of $\ker(M)$ plays an important role for the structure of the pretail tree. Together with the linearity of M, it constrains the class of trees that are isomorphic to the pretail tree of some integer matrix. A more detailed analysis is contained in [36].

4. **Symmetry and reversibility.** Reversibility is an important concept in dynamics, compare [39] and references therein for background, and [20] for an early study in continuous dynamics. Here, we focus on discrete dynamics, as induced by toral auto- and endomorphisms.

A matrix M is called *reversible*, within a given or specified matrix group $\mathcal{G}$, if it is conjugate to its inverse within $\mathcal{G}$. Clearly, this is only of interest when $M^2 \neq \mathbb{1}$. To put this into perspective, one usually defines

$$\mathcal{S}(M) = \{G \in \mathcal{G} \mid GMG^{-1} = M\} \quad \text{and} \quad \mathcal{R}(M) = \{G \in \mathcal{G} \mid GMG^{-1} = M^{\pm 1}\}$$

as the *symmetry* and *reversing symmetry* groups of M; see [11] and references therein for background and [9, 10] for examples in our present context. In particular, one always has $\mathcal{R}(M) = \mathcal{S}(M)$ when $M^2 = \mathbb{1}$ or when M is not reversible, while $\mathcal{R}(M)$ is an extension of $\mathcal{S}(M)$ of index 2 otherwise.

Note that a nilpotent matrix M (or a matrix with nilpotent summand, as in Corollary 3) cannot be reversible in this sense. However, they can still possess interesting and revealing symmetry groups, although it is more natural to look at the *ring* of matrices that commute with M in this case.

Example 2. Reconsider the matrix $M = \left(\begin{smallmatrix} 4 & 4 \\ 1 & 4 \end{smallmatrix}\right)$ from Example 1, and its action on $\tilde{L}_8$. Clearly, M commutes with every element of the ring $\mathbb{Z}/8\mathbb{Z}\,[M]$, which contains 64 elements. This follows from the existence of a cyclic vector, but can also be checked by a simple direct calculation. Consequently, the symmetry group (in our above sense) is the intersection of this ring with $\mathrm{GL}(8, \mathbb{Z}/8\mathbb{Z})$, which results in

$$\mathcal{S}(M) \, = \, \left\langle \left(\begin{smallmatrix} 1 & 4 \\ 1 & 1 \end{smallmatrix}\right), 3{\cdot}\mathbb{1}, 5{\cdot}\mathbb{1} \right\rangle \, \simeq \, C_8 \times C_2 \times C_2 ,$$

which is an Abelian group of order 32. The matrices in $\mathcal{S}(M)$ have either determinant 1 or 5, with $\{A \in \mathcal{S}(M) \mid \det(A) = 1\} \simeq C_4 \times C_2 \times C_2$.

One can now study the action of $\mathcal{S}(M)$ on the pretail graph of Figure 3, which actually explains all its symmetries. $\Diamond$

In what follows, we derive certain general properties, where we focus on the reversing symmetry group, with invertible matrices M in mind.

4.1. **Reversibility of $\mathrm{SL}(2,\mathbb{Z})$-matrices mod n.** Recall the matrix mgcd from Eq. (13), which is a conjugation invariant. It can be used to solve the reversibility at hand as follows.

Theorem 1. *Let $M \in \mathrm{SL}(2,\mathbb{Z})$ and $n \in \mathbb{N}$ be arbitrary. Then, the reduction of M mod n is conjugate to its inverse within the group $\mathrm{GL}(2, \mathbb{Z}/n\mathbb{Z})$. The action mod 1 of any $M \in \mathrm{SL}(2,\mathbb{Z})$ on L_n is thus reversible for all $n \in \mathbb{N}$.*

Moreover, if $M \in \mathrm{SL}(2,\mathbb{Z})$ has $\mathrm{mgcd}(M) = r \neq 0$, its reduction mod n, for every $n \in \mathbb{N}$, possesses an involutory reversor.

Proof. When $M \in \mathrm{SL}(2,\mathbb{Z})$, also its inverse is in $\mathrm{SL}(2,\mathbb{Z})$, and M and M^{-1} share the same determinant and trace. Moreover, they also have the same mgcd, so that the first claim follows from [12, Thm. 2] (or from Lemma 1). This immediately implies, for all $n \in \mathbb{N}$, the reversibility of the action mod n of M on the lattice $\tilde{L}_n$, so that the statement on the equivalent action of M mod 1 on L_n is clear.

Now, let $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}(2,\mathbb{Z})$, so that $M^{-1} = \left(\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right)$, and M and M^{-1} share the same determinant (1), trace $(a+d)$ and mgcd (r). Assume $r \neq 0$, let $n \geq 2$ be fixed and consider the matrices mod n. Recall the normal forms

$$N(M) = \begin{pmatrix} a & \frac{bc}{r} \\ r & d \end{pmatrix} \quad \text{and} \quad N(M^{-1}) = \begin{pmatrix} d & \frac{bc}{r} \\ r & a \end{pmatrix},$$

as defined in the proof of [12, Prop. 6], and note that they are not inverses of each other. However, by [12, Prop. 5], there is some matrix $P_n \in \mathrm{GL}(2,\mathbb{Z}/n\mathbb{Z})$ with $M = P_n N(M) P_n^{-1}$, hence we also have $M^{-1} = P_n \big(N(M)\big)^{-1} P_n^{-1}$. Observe next that

$$\big(N(M)\big)^{-1} = \begin{pmatrix} d & -\frac{bc}{r} \\ -r & a \end{pmatrix} = C \begin{pmatrix} d & \frac{bc}{r} \\ r & a \end{pmatrix} C^{-1} = C N(M^{-1}) C^{-1},$$

where $C = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ is an involution. On the other hand, $N(M)$ and $N(M^{-1})$ satisfy the assumptions of [12, Prop. 6], so that

$$N(M^{-1}) = A N(M) A^{-1} \quad \text{with} \quad A = \begin{pmatrix} 1 & \frac{d-a}{r} \\ 0 & 1 \end{pmatrix},$$

where we globally have $A = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ whenever $d = a$ in the original matrix M. Together with the previous observation, this implies $\big(N(M)\big)^{-1} = (CA) N(M) (CA)^{-1}$ where

$$CA = \begin{pmatrix} 1 & \frac{d-a}{r} \\ 0 & -1 \end{pmatrix}$$

is an involution. Putting everything together, we have

$$M^{-1} = \big(P_n (CA) P_n^{-1}\big) M \big(P_n (CA) P_n^{-1}\big)^{-1},$$

which is the claimed conjugacy by an involution (which depends on n in general). $\square$

Note that the matrix M in Theorem 1 need not be reversible in $\mathrm{GL}(2,\mathbb{Z})$, as the example $M = \left(\begin{smallmatrix} 4 & 9 \\ 7 & 16 \end{smallmatrix}\right)$ from [9, Ex. 2] shows. Nevertheless, for any $M \in \mathrm{SL}(2,\mathbb{Z})$ with $\mathrm{mgcd}(M) \neq 0$ and $n \geq 2$, the (finite) reversing symmetry group of M within $\mathrm{GL}(2,\mathbb{Z}/n\mathbb{Z})$ is always of the form $\mathcal{R}(M) = \mathcal{S}(M) \rtimes C_2$, with C_2 being generated by the involutory reversor. The structure of $\mathcal{S}(M)$ remains to be determined.

In the formulation of Theorem 1, we have focused on matrices $M \in \mathrm{SL}(2,\mathbb{Z})$ because the condition $\mathrm{tr}(M) = \mathrm{tr}(M^{-1})$ for a matrix M with $\det(M) = -1$ forces $\mathrm{tr}(M) = 0$, which means that M is itself an involution (and thus trivially reversible in $\mathrm{GL}(2,\mathbb{Z})$). More interesting (beyond Theorem 1) is the question which matrices $M \in \mathrm{Mat}(2,\mathbb{Z})$, when considered mod n for some $n \in \mathbb{N}$, are reversible in $\mathrm{GL}(2,\mathbb{Z}/n\mathbb{Z})$. Let us begin with $n = p$ being a prime, where $\mathbb{Z}/p\mathbb{Z} \simeq \mathbb{F}_p$ is the finite field with p elements.

4.2. **Reversibility in $\mathrm{GL}(2,\mathbb{F}_p)$.** Let us consider the symmetry and reversing symmetry group of an element of $\mathrm{GL}(2,\mathbb{F}_p)$ with p prime, the latter being a group of order

$$|\mathrm{GL}(2,\mathbb{F}_p)| \;=\; (p^2-1)(p^2-p) \;=\; p(p-1)^2(p+1),$$

compare Eq. (3). For our further discussion, it is better to distinguish $p = 2$ from the odd primes. For convenience, we summarise the findings also in Table 4.2.

Example 3. For $p = 2$, one has $\mathrm{GL}(2, \mathbb{F}_2) = \mathrm{SL}(2, \mathbb{F}_2) \simeq D_3$, the latter denoting the dihedral group of order 6. There are now three conjugacy classes to consider, which may be represented by the matrices $\mathbb{1}$, the involution $R = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, and the matrix $M = \left(\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ of order 3. The corresponding cycle structure on L_2 is encapsulated in the generating polynomials $Z_2(t)$. They read

$$(1-t)^4\,, \quad (1-t)^2(1-t^2) \quad \text{and} \quad (1-t)(1-t^3),$$

respectively, and apply to entire conjugacy classes of matrices.

For the (reversing) symmetry groups, one clearly has $\mathcal{R}(\mathbb{1}) = \mathcal{S}(\mathbb{1}) = \mathrm{GL}(2, \mathbb{F}_2)$, while $\mathcal{R}(R) = \mathcal{S}(R) = \langle R \rangle \simeq C_2$. The only nontrivial reversing symmetry group occurs in the third case, where $\mathcal{S}(M) = \langle M \rangle \simeq C_3$. Since $RMR = M^2 = M^{-1}$, one has $\mathcal{R}(M) = \mathrm{GL}(2, \mathbb{F}_2) \simeq C_3 \rtimes C_2$. So, all elements of $\mathrm{GL}(2, \mathbb{F}_2)$ are reversible, though only M and M^2 are nontrivial in this respect. ♢

For p an odd prime, one can use the normal forms for $\mathrm{GL}(2, \mathbb{F}_p)$, see [33, Ch. XVIII.12], to formulate the results; compare Table 4.2. We summarise the reversibility and orbit structure here, but omit proofs whenever they emerge from straight-forward calculations.

I. The first type of conjugacy class is represented by matrices $M = a\mathbb{1}$ with $a \in \mathbb{F}_p^\times \simeq C_{p-1}$. The order of M coincides with the order of a mod p, $\mathrm{ord}(a, p)$, which divides $p - 1$. One clearly has $\mathcal{R}(M) = \mathcal{S}(M) = \mathrm{GL}(2, \mathbb{F}_p)$ in this case, either because $a^2 = 1$ (so that $M = M^{-1}$) or because $a^2 \neq 1$ (so that no reversors are possible). The corresponding orbit structure on L_p comprises one fixed point ($x = 0$) together with $\frac{p^2-1}{\mathrm{ord}(a,p)}$ orbits of length $\mathrm{ord}(a, p)$. The non-trivial orbits starting from some $x \neq 0$ must all be of this form, as x gets multiplied by a under the action of M and returns to itself precisely when $a^k = 1$, which first happens for $k = \mathrm{ord}(a, p)$.

II. The next type of conjugacy class is represented by matrices $M = \left(\begin{smallmatrix} a & 1 \\ 0 & a \end{smallmatrix}\right)$ with $a \in \mathbb{F}_p^\times$. Its symmetry group is given by

$$\mathcal{S}(M) \,=\, \bigl\{ \left(\begin{smallmatrix} \alpha & \beta \\ 0 & \alpha \end{smallmatrix}\right) \bigm| \alpha \in \mathbb{F}_p^\times,\, \beta \in \mathbb{F}_p \bigr\} \,\simeq\, C_p \times C_{p-1}\,,$$

which is Abelian. As generators of the cyclic groups, one can choose $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, which has order p in $\mathrm{GL}(2, \mathbb{F}_p)$, and $\gamma\mathbb{1}$, with γ a generating element of $\mathbb{F}_p^\times$. The reversible cases are precisely the ones with $a^2 = 1$ in $\mathbb{F}_p$, hence with $\det(M) = 1$. Here, $R = \mathrm{diag}(1, -1)$ is a possible choice for the (involutory) reversor, so that we obtain $\mathcal{R}(M) = \mathcal{S}(M) \rtimes \langle R \rangle \simeq (C_p \times C_{p-1}) \rtimes C_2$.

A matrix M of type II (in its normal form as in Table 4.2) satisfies

$$M^k = \begin{pmatrix} a^k & ka^{k-1} \\ 0 & a^k \end{pmatrix} \qquad \text{for } k \geq 0\,,$$

whence a point $(x, 0)$ with $x \neq 0$ is fixed by M^k if and only if $k = \mathrm{ord}(a, p)$, and a point (x, y) with $xy \neq 0$ if and only if $p|k$ and $\mathrm{ord}(a, p)|k$. Since $\mathrm{ord}(a, p)|(p - 1)$, one has $\mathrm{lcm}(p, \mathrm{ord}(a, p)) = 1$, wherefore this gives $\frac{p-1}{\mathrm{ord}(a,p)}$ orbits of length $p - 1$ and $\frac{p\cdot(p-1)}{p\cdot\mathrm{ord}(a,p)} = \frac{p-1}{\mathrm{ord}(a,p)}$ orbits of length $p\,\mathrm{ord}(a, p)$ in total.

III. The third type of conjugacy class is represented by $M = \mathrm{diag}(a, b)$ with $a, b \in \mathbb{F}_p^\times$ and $a \neq b$. This results in $\mathcal{S}(M) = \{\mathrm{diag}(\alpha, \beta) \mid \alpha, \beta \in \mathbb{F}_p^\times\} \simeq C_{p-1}^2$.

TABLE 1. Summary of conjugacy structure for $\mathrm{GL}(2, \mathbb{F}_p)$ via normal forms. Note that class III is absent for $p = 2$. The second possibility for $\mathcal{R}(M)$ always applies when $\det(M) = 1$. Only non-trivial orbits are counted.

class	I	II	III	IV
normal form of matrix class	$a\mathbb{1}$ $a \in \mathbb{F}_p^\times$	$\left(\begin{smallmatrix} a & 1 \\ 0 & a \end{smallmatrix}\right)$ $a \in \mathbb{F}_p^\times$	$\left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right)$ $a \neq b \in \mathbb{F}_p^\times$	$\left(\begin{smallmatrix} 0 & -D \\ 1 & T \end{smallmatrix}\right)$ $z^2 - Tz + D$ irred.
min. polynomial	$(z-a)$	$(z-a)^2$	$(z-a)(z-b)$	$z^2 - Tz + D$
size of class	1	$p^2 - 1$	$p^2 + p$	$p^2 - p$
no. of classes	$p-1$	$p-1$	$\frac{1}{2}(p-1)(p-2)$	$\frac{1}{2}p(p-1)$
$\mathcal{S}(M)$	$\mathrm{GL}(2, \mathbb{F}_p)$	$C_p \times C_{p-1}$	$C_{p-1} \times C_{p-1}$	C_{p^2-1}
$\mathcal{R}(M)$	$\mathcal{S}(M)$	$\mathcal{S}(M)$ or $\mathcal{S}(M) \rtimes C_2$	$\mathcal{S}(M)$ or $\mathcal{S}(M) \rtimes C_2$	$\mathcal{S}(M)$ or $\mathcal{S}(M) \rtimes C_2$
orbit length	$\mathrm{ord}(a, p)$	see text	see text	$\mathrm{ord}(\chi_M, p)$
orbit count	$\frac{p^2-1}{\mathrm{ord}(a,p)}$	see text	see text	$\frac{p^2-1}{\mathrm{ord}(\chi_M,p)}$

The condition for reversibility leads either to $a^2 = b^2 = 1$, hence to $b = -a$, or to $ab = 1$. In the former case, M itself is an involution, so that $\mathcal{R}(M) = \mathcal{S}(M)$ is once again the trivial case, while $\det(M) = ab = 1$ leads to genuine reversibility, with involutory reversor $R = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ and hence to $\mathcal{R}(M) = \mathcal{S}(M) \rtimes C_2$.

For a type III matrix, one has $M^k (x, y)^t = (a^k x, b^k y)^t$, so each of the $p-1$ non-zero points $(x, 0)^t$ is fixed by $M^{\mathrm{ord}(a,p)}$; analogously, each of the $p-1$ non-zero points $(0, y)^t$ is fixed by $M^{\mathrm{ord}(b,p)}$. The remaining points that are non-zero in both coordinates have period $\mathrm{lcm}(\mathrm{ord}(a, p), \mathrm{ord}(b, p))$. In summary, this gives one fixed point, $\frac{p-1}{\mathrm{ord}(a,p)}$ orbits of length $\mathrm{ord}(a, p)$, $\frac{p-1}{\mathrm{ord}(b,p)}$ orbits of length $\mathrm{ord}(b, p)$, and $\frac{(p-1)^2}{\mathrm{lcm}(\mathrm{ord}(a,p),\mathrm{ord}(b,p))}$ orbits of length $\mathrm{lcm}(\mathrm{ord}(a, p), \mathrm{ord}(b, p))$.

IV. Finally, the last type of conjugacy class can be represented by companion matrices of the form $\left(\begin{smallmatrix} 0 & -D \\ 1 & T \end{smallmatrix}\right)$ with the condition that the characteristic polynomial $z^2 - Tz + D$ is irreducible over $\mathbb{F}_p$. The determinant and the trace satisfy $D = \eta\eta'$ and $T = \eta + \eta'$, where η and η' are not in $\mathbb{F}_p$, but distinct elements of the splitting field of the polynomial, which can be identified with $\mathbb{F}_{p^2}$. One consequence is that $1 + D \pm T = (1 \pm \eta)(1 \pm \eta') \neq 0$.

The symmetry group is $\mathcal{S}(M) = \{\alpha\mathbb{1} + \gamma M \mid \alpha, \gamma \in \mathbb{F}_p, \text{ not both } 0\}$, which is an Abelian group with $p^2 - 1$ elements. The order follows from the observation that $\det(\alpha\mathbb{1} + \gamma M) = (\alpha + \gamma\eta)(\alpha + \gamma\eta')$ vanishes only for $\alpha = \gamma = 0$ in this case. In fact, one has $\mathcal{S}(M) \simeq C_{p^2-1}$, as any matrix $\left(\begin{smallmatrix} 0 & -\eta\eta' \\ 1 & \eta+\eta' \end{smallmatrix}\right) \in \mathrm{GL}(2, \mathbb{F}_p)$ with $\eta \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$ has order $p^2 - 1$ or possesses a root in $\mathrm{GL}(2, \mathbb{F}_p)$ of that order. This relies on the facts that we can always write $\eta = \lambda^m$, where λ is a generating element of $\mathbb{F}_{p^2}^\times \simeq C_{p^2-1}$, and that $\lambda\lambda'$ and $\lambda + \lambda'$ are in $\mathbb{F}_p$. This is a special case of Fact 9 below and of a statement on the existence of roots in $\mathrm{GL}(d, \mathbb{Z})$; see Lemma 6 below.

The condition for reversibility, in view of the above restriction on D and T, can only be satisfied when $D = 1$, in which case $R = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ turns out to be an involutory reversor, so that again $\mathcal{R}(M) = \mathcal{S}(M) \rtimes C_2$ in this case.

Matrices with irreducible characteristic polynomial χ_M produce orbits of one length r only, where r is the smallest integer such that $\chi_M(z) | (z^r - 1)$, or, equivalently, the order of its roots in the extension field $\mathbb{F}_{p^2}$.

Putting these little exercises together gives the following result.

Theorem 2. *A matrix $M \in \mathrm{GL}(2, \mathbb{F}_p)$ is reversible within this group if and only if $M^2 = \mathbb{1}$ or $\det(M) = 1$. Whenever $M^2 = \mathbb{1}$, one has $\mathcal{R}(M) = \mathcal{S}(M)$. If $\det(M) = 1$ with $M^2 \neq \mathbb{1}$, there exists an involutory reversor, and one has the group $\mathcal{R}(M) = \mathcal{S}(M) \rtimes C_2$.* □

Remark 2. Since $\mathbb{F}_p$ is a field, we can use the following dichotomy to understand the structure of $\mathcal{S}(M)$, independently of the chosen normal forms. A $\mathrm{GL}(2, \mathbb{F}_p)$-matrix M is either a multiple of the identity (which then commutes with every element of $\mathrm{Mat}(2, \mathbb{F}_p)$) or it possesses a cyclic vector (meaning an element $v \in \mathbb{F}_p^2$ such that v and Mv form a basis of $\mathbb{F}_p^2$). In the latter case, M commutes precisely with the matrices of the ring $\mathbb{F}_p[M]$, and we have $\mathcal{S}(M) = \mathbb{F}_p[M]^\times = \mathbb{F}_p[M] \cap \mathrm{GL}(2, \mathbb{F}_p)$. This systematic approach provides an alternative (but equivalent) parametrisation of the above results for the normal forms. ◊

The question for reversibility in $\mathrm{GL}(2, \mathbb{Z}/n\mathbb{Z})$ with general n is more complicated. The matrix $M = \left(\begin{smallmatrix} 0 & -4 \\ 1 & 0 \end{smallmatrix}\right)$ is reversible over $\mathbb{Z}/3\mathbb{Z}$ (where it is an example of type IV), but fails to be reversible over $\mathbb{Z}/9\mathbb{Z}$, as one can check by a direct computation. Here, zero divisors show up via non-zero matrices A with $AM = M^{-1}A$, but all of them satisfy $\det(A) \equiv 0 \bmod 9$. In fact, one always has $A(L_9) \subset L_3$ here.

In general, the relation $AMA^{-1} = M^{-1}$ with $A, M \in \mathrm{GL}(2, \mathbb{Z}/n\mathbb{Z})$ implies $MAM = A$ and hence $\det(M)^2 = 1$, because $\det(A) \in (\mathbb{Z}/n\mathbb{Z})^\times$. Over $\mathbb{F}_p$, this gives $\det(M) = \pm 1$, with reversibility precisely for $\det(M) = 1$ according to Theorem 2. In general, one has further solutions of the congruence $m^2 \equiv 1 \bmod n$, such as $m = 3$ for $n = 8$ or $m = 4$ for $n = 15$.

In any such case, $M = \left(\begin{smallmatrix} 0 & -m \\ 1 & 0 \end{smallmatrix}\right)$ is a matrix with $M^2 = -m\mathbb{1}$. Whenever one has $m \not\equiv -1 \bmod n$, M is of order 4 in $\mathrm{GL}(2, \mathbb{Z}/n\mathbb{Z})$. It is easy to check that $RMR = M^{-1} = \left(\begin{smallmatrix} 0 & 1 \\ -m & 0 \end{smallmatrix}\right)$ in $\mathrm{GL}(2, \mathbb{Z}/n\mathbb{Z})$, with the involution $R = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. This establishes reversibility with $\mathcal{R}(M) = \mathcal{S}(M) \rtimes C_2$.

4.3. **Some extensions to higher dimensions.** In principle, a similar reasoning, based on a normal form approach, can be applied to arbitrary dimensions. Over the finite field $\mathbb{F}_p$, normal forms are given by the rational canonical form and the elementary divisor normal form ('First' and 'Second natural normal form' in the terminology of [24, §6]), which are block diagonal matrices with companion matrices on the diagonal.

The advantage of dealing with companion matrices is that one can employ the theory of linear recursions: there is a one-to-one correspondence between the cycle lengths modulo $n \in \mathbb{N}$ of a certain initial condition $\boldsymbol{u} = (u_0, \dots, u_{d-1})$ under the recursion induced by the polynomial f, and the period of the corresponding point $\boldsymbol{u}^t$ under the matrix iteration of C_f; compare the final remark in [48], and Section 2.4.

Working with a block diagonal matrix of this shape, the analysis can be done block-wise; in particular, the symmetry groups are the direct product of the symmetry groups of the component matrices on the diagonal, augmented by all additional symmetries that emerge from equal blocks, which can be permuted.

Determining the period lengths associated with irreducible polynomials amounts to finding their orders in the sense of [34, Def. 3.3.2]. The periods and their multiplicities arising from the powers of irreducible polynomials that show up in the factorisation of the invariant factors (the elementary divisors) are then given by [48, Thm. 4].

Extending the analysis to matrices over the local rings $\mathbb{Z}/p^r\mathbb{Z}$ is more difficult. In general, it seems hard to write down an exhaustive system of normal forms for the similarity classes, and to decide whether given matrices are similar. However, a solution for a large subclass of square matrices over the p-adic integers $\mathbb{Z}_p$ and the residue class rings $\mathbb{Z}/p^r\mathbb{Z}$ is presented in [17]. For a polynomial $f \in \mathbb{Z}_p[x]$ whose reduction modulo p has no multiple factors, a complete system of $d \times d$ matrix representatives X with respect to similarity that satisfy $f(X) \equiv 0 \mod p^r$ is given by all direct sums of companion matrices which are in agreement with the factorisation of f mod p. For instance, if the reduction of the common characteristic polynomial modulo p of two matrices does not have any quadratic factors, the matrices are conjugate mod p^r if and only if they are conjugate mod p [17, Thm. 3 and Corollary].

An exhaustive treatment of conjugacy classes of 3×3 matrices over an arbitrary local principal ideal ring can be found in [4].

Remark 3. In [4], it is pointed out that 2×2 matrices over a local ring can be decomposed into a scalar and a cyclic part. Over $\mathbb{Z}/p^r\mathbb{Z}$, this decomposition reads

$$M = d\mathbb{1} + p^\ell C,$$

where $p^\ell = \gcd(\mathrm{mgcd}(M), p^r) = p^{v_p(\mathrm{mgcd}(M))}$ with v_p denoting the standard p-adic valuation, unique $d \in \{\sum_{j=0}^{\ell-1} a_j p^j \mid p \nmid a_j\}$ and cyclic $C \in \mathrm{Mat}(2, \mathbb{Z}/p^{r-\ell}\mathbb{Z})$, which is unique up to similarity. Moreover, C can be chosen as a companion matrix with the appropriate trace and determinant.

Since $d\mathbb{1}$ and C commute, powers of M can be expanded via the binomial theorem. Using that the binomials satisfy $\frac{n}{\gcd(n,k)} | \binom{n}{k}$, the period $\mathrm{per}(x, p^r)$ of all $x \in \mathrm{L}_{p^r}$ is bounded by

$$\mathrm{per}(x, p^r) \leq \mathrm{ord}(d, p^r) \cdot p^{r-\ell},$$

provided that $1 \leq \ell \leq r$. Let $\Pi_j : \mathbb{Z}/p^r\mathbb{Z} \to \mathbb{Z}/p^j\mathbb{Z}$ denote the canonical projection, and let $\mathcal{S}_j(A)$ be the symmetry group of an integer matrix A, viewed as a matrix over $\mathbb{Z}/p^j\mathbb{Z}$. Then, for $p \neq 2$ and $\ell \geq 1$, one obtains $\mathcal{S}_r(M) = \Pi_\ell^{-1}(\mathcal{S}_\ell(C))$ from the symmetry equations. ♢

4.4. **Reversibility mod n.** In this section, let M be a general integer matrix, with determinant D.

Fact 4. *If $M \in \mathrm{Mat}(d, \mathbb{Z})$ is reversible mod n, one has $D^2 \equiv 1$ mod n. Moreover, reversibility for infinitely many n implies $D = 1$ or $D = -1$.*

Proof. The reversibility equation yields $\det M \equiv \det M^{-1}$, hence $D^2 \equiv 1 \mod n$. If $D^2 - 1$ has infinitely many divisors, one has $D^2 = 1$, hence $D = 1$ or $D = -1$. □

Before we continue with some general result, let us pause to see what Fact 4 specifically implies for $d = 2$.

Fact 5. *If $M \in \mathrm{Mat}(2,\mathbb{Z})$ with $D \equiv -1$ mod n is reversible mod n, one has $2\,\mathrm{tr}(M) \equiv 0$ mod n. In particular, $\mathrm{tr}(M) \equiv 0$ mod n holds whenever n is odd.*

Proof. The trace is a conjugacy invariant, so reversibility mod n implies the relation $\mathrm{tr}(M) \equiv \mathrm{tr}(M^{-1}) \mod n$. The inversion formula for 2×2 matrices yields $\mathrm{tr}(M^{-1}) \equiv \frac{\mathrm{tr}(M)}{D} \equiv -\mathrm{tr}(M) \mod n$, and thus $2\,\mathrm{tr}(M) \equiv 0 \mod n$. □

Fact 6. *Consider $M \in \mathrm{Mat}(2,\mathbb{Z})$ with $D \equiv -1$ mod n. Then, M is an involution mod n if and only if $\mathrm{tr}(M) \equiv 0$ mod n.*

Proof. Let $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. With $D \equiv -1$, the inversion formula for M shows that $M \equiv M^{-1}$ is equivalent to $d \equiv -a$. Thus, $M^2 \equiv \mathbb{1}$ if and only if $\mathrm{tr}(M) \equiv 0$. □

The previous two facts imply

Corollary 5. *Let $M \in \mathrm{Mat}(2,\mathbb{Z})$ be reversible mod $n > 2$ with $D \equiv -1$ mod n. Then, $M^2 \equiv \mathbb{1}$ mod n for n odd, and $M^2 \equiv \mathbb{1}$ mod $n/2$ for n even.* □

Let us continue with the general arguments and formulate a necessary condition for local reversibility.

Lemma 4. *Let $p \neq 2$ be a prime. If $M \in \mathrm{Mat}(d,\mathbb{Z})$ is reversible mod p^r, one has $D \equiv \pm 1$ mod p^r. If $d = 2$, M is reversible mod p^r if and only if $D \equiv 1$ or $M^2 \equiv \mathbb{1}$ mod p^r.*

If $M \in \mathrm{Mat}(d,\mathbb{Z})$ is reversible mod 2^r, then $D \equiv \pm 1$ mod 2^{r-1}. When $d = 2$ and M is reversible with $D \equiv -1$ mod 2^{r-1}, one has $M^2 \equiv \mathbb{1}$ mod 2^{r-2}.

Proof. For $p \neq 2$, Fact 4 implies $D^2 \equiv 1$ mod p^r. Since p cannot divide both $D-1$ and $D+1$, one has $p^r|(D-1)$ or $p^r|(D+1)$, which gives the first claim. When $2^r|(D-1)(D+1)$, 2 divides one of the factors and 2^{r-1} the other one, so $D \equiv 1$ or $D \equiv -1$ mod 2^{r-1}. If $D \equiv -1$ mod 2^{r-1}, Fact 5 gives $2\,\mathrm{tr}(M) \equiv 0$ mod 2^{r-1} and thus $M^2 \equiv \mathbb{1}$ mod 2^{r-2} by Fact 6. □

One immediate consequence for $d = 2$ is the following.

Corollary 6. *If $M \in \mathrm{GL}(2,\mathbb{Z})$ with $D = -1$ is reversible for infinitely many $n \in \mathbb{N}$, one has $M^2 = \mathbb{1}$.* □

Fact 7. *Let A be an integer matrix whose determinant is coprime with $n \in \mathbb{N}$. The reduction of the inverse of A over $\mathbb{Z}/n\mathbb{Z}$, taken modulo $k|n$, is then the inverse of A over $\mathbb{Z}/k\mathbb{Z}$.* □

Lemma 5. *Let $n = p_1^{r_1} \dots p_s^{r_s}$ be the prime decomposition of $n \in \mathbb{N}$. Then, two matrices $M, M' \in \mathrm{Mat}(d,\mathbb{Z})$ are conjugate mod n if and only if they are conjugate mod $p_i^{r_i}$ for all $1 \leq i \leq s$.*

Proof. $M \sim M'$ mod n means $M' = AMA^{-1}$ for some $A \in \mathrm{GL}(n,\mathbb{Z})$, which implies conjugacy mod k for all $k|n$.

For the converse, let $A_i \in \mathrm{GL}(d,\mathbb{Z}/p_i^{r_i}\mathbb{Z})$ denote the conjugating matrix mod $p_i^{r_i}$. The Chinese remainder theorem, applied to each component of the matrices A_i and A_i^{-1}, respectively, gives matrices A and B that reduce to A_i and A_i^{-1} modulo $p_i^{r_i}$, respectively. By construction, $AB \equiv \mathbb{1} \mod p_i^{r_i}$ for all i, hence also $AB \equiv \mathbb{1}$ mod n and thus $B = A^{-1}$ in $\mathrm{GL}(d,\mathbb{Z}/n\mathbb{Z})$. □

Proposition 4. *With n as in Lemma 5, a matrix $M \in \mathrm{Mat}(d,\mathbb{Z})$ is reversible mod n if and only if M is reversible mod $p_i^{r_i}$ for all $1 \leq i \leq s$.*

Proof. The claim is a statement about the conjugacy of M and M^{-1} in the group $\mathrm{GL}(d, \mathbb{Z}/n\mathbb{Z})$, which is thus a consequence of Lemma 5. We just have to add that, by Fact 7, the inverse of M mod n reduces to the inverse mod $p_i^{r_i}$, so $MR \equiv RM^{-1}$ mod $p_i^{r_i}$ for all i. □

Corollary 7. *Consider a matrix $M \in \mathrm{Mat}(2, \mathbb{Z})$ with $D = \det(M)$ and write $n = p_1^{r_1} p_2^{r_2} \dots p_s^{r_s}$. When n is not divisible by 4, M is reversible mod n if and only if, for each $1 \le i \le s$, $D \equiv 1$ or $M^2 \equiv \mathbb{1}$ mod $p_i^{r_i}$. When $n = 2^{r_1} p_2^{r_2} \dots p_s^{r_s}$ with $r_1 \ge 2$, M is reversible mod n if and only if it is reversible mod 2^{r_1} and, for all $i > 1$, $D \equiv 1$ or $M^2 \equiv \mathbb{1}$ mod $p_i^{r_i}$.*

Proof. According to Lemma 5, the matrix M is reversible mod n if and only if it is reversible mod $p_i^{r_i}$ for all $1 \le i \le s$. By Lemma 4, this is equivalent with $D \equiv 1$ or $M^2 \equiv 1$ mod $p_i^{r_i}$ for all i with $4 \nmid p_i^{r_i}$. □

Remark 4. To see that reversibility mod p for all primes p which divide n is not sufficient for reversibility mod n, one can consider a locally reversible matrix M with $\det M \neq 1$: according to Fact 4, only finitely many n exist such that M is reversible mod n, so for each prime p there must be a maximum r for which M is reversible mod p^r. Recalling an example from above, $M = \left(\begin{smallmatrix} 0 & -4 \\ 1 & 0 \end{smallmatrix}\right)$ is reversible mod 3 but not mod 9 as can be verified by explicit calculation. It is an involution mod 5, hence also reversible mod 15, but not mod 45. ◊

Reversibility can be viewed as a structural property that reflects additional 'regularity' in the dynamics, in the sense that it typically reduces the spread in the period distribution. For 2×2-matrices, the normal form approach shows that reversibility implies the existence of only one non-trivial period length on L_p; compare our comments in Section 4.5.

4.5. **Matrix order and symmetries over $\mathbb{F}_p$.** Let us now discuss the order of a matrix $M \in \mathrm{GL}(d, \mathbb{F}_p)$, with p a prime, in conjunction with the existence of roots of M in that group. We begin by recalling the following result from [34, Thm. 2.14, Cor. 2.15 and Cor. 2.16].

Fact 8. *If f is an irreducible polynomial of degree d over $\mathbb{F}_p$, its splitting field is isomorphic with $\mathbb{F}_{p^d}$. There, it has the d distinct roots $\alpha, \alpha^p, \dots, \alpha^{p^{d-1}}$ that are conjugates and share the same order in $(\mathbb{F}_{p^d})^\times$.*

In particular, two irreducible polynomials over $\mathbb{F}_p$ of the same degree have isomorphic splitting fields. □

From now on, we will identify isomorphic fields with each other. In particular, we write $\mathbb{F}_{p^d}$ for the splitting field of an irreducible polynomial of degree d over $\mathbb{F}_p$.

Next, let K be an arbitrary finite field, consider an irreducible, monic polynomial $f \in K[x]$ of degree d, and let L be the splitting field of f. When $\lambda_1, \lambda_2, \dots, \lambda_d$ are the roots of f in L, one has the well-known factorisation

$$f(x) \;=\; \prod_{j=1}^{d} (x - \lambda_j) \;=\; x^d - e_1(\lambda_1, \dots, \lambda_d) + \dots + (-1)^d e_d(\lambda_1, \dots, \lambda_d), \qquad (20)$$

where the e_i denote the elementary symmetric polynomials,

$$e_1(x_1, \dots, x_d) = x_1 + x_2 + \dots + x_d\,, \;\dots\;, \; e_d(x_1, \dots, x_d) = x_1 \cdot x_2 \cdot \dots \cdot x_d\,.$$

The elementary symmetric polynomials, when evaluated at the roots of f, are fixed under all Galois automorphisms of the field extension L/K, so that the following property is clear.

Fact 9. *An irreducible, monic polynomial $f \in K[x]$ satisfies (20) over its splitting field L. In particular, the elementary symmetric polynomials $e_1, \ldots, e_d$, evaluated at the d roots of f in L, are elements of K.* □

Let M be a $d \times d$ integer matrix with irreducible characteristic polynomial χ_M over $\mathbb{F}_p$. Let α be a root of χ_M in $\mathbb{F}_{p^d}$ and λ a generating element of the unit group $(\mathbb{F}_{p^d})^{\times}$. Clearly, there is an $n \in \mathbb{N}$ with $\alpha = \lambda^n$. By Fact 8, one has $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^d} = \mathbb{F}_p(\lambda)$, where the degree of the extension field over $\mathbb{F}_p$ equals d. Consequently, the minimal polynomial of λ over $\mathbb{F}_p$ is an irreducible monic polynomial of degree d over $\mathbb{F}_p$, and the conjugates of α are powers of the conjugates of λ. Let $\alpha_1, \ldots, \alpha_d$ and $\lambda_1, \ldots, \lambda_d$ denote the respective collections of conjugates. Thus, over $\mathbb{F}_{p^d}$, one has the matrix conjugacy

$$M \sim \operatorname{diag}(\alpha_1, \ldots, \alpha_d) = \operatorname{diag}(\lambda_1, \ldots, \lambda_d)^n \sim C(f)^n,$$

with $f(x) \in \mathbb{F}_p[x]$ as in (20) and $C(f)$ denoting the companion matrix of f. Here, it was exploited that a $d \times d$ matrix whose characteristic polynomial f has d distinct roots is always similar to the companion matrix of f. Note that $C(f) \in \mathrm{GL}(d, \mathbb{F}_p)$ by Fact 9.

Now, M and $C(f)$ are matrices over $\mathbb{F}_p$ that are conjugate over $\mathbb{F}_{p^d}$, so (by a standard result in algebra, see [1, Thm. 5.3.15]) they are also conjugate over $\mathbb{F}_p$, which means that we have the relation

$$M = A^{-1} C(f)^n A = (A^{-1} C(f) A)^n =: W^n \tag{21}$$

with some $A \in \mathrm{GL}(d, \mathbb{F}_p)$. By similarity, one obtains $\operatorname{ord}(W) = \operatorname{ord}(C(f)) = \operatorname{ord}(\operatorname{diag}(\lambda_1, \ldots, \lambda_d)) = p^d - 1$. This gives the following result.

Lemma 6. *A matrix $M \in \mathrm{GL}(d, \mathbb{F}_p)$ with irreducible characteristic polynomial has either the maximally possible order $p^d - 1$, or admits an n-th root $W \in \mathrm{GL}(d, \mathbb{F}_p)$ as in (21). Here, n can be chosen as $n = \frac{p^d - 1}{\operatorname{ord}(M)}$, so that the root has order $p^d - 1$.* □

Fact 10. *Let A be a matrix over $\mathbb{F}_p$ with minimal polynomial of degree d. Then, the ring*

$$\mathbb{F}_p[A] = \{\xi_1 \mathbb{1} + \ldots + \xi_d A^{d-1} \mid \xi_j \in \mathbb{F}_p\}$$

has precisely p^d elements, which correspond to the different d-tuples $(\xi_1, \ldots, \xi_d)$.

Proof. Two distinct d-tuples producing the same matrix would give rise to a non-trivial linear combination that vanishes, involving powers of A of degree $d - 1$ at most, which contradicts the minimal polynomial having degree d. □

Lemma 7. *Let $W, M \in \mathrm{GL}(d, \mathbb{F}_p)$ satisfy $W^n = M$ and $\operatorname{ord}(W) = p^d - 1$. Then, $\mathbb{F}_p[M] = \mathbb{F}_p[W]$ and*

$$\mathbb{F}_p[M]^{\times} = \mathbb{F}_p[M] \setminus \{0\} = \langle W \rangle \simeq C_{p^d - 1},$$

where $\langle W \rangle$ denotes the cyclic group generated by W.

Proof. Clearly, $\mathbb{F}_p[M] = \mathbb{F}_p[W^n] \subset \mathbb{F}_p[W]$, while Fact 10 implies the relation $|\mathbb{F}_p[M]| = |\mathbb{F}_p[W]| = p^d$, whence we have equality. Further,

$$\langle W \rangle \subset \mathbb{F}_p[W]^{\times} \subset \mathbb{F}_p[W] \setminus \{0\} = \mathbb{F}_p[M] \setminus \{0\},$$

and again, comparing cardinalities, one finds $|\langle W\rangle| = p^d - 1 = |\mathbb{F}_p[M] \setminus \{0\}|$, from which the claim follows. $\square$

Let us summarise and extend the above arguments as follows.

Corollary 8. *A $d \times d$ integer matrix M with irreducible characteristic polynomial over the field $\mathbb{F}_p$ has a primitive root $W \in \mathrm{GL}(d, \mathbb{F}_p)$ with $\mathrm{ord}(W) = p^d - 1$. Moreover, one then has $\mathbb{F}_p[M]^\times = \mathbb{F}_p[M] \setminus \{0\} = \langle W\rangle \simeq C_{p^d-1}$. In particular, $\mathcal{S}(M) \simeq C_{p^d-1}$ in this case.*

More generally, we have $\mathcal{S}(M) = \mathbb{F}_p[M]^\times$ whenever the minimal polynomial has degree d.

Proof. Since we work over the field $\mathbb{F}_p$, the irreducibility of the characteristic polynomial of M means that the minimal polynomial agrees with the characteristic polynomial and has thus maximal degree d. This situation is equivalent with M being cyclic [27, Thm. III.2]. By Thm. 17 of [27] and the Corollary following it, we know that any matrix which commutes with M is a polynomial in M, so that $\mathcal{S}(M) = \mathbb{F}_p[M]^\times$ is clear.

The claim for matrices M with an irreducible characteristic polynomial follows by Lemmas 6 and 7. $\square$

When a matrix $M \in \mathrm{Mat}(d, \mathbb{F}_p)$ fails to be cyclic, there are always commuting matrices that are not elements of $\mathbb{F}_p[M]$, see Thm. 19 of [27] and the following Corollary. In such a case, $\mathcal{S}(M)$ is a true group extension of $\mathbb{F}_p[M]^\times$. The situation is thus particularly simple for matrices $M \in \mathrm{Mat}(2, \mathbb{F}_p)$: Either they are of the form $M = a\mathbb{1}$ (then with $\mathcal{S}(M) = \mathrm{GL}(2, \mathbb{F}_p)$), or they are cyclic (then with the group $\mathcal{S}(M) = \mathbb{F}_p[M]^\times$).

Appendix: Two classic examples. If one reads through the literature, two matrices are omnipresent as examples, the Arnold and the Fibonacci cat map. Still, several aspects of them are unclear or conjectural, despite the effort of many. Let us sum up some aspects, with focus on properties in line with our above reasoning.

A.1. **Arnold's cat map.** Here, we collect some results for the classic matrix $M_\mathrm{A} = \left(\begin{smallmatrix} 2 & 1 \\ 1 & 1 \end{smallmatrix}\right) \in \mathrm{SL}(2, \mathbb{Z})$ in an informal manner. This case was studied in [37, 21, 25] and appeared in many other articles as main example. It was introduced in [3, Example 1.16] as a paradigm of (discrete) hyperbolic dynamics.

The integer matrix M_A is reversible within the group $\mathrm{GL}(2, \mathbb{Z})$, with a reversor of order 4, but none of order 2. One has $\mathcal{S}(M_\mathrm{A}) \simeq C_2 \times C_\infty$, where $C_2 = \{\pm 1\}$ and the infinite cyclic group is generated by the unique square root of M_A in $\mathrm{GL}(2, \mathbb{Z})$ (see below), while $\mathcal{R}(M_\mathrm{A}) = \mathcal{S}(M_\mathrm{A}) \rtimes C_4$; see [9] for more. In particular, M_A inherits local reversibility in $\mathrm{GL}(2, \mathbb{Z}/p\mathbb{Z})$ for all primes p from its 'global' reversibility within $\mathrm{GL}(2, \mathbb{Z})$.

It was shown in [25] that M_A, except for the trivial fixed point 0, has orbits of only one period length on each prime lattice L_p with $p \neq 5$. In view of the normal forms, this is clear whenever the characteristic polynomial is irreducible. However, a matrix of type III from Table 4.2 has reducible characteristic polynomial and occurs for primes with $\left(\frac{5}{p}\right) = -1$. Here, different orbit lengths would still be possible in general, but reversibility forces the two roots to be multiplicative inverses of one another and thus to have the same order modulo p.

The iteration numbers are $u_m = f_{2m}$, where the f_k are the Fibonacci numbers, defined by the recursion $f_{k+1} = f_k + f_{k-1}$ for $k \in \mathbb{N}$ with initial conditions $f_0 = 0$ and $f_1 = 1$. Since $\mathrm{mgcd}(M_{\mathrm{A}}) = 1$, Proposition 2 implies

$$\mathrm{ord}(M_{\mathrm{A}}, n) \;=\; \kappa_{\mathrm{A}}(n) \;=\; \mathrm{period}\big\{(f_{2m})_{m\geq 0} \bmod n\big\},$$

where the periods for prime powers (with $r \in \mathbb{N}$) are given by

$$\kappa_{\mathrm{A}}(2^r) = 3 \cdot 2^{\max\{0, r-2\}} \quad \text{and} \quad \kappa_{\mathrm{A}}(5^r) = 10 \cdot 5^{r-1}$$

together with

$$\kappa_{\mathrm{A}}(p^r) \;=\; p^{r-1}\, \kappa_{\mathrm{A}}(p)$$

for all remaining plateau-free primes. It has been conjectured that this covers all primes [44]. No exception is known to date; the conjecture was tested for all $p < 10^8$ in [5]. Note that each individual prime can be analysed on the basis of Proposition 1.

The periods mod p are $\kappa_{\mathrm{A}}(2) = 3$, $\kappa_{\mathrm{A}}(5) = 10$, together with

$$\kappa_{\mathrm{A}}(p) \;=\; \frac{p - \big(\frac{5}{p}\big)}{2m_p - \frac{1}{2}\Big(1 - \big(\frac{5}{p}\big)\Big)}$$

for odd primes $p \neq 5$, where $\big(\frac{5}{p}\big)$ denotes the Legendre symbol and $m_p \in \mathbb{N}$ is a characteristic integer that covers the possible order reduction. It is 1 in 'most' cases (in the sense of a density definition), but there are infinitely many cases with $m_p > 1$; this integer is tabulated to some extent in [44, 25].

Let us write down the generating polynomials for the distribution of cycles on the lattices L_n. Once again, this is only necessary for n a prime power. We use a formulation with a factorisation that shows the structure of orbits on $L_{p^r} \setminus L_{p^{r-1}}$. In the notation of [12], one finds $Z_1(t) = (1-t)$ and

$$Z_{2^r}(t) \;=\; (1-t)(1-t^3) \prod_{\ell=0}^{r-2} \big(1 - t^{3\cdot 2^\ell}\big)^{4\cdot 2^\ell}$$

with $r \geq 1$ for the prime $p = 2$, as well as

$$Z_{5^r}(t) \;=\; (1-t) \prod_{\ell=0}^{r-1} \big((1 - t^{2\cdot 5^\ell})(1 - t^{10\cdot 5^\ell})\big)^{2\cdot 5^\ell}$$

with $r \geq 1$ for $p = 5$. As usual, we adopt the convention to treat an empty product as 1. The remaining polynomials read

$$Z_{p^r}(t) \;=\; (1-t) \prod_{\ell=0}^{r-1} \big(1 - t^{\kappa_{\mathrm{A}}(p) p^\ell}\big)^{\frac{p^2-1}{\kappa_{\mathrm{A}}(p)}\, p^\ell},$$

as long as the plateau phenomenon is absent (see above).

A.2. **Fibonacci cat map.** Closely related is the matrix $M_{\mathrm{F}} = \left(\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right) \in \mathrm{GL}(2,\mathbb{Z})$, which is the unique square root of the Arnold cat map M_{A} in $\mathrm{GL}(2,\mathbb{Z})$. It appears in numerous applications; see [38, 6, 7, 16] and references therein for some of them. Here, the iteration numbers are the Fibonacci numbers themselves, and the periods are the so-called *Pisano periods*; compare [42, A001175] and references given there, or [44].

The matrix M_{F} is not reversible in $\mathrm{GL}(2,\mathbb{Z})$ (while its square M_{A} is, see above), and has the same symmetry group as M_{A}. In fact, $\pm M_{\mathrm{F}}$ are the only roots of M_{A} in $\mathrm{GL}(2,\mathbb{Z})$. This situation implies that the orbit structure for M_{F} must be such that the iteration of its square gives back the counts we saw in the previous example.

For prime powers p^r, with $r \in \mathbb{N}$, one finds $\kappa_{\mathrm{F}}(5^r) = 20 \cdot 5^{r-1}$ together with

$$\kappa_{\mathrm{F}}(p^r) \;=\; p^{r-1}\, \kappa_{\mathrm{F}}(p)$$

for all remaining primes, with the same proviso as for the Arnold cat map. The periods $\kappa_{\mathrm{F}}(p)$ are given by $\kappa_{\mathrm{F}}(2) = \kappa_{\mathrm{A}}(2) = 3$ together with

$$\kappa_{\mathrm{F}}(p) \;=\; 2\, \kappa_{\mathrm{A}}(p)$$

for all odd primes, which is not surprising in view of the relation between the two matrices M_{F} and M_{A}.

The orbit distribution is more complicated in this case, as usually orbits of two possible lengths arise in each step. One finds

$$Z_{2^r}(t) \;=\; (1-t) \prod_{\ell=0}^{r-1} \bigl(1 - t^{3\cdot 2^{\ell}}\bigr)^{2^{\ell}}$$

and

$$Z_{5^r}(t) \;=\; (1-t) \prod_{\ell=0}^{r-1} \bigl((1 - t^{4\cdot 5^{\ell}})(1 - t^{20\cdot 5^{\ell}})\bigr)^{5^{\ell}}$$

for the primes 2 and 5 (with $r \in \mathbb{N}_0$ as before), as well as

$$Z_{p^r}(t) \;=\; (1-t) \prod_{\ell=0}^{r-1} \bigl(1 - t^{\frac{1}{2}\,\kappa_{\mathrm{F}}(p) p^{\ell}}\bigr)^{2 n_p} \bigl(1 - t^{\kappa_{\mathrm{F}}(p) p^{\ell}}\bigr)^{\frac{p^2-1}{\kappa_{\mathrm{F}}(p)}\, p^{\ell} - n_p}$$

for all remaining primes that are free of the plateau phenomenon (which possibly means all, see above). Here, $n_p \in \mathbb{N}_0$ is a characteristic integer which often takes the values 1 or 0, but does not seem to be bounded.

Acknowledgments. It is our pleasure to thank A. Weiss for his cooperation and R.V. Moody for helpful discussions. This work was supported by the Australian Research Council (ARC), via grant DP0774473, and by the German Resarch Council (DFG), within the CRC 701.

REFERENCES

[1] W. A. Adkins and S. H. Weintraub, "Algebra – An Approach via Module Theory," corr. 2nd printing, Springer, New York, 1999.

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

[3] V. I. Arnold and A. Avez, "Ergodic Problems of Classical Mechanics," reprint, Addison-Wesley, Redwood City, CA, 1989.

[4] N. Avni, U. Onn, A. Prasad and L. Vaserstein, *Similarity classes of 3×3 matrices over a localprincipal ideal ring*, Commun. Algebra, **37** (2009), 2601–2615.

[5] H. Aydin, R. Dikici and G. C. Smith, *Wall and Vinston revisited*, in "Applications of Fibonacci Numbers," **5** (1992), K 61–68. Kluwer Acad. Publ., Dordrecht, 1993.

[6] M. Baake, U. Grimm and D. Joseph, *Trace maps, invariants, and some of their applications*, Int. J. Mod. Phys. B, **7** (1993), 1527–1550.

[7] M. Baake, J. Hermisson and P. A. B. Pleasants, *The torus parametrization of quasiperiodic LI-classes*, J. Phys. A: Math. Gen., **30** (1997), 3029–3056.

[8] M. Baake, E. Lau and V. Paskunas, *A note on the dynamical zeta function of general toral endomorphisms*, Monatsh. Math., **161** (2010), 33–42.

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

[10] M. Baake and J. A . G. Roberts, *symmetries of toral automorphisms*, Nonlinearity, **14** (2001), R1–R24.

[11] M. Baake and J. A. G. Roberts, *The structure of reversing symmetry groups*, Bull. Austral. Math. Soc., **73** (2006), 445–459.

[12] M. Baake, J. A. G. Roberts and A. Weiss, *Periodic orbits of linear endomorphisms of the 2-torusand its lattices*, Nonlinearity, **21** (2008), 2427–2446.

[13] E. Behrends and B. Fiedler, *Periods of discretized linear Anosov maps*, Ergod. Th. & Dynam. Syst., **18** (1998), 331–341.

[14] E. Brown and T. P. Vaughan, *Cycles of directed graphs definedby matrix multiplication (mod n)*, Discr. Math., **239** (2001), 109–120.

[15] P. Bundschuh and J. S. Shiue, *A generalization of a paper by D. D. Wall*, Rendiconti Accademia Nazionale dei Lincei, Roma,Classe di Scienze Fisiche,Matematiche e Naturali, **56** (1974), 135–144.

[16] D. Damanik, *Gordon-type arguments in the spectral theory of one-dimensional quasicrystals*, in "Directions in Mathematical Quasicrystals" (eds. M. Baake and R. V. Moody), CRM Monograph Series, AMS, Providence, RI, **13** (2000), 277–305.

[17] R. W. Davis, *Certain matrix equations over rings of integers*, Duke Math. J., **35** (1968), 49–59.

[18] M. Degli Esposti and S. Isola, *Distribution of closed orbits for linear automorphisms of tori*, Nonlinearity, **8** (1995), 827–842.

[19] M. Degli Esposti and B. Winn, *The quantum perturbed cat map and symmetry*, J. Phys. A: Math. Gen., **38** (2005), 5895–5912.

[20] R. De Vogelaere, *On the structure of symmetric periodic solutions of conservative systems, with applications*, Ch. IV of Contributions to the Theory of NonlinearOscillations, ed. S. Lefschetz, Princeton Univ. Press, Princeton, **IV** 1958, 53–84.

[21] F. J. Dyson and H. Falk, *Period of a discrete cat mapping*, Amer. Math. Monthly, **99** (1992), 603–614.

[22] H. T. Engstrom, *On sequences defined by linear recurrence relations*, Trans. Amer. Math. Soc., **33** (1931), 210–218.

[23] A. Fel'shtyn, *Dynamical zeta functions, nielsen theory and reidemeister torsion*, Memoirs AMS, Providence, RI, **147** (2000), xii+146 pp.

[24] F. R. Gantmacher, "Matrix Theory," Chelsea, New York, **I** 1960.

[25] G. Gaspari, *The Arnold cat map on prime lattices*, Physica, **73** (1994), 352–372.

[26] H. Hasse, "Number Theory," Springer, Berlin 1980.

[27] N. Jacobson, "Lectures in Abstract Algebra. II. Linear Algebra," reprint, Springer, New York, 1975.

[28] A. Katok and B. Hasselblatt, "Introduction to the Modern Theory of Dynamical Systems," Cambridge University Press, Cambridge, 1995.

[29] J. P. Keating, *Asymptotic properties of the periodic orbits of the cat maps*, Nonlinearity, **4** (1991), 277–307.

[30] J. P. Keating and F. Mezzadri, *Pseudo-symmetries of Anosov maps and spectral statistics*, Nonlinearity, **13** (2000), 747–775.

[31] P. Kurlberg, *On the order of unimodular matrices modulo integers*, Acta Arithm., **110** (2003), 141–151.

[32] P. Kurlberg and Z. Rudnick, *Hecke theory and equidistribution for the quantization of linear maps of the torus*, Duke Math. J., **103** (2000), 47–77.

[33] S. Lang, "Algebra," rev. 3rd ed., Springer, New York, 2002.

[34] R. Lidl and H. Niederreiter, "Introduction to Finite Fields and Their Applications," Cambridge University Press, Cambridge, 1986.

[35] N. Neumärker, "Orbitstatistik und Relative Realisierbarkeit," Diploma Thesis, Univ. Bielefeld, 2007.

[36] N. Neumärker, "The Arithmetic Structure of Discrete Dynamical Systems on the Torus," PhD thesis, Univ. Bielefeld, 2012.

[37] I. Percival and F. Vivaldi, *Arithmetical properties of strongly chaotic motions*, Physica, **25** (1987), 105–130.

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

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

[40] D. Ruelle, "Dynamical Zeta Functions for Piecewise Monotone Maps of the Interval," CRM Monograph Series,,AMS, Providence, RI, **4** 1994.

[41] P. Seibt, *A period formula for torus automorphisms*, Discr. Cont. Dynam. Syst., **9** (2003), 1029–1048.

[42] N. J. A. Sloane, "The Online Encyclopedia of Integer Sequences," http://oeis.org

[43] O. Taussky, *Introduction into connections between algebraic number theory and integral matrices*, 2nd appendix to: H. Cohn, A Classical Invitation to Algebraic Numbers and Class Fields, 2nd printing, Springer, New York, (1988), 305–321.

[44] D. D. Wall, *Fibonacci series modulo m*, Amer. Math. Monthly, **67** (1960), 525–532.

[45] P. Walters, "An Introduction to Ergodic Theory," Graduate Texts in Mathematics, 79, Springer-Verlag, New York-Berlin, 1982.

[46] M. Ward, *The arithmetic theory of linear recurring sequences*, Trans. Amer. Math. Soc., **35** (1933), 600–628.

[47] R. J. Wilson, "Introduction to Graph Theory," 4th ed., Prentice Hall, Harlow, 1996.

[48] N. Zierler, *Linear recurring sequences*, J. Soc. Indust. Appl. Math., **7** (1959), 31–48.

Received August 2011; revised May 2012.

E-mail address: mbaake@math.uni-bielefeld.de
E-mail address: naneumae@math.uni-bielefeld.de
E-mail address: jag.roberts@unsw.edu.au