TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 347, Number 12, December 1995

PERIODS FOR TRANSVERSAL MAPS VIA LEFSCHETZ NUMBERS FOR PERIODIC POINTS

A. GUILLAMON, X. JARQUE, J. LLIBRE, J. ORTEGA AND J. TORREGROSA

ABSTRACT. Let $f : M \to M$ be a C^1 map on a C^1 differentiable manifold. The map f is called transversal if for all $m \in \mathbb{N}$ the graph of f^m intersects transversally the diagonal of $M \times M$ at each point (x, x) such that x is a fixed point of f^m. We study the set of periods of f by using the Lefschetz numbers for periodic points. We focus our study on transversal maps defined on compact manifolds such that their rational homology is $H_0 \approx \mathbb{Q}$, $H_1 \approx \mathbb{Q} \oplus \mathbb{Q}$ and $H_k \approx \{0\}$ for $k \neq 0, 1$.

1. INTRODUCTION AND STATEMENT OF THE MAIN RESULTS

In dynamical systems it is often the case that differentiable topological information can be used to study qualitative and quantitative properties of the system. This paper deals with the problem of determining the periods (of the periodic points) of a class of C^1 self-maps given the homology class of the map. In order to state our main results we need some preliminary notation and definitions.

Let $f : X \to X$ be a continuous map. A *fixed point* of f is a point x of X such that $f(x) = x$. Denote the totality of fixed points by $\mathrm{Fix}(f)$. The point $x \in X$ is *periodic with period* m if $x \in \mathrm{Fix}(f^m)$ but $x \notin \mathrm{Fix}(f^k)$ for all $k = 1, \ldots, m-1$. Let $\mathrm{Per}(f)$ denote the set of all periods of periodic points of f.

Let M be a compact manifold of dimension n. A continuous map $f : M \to M$ induces endomorphisms $f_{*k} : H_k(M; \mathbb{Q}) \to H_k(M; \mathbb{Q})$ (for $k = 0, 1, \ldots, n$) on the rational homology groups of M. The *Lefschetz number* of f is defined by

$$L(f) = \sum_{k=0}^{n} (-1)^k \mathrm{trace}(f_{*k}).$$

By the renowned Lefschetz fixed point theorem: if $L(f) \neq 0$ then f has fixed points (see, for instance, [B]). Of course, we can consider the Lefschetz number of f^m but (in general) it is not true that if $L(f^m) \neq 0$ then f has periodic points of period m. As it is well-known a fixed point of f^m need not have period m, so it will be useful to have a method for detecting the difference

Received by the editors June 1, 1993 and, in revised form, August 1, 1994.
1991 *Mathematics Subject Classification.* Primary 58F20.
Key words and phrases. Periods, transversal maps, Lefschetz numbers.
Some of the authors are partially supported by DGICYT and MEC grants.

between "real" and "false" periodic points of period m (i.e., points having period some proper divisor of m).

We will use the Lefschetz numbers for periodic points introduced in [Ll] for analysing if a given period belongs to the set of periods of a self-map. More precisely, for every $m \in \mathbb{N}$ we define the *Lefschetz number of period* m, $l(f^m)$, as follows

$$l(f^m) = \sum_{r|m} \mu(r) L(f^{\frac{m}{r}}),$$

where $\sum_{r|m}$ denotes the sum over all positive divisors r of m, and μ is the *Moebius function* defined by

$$\mu(m) = \begin{cases} 1 & \text{if } m = 1, \\ 0 & \text{if } k^2|m \text{ for some } k \in \mathbb{N}, \\ (-1)^r & \text{if } m = p_1 \cdots p_r \text{ distinct prime factors.} \end{cases}$$

According to the inversion formula (see for instance [NZ])

$$L(f^m) = \sum_{r|m} l(f^r).$$

The Lefschetz number of period m will become interesting after showing that for many classes of maps we have: if $l(f^m) \neq 0$ then $m \in \text{Per}(f)$. Dold [D] showed that for any $m \in \mathbb{N}$ if $\text{Fix}(f^m)$ is compact then m divides $l(f^m)$. Other authors like Halpern [H] or Heath, Piccinini and You [HPY] have introduced a similar definition for Nielsen numbers instead of Lefschetz numbers.

A C^1 map $f : M \to M$ defined on a compact C^1 differentiable manifold is called *transversal* if $f(M) \subset \text{Int}(M)$ and if for all $m \in \mathbb{N}$ at each point $x \in \text{Fix}(f^m)$ we have $\det(I - df^m(x)) \neq 0$, i.e., 1 is not an eigenvalue of $df^m(x)$. Notice that if f is transversal then for all $m \in \mathbb{N}$ the graph of f^m intersects transversally the diagonal $\{(y, y) : y \in M\}$ at each point (x, x) such that $x \in \text{Fix}(f^m)$. Notice that for a tranversal map f the fixed points of f^m are isolated. Since M is compact, the cardinal of $\text{Fix}(f^m)$ is finite for every $m \in \mathbb{N}$.

Periodic points of transversal maps have been studied by several authors: Franks [F1, F3], Matsuoka [M], Matsuoka and Shiraki [MS], Casasayas, Llibre and Nunes [CLN1,CLN2], ... The following result was proved in [Ll].

Theorem A. *Let f be a transversal map. Suppose that $l(f^m) \neq 0$ for some $m \in \mathbb{N}$.*

(a) *If m is odd then $m \in \text{Per}(f)$.*
(b) *If m is even then $\{m/2, m\} \cap \text{Per}(f) \neq \varnothing$.*

Theorem A will play a key role in this work. Since its proof is short, in Section 2 we will present it for the sake of completeness.

The results on transversal maps on arbitrary compact manifolds given in Theorem A are in general difficult to apply because of the computation of $l(f^m)$. Of course, if the homological rational groups are simple then these computations become easier. For instance, if $H_k(M; \mathbb{Q}) \approx \mathbb{Q}$ for $k = 0, 1$ and $H_k(M; \mathbb{Q}) \approx \{0\}$ otherwise, the Lefschetz numbers of period m are easily computed. This is the case for the circle, where we can compute the sets of periods for its transversal maps; however, the sets of periods of continuous self-maps on the circle are already well-known, see [ALM].

A distinct problem is to know whether the set of periods of a transversal map coincides or not with the set $\{m \in \mathbb{N} : l(f^m) \neq 0\}$. In general, this is a difficult question. But for a transversal map g on the circle, the results obtained from Theorem A are optimal in the following sense: if D is the degree of g, then

$$L_D = \{m \in \mathbb{N} : l(g^m) \neq 0\} = \begin{cases} \varnothing & \text{if } D = 1, \\ \{1\} & \text{if } D \in \{-1, 0\}, \\ \mathbb{N} \setminus \{2\} & \text{if } D = -2, \\ \mathbb{N} & \text{otherwise;} \end{cases}$$

and there are transversal maps on the circle such that any $D \in \mathbb{Z}$ verifies $\mathrm{Per}(f) = L_D$, see again [ALM].

Here the Lefschetz numbers for periodic points are applied to study the set of periods of transversal maps on a compact manifold M with rational homology

$$(1) \qquad H_0(M; \mathbb{Q}) \approx \mathbb{Q}, \ H_1(M; \mathbb{Q}) \approx \mathbb{Q} \oplus \mathbb{Q}, \ H_k(M; \mathbb{Q}) \approx \{0\} \text{ for } k \neq 0, 1.$$

The transversal maps on compact manifolds with such homology are the easiest nontrivial maps for which we can compute $l(f^m)$ and apply Theorem A to obtain information about their sets of periods.

For instance, there are exactly five compact manifolds of dimension 2 with the above homology: the sphere with 3 holes, the torus with 1 hole, the connected sum of three real projective planes, the connected sum of two real projective planes with 1 hole, and the real projective plane with 3 holes. Of course, there are higher dimensional compact manifolds with this homology. The easiest higher examples are the products of the above surfaces with acyclic manifolds, but there are many other. For example, the three-dimensional compact manifold obtained from the sphere S^3 removing the connected sum of two open solid tori, eventually knotted, see Figure 1.1, have also the homology given by (1). For more details, see the Appendix.

Our main result on the set of periods of transversal maps follows from the next theorems and Theorem A. Essentially, we give information on the set of periods for a transversal map f on a compact manifold having the homology given by (1), by using the first induced homology endomorphism by f. This is a 2×2 integral matrix. The description of our results is given in terms of the trace t and the determinant d of this matrix. First, we deal with the case where the eigenvalues of the matrix are real (Theorem B and Corollary C); later on, we consider the non-real case (Theorem D and Corollary E).

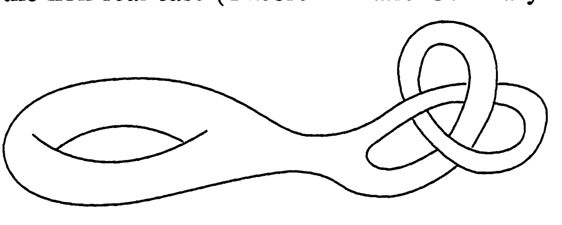

FIGURE 1.1

Theorem B. *Let $f : M \to M$ be a transversal map. Suppose that the rational homology of M satisfies* (1). *If we denote by t and d the trace and the determinant of the first induced homology endomorphism $f_{*1} : H_1(M; \mathbb{Q}) \to H_1(M; \mathbb{Q})$ (corresponding to some 2×2 integral matrix) and assume that the eigenvalues of f_{*1} are real, then the following statements hold.*

(a) *Assume that $m > 1$ is odd. Then $l(f^m) = 0$ if and only if $(t, d) \in \{(\pm 1, 0), (\pm 2, 1)\} \cup \{(0, d) : d \in \mathbb{Z}$ and $d \le 0\}$.*
(b) *$l(f) = L(f) = 0$ if and only if $t = 1$.*
(c) *Assume that $m > 2$ is even. Then $l(f^m) = 0$ if and only if $(t, d) \in \{(\pm 1, 0), (\pm 2, 1), (0, 0), (0, -1)\}$.*
(d) *$l(f^2) = 0$ if and only if $(t, d) \in \{(1, 0), (2, 1), (0, 0)\}$.*

Theorem B will be proved in Section 3. From Theorems A and B the following corollary follows easily.

Corollary C. *In the assumptions of Theorem* B *the following statements hold.*

(a) *If $(t, d) \neq (1, 0)$, then* $\mathrm{Per}(f) \neq \varnothing$.
(b) *If $(t, d) \notin \{(\pm 1, 0), (\pm 2, 1)\} \cup \{(0, d) : d \in \mathbb{Z}$ and $d \le 0\}$, then* $\mathrm{Per}(f) \supset \{3, 5, 7, 9, \dots\}$.
(c) *If $t \neq 1$, then $1 \in \mathrm{Per}(f)$.*
(d) *If $(t, d) \notin \{(\pm 1, 0), (\pm 2, 1), (0, 0), (0, -1)\}$, then for any odd natural q at least one of each consecutive pair of the sequence $q, 2q, 4q, 8q, \dots$ is a period of f.*

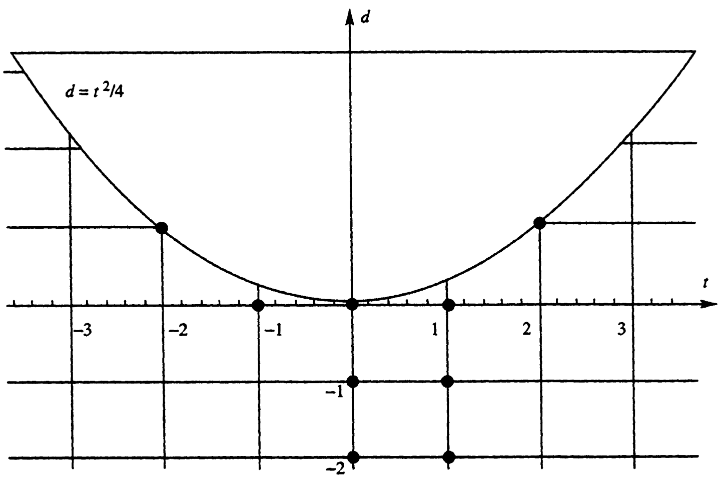

FIGURE 1.2. Exceptional points appearing in the different statements of Corollary C. For such points, some periods may not exist.

We remark that the sequence of statement (d) of Corollary C appears in the Sharkovskii ordering, which controls the periodic structure of a continuous self-map of a closed interval, see [S]. Then, in some sense, statement (d) of Corollary C reflects some periodic structure from dimension one to higher dimension.

Note that in Theorem B we have described completely the zero set of $l(f^m)$ for all $m \in \mathbb{N}$, when the eigenvalues of f are real. So, in Corollary C we give all possible information of the set of periods that can be obtained by means of Theorem A.

When the eigenvalues of f_{*1} are complex, the problem of studying the pairs (t, d) for which $l(f^m) = 0$ changes completely. The techniques that we will use in the proof of Theorem B are not valid in that case, and the results will not cover all the possibilities as in the real case. In fact, in the complex case, we restrict our analysis to periods of the form p^n with p prime and $n \in \mathbb{N}$.

We denote by $P_m(t, d)$ the polynomial $l(f^m)$ in the variables (t, d). In Section 4 we will see that $P_m(t, d)$ is a polynomial with integer coefficients. Let also be $T = \{(t, d) \in \mathbb{Z}^2 : t = 0\}$, $V = \{(t, d) \in \mathbb{Z}^2 : t = 3k, d = 3k^2 \text{ for all } k \in \mathbb{Z}\}$ and $Z_m = \{(t, d) \in \mathbb{Z}^2 : P_m(t, d) = 0\}$. The following theorem is obtained by studying the diophantine equations $P_m(t, d) = 0$.

Theorem D. *Let $f : M \to M$ be a transversal map. Suppose that the rational homology of M satisfies* (1). *We denote by t and d the trace and the determinant of the first induced homology endomorphism $f_{*1} : H_1(M; \mathbb{Q}) \to H_1(M; \mathbb{Q})$ (corresponding to some 2×2 integral matrix). Then, the following statements hold.*

(a) *If $m > 1$ is odd, $T \subset Z_m$. $Z_1 = \{(1, d) : d \in \mathbb{Z}\}$. If m is a multiple of 9, then $V \subset Z_m$.*
(b) *If m is a power of two, then $Z_2 = \{(t, \frac{t(t-1)}{2}) : t \in \mathbb{Z}\}$, $Z_4 = \{(\pm1, 1), (\pm1, 0), (0, -1), (0, 0), (\pm2, 1), (\pm2, 6)\}$, and $\mathrm{Card}(Z_{2^n}) < \infty$ if $n \geq 3$.*
(c) *If m is a power of three, then $Z_3 = T \cup \{(t, \frac{t^2-1}{3}) :$ for all $t \in \mathbb{Z}$ such that $t \equiv 1, 2 \pmod 3\}$, and $\mathrm{Card}(Z_{3^n} \setminus \{T \cup V\}) < \infty$ if $n \geq 2$.*
(d) *If m is a power of the prime $p \geq 5$, then $\mathrm{Card}(Z_{p^n} \setminus T) < \infty$ for $n \in \mathbb{N}$. Furthermore, $Z_5 \setminus T = \{(\pm1, 1), (\pm1, 0), (\pm2, 1), (\pm2, 3)\}$, and $Z_{5^n} \setminus T = \{(\pm1, 1), (\pm1, 0), (\pm2, 1)\}$ if $n > 1$.*
(e) *If $p > 5$ is a prime number, then there exists $n_0 = n_0(p)$ such that*
$$Z_{p^n} \setminus T = \{(\pm1, 1), (\pm1, 0), (\pm2, 1)\} \text{ for all } n \geq n_0.$$
(f) *For all $m \in \mathbb{N} \setminus \{2, 3, 6\}$, $(1, 1) \in Z_m$. For all $m \in \mathbb{N} \setminus \{1, 3\}$, $(-1, 1) \in Z_m$.*

Theorem D will be proved in Section 3. From Theorems A and D the following corollary follows immediately.

Corollary E. *In the assumptions of Theorem* D *the following statements hold.*

(a) *If $(t, d) \notin \{(t, \frac{t(t-1)}{2}) : t \in \mathbb{Z}\}$, then $\{1, 2\} \cap \mathrm{Per}(f) \neq \varnothing$.*
(b) *If $(t, d) \notin \{(t, \frac{t^2-1}{3}) :$ for all $t \in \mathbb{Z}$ such that $t \equiv 1, 2 \pmod 3\} \cup T$, then $3 \in \mathrm{Per}(f)$.*
(c) *If $(t, d) \notin \{(\pm1, 1), (\pm1, 0), (0, -1), (0, 0), (\pm2, 1), (\pm2, 6)\}$, then $\{2, 4\} \cap \mathrm{Per}(f) \neq \varnothing$.*
(d) *If $n \geq 3$, then $\{2^{n-1}, 2^n\} \cap \mathrm{Per}(f) \neq \varnothing$ except for a finite number of pairs (t, d).*
(e) *If $n \geq 2$, then $3^n \in \mathrm{Per}(f)$ for any $(t, d) \notin T \cup V$, except for a finite number of them.*
(f) *If $n \geq 1$, then $5^n \in \mathrm{Per}(f)$ for $(t, d) \notin T \cup \{(\pm1, 1), (\pm1, 0), (\pm2, 1), (\pm2, 3)\}$. For $(t, d) = (\pm2, 3)$ and $n \geq 2$, $5^n \in \mathrm{Per}(f)$.*

(g) *If* $n \geq 1$ *and* $p > 5$ *is prime, then* $p^n \in \mathrm{Per}(f)$, *for any* $(t, d) \notin T$ *except for a finite number of them.*

(h) *For any prime* $p > 5$, *there exists* $n_0 = n_0(p) \in \mathbb{N}$ *such that for all* $n \geq n_0(p)$, $p^n \in \mathrm{Per}(f)$ *for* $(t, d) \notin T \cup \{(\pm 1, 1), (\pm 1, 0), (\pm 2, 1)\}$.

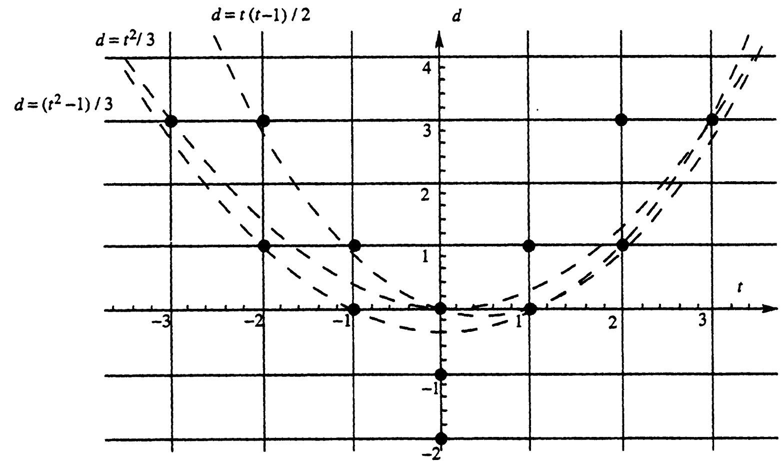

FIGURE 1.3. Exceptional points appearing in the different statements of Corollary E. For such points, some periods may not exist.

Compared to Theorem B (f_{*_1} with real eigenvalues), in Theorem D there is not the whole information about the zeroes of the $l(f^m)$. First of all, only the case $m = p^n$, p prime, $n \geq 1$, is dealt with. Even in this case, some of the statements of Theorem D (and so, of Corollary E) are valid except for a finite number of pairs (t, d) which we do not specify. However, as it is stated in the next conjecture, we feel that this finite set of pairs is empty.

We remark that for $m > 5$ and $(t, d) \notin T \cup V$, in Theorem D $l(f^m) = 0$ at the same points (t, d) of Theorem B, except for $(t, d) = (\pm 1, 1)$. Theorem D and some numerical computations allows us to conjecture that for $m > 6$ we have

$$Z_m = \begin{cases} \{(\pm 1, 1), (\pm 1, 0), (0, -1), (0, 0), (\pm 2, 1)\} & \text{if } m \text{ is even, } 9 \nmid m, \\ T \cup \{(\pm 1, 1), (\pm 1, 0), (\pm 2, 1)\} & \text{if } m \text{ is odd, } 9 \nmid m, \\ V \cup \{(\pm 1, 1), (\pm 1, 0), (0, -1), (0, 0), (\pm 2, 1)\} & \text{if } m \text{ is even, } 9 \mid m, \\ T \cup V \cup \{(\pm 1, 1), (\pm 1, 0), (\pm 2, 1)\} & \text{if } m \text{ is odd, } 9 \mid m. \end{cases}$$

$$Z_6 = \{(\pm 1, 0), (0, -1), (0, 0), (\pm 2, 1)\}.$$

2. Proof of Theorem A

Let $f : M \to M$ be a transversal map. We are interested in studying the set of periods of f. To this purpose it is useful to have information on the whole sequence $\{L(f^m)\}_{m \in \mathbb{N}}$ of the Lefschetz numbers of all the iterates of f. The *Lefschetz zeta function of* f defined as

$$Z_f(t) = \exp\left(\sum_{m=1}^{+\infty} \frac{L(f^m)}{m} t^m\right)$$

is a generating function for that sequence, and it may be computed independently through

$$Z_f(t) = \prod_{k=0}^{\dim M} \det(I_{n_k} - tf_{*k})^{(-1)^{k+1}},$$

where $n_k = \dim H_k(M;\mathbb{Q})$, I_{n_k} is the $n_k \times n_k$ identity matrix and we take $\det(I_{n_k} - tf_{*k}) = 1$ if $n_k = 0$, see for more details [F2].

For transversal maps the Lefschetz zeta function may be related in a simple way with its set of periodic orbits. Given γ a periodic orbit of f of period $m = p(\gamma)$ and $x \in \gamma$, we define $u_+(\gamma) = u_+(x)$ and $u_-(\gamma) = u_-(x)$, where $u_+(x)$ (respectively $u_-(x)$) denotes the number of real eigenvalues of $df^m(x)$ which are strictly greater than 1 (respectively less than -1). It is easy to check that $u_+(\gamma)$ and $u_-(\gamma)$ are well-defined. With this notation, we have the following proposition due to Franks [F1].

Proposition 2.1. *Let $f: M \to M$ be a transversal map. Then*

$$Z_f(t) = \prod_{\gamma} \left(1 - (-1)^{u_-(\gamma)} t^{p(\gamma)}\right)^{(-1)^{u_+(\gamma)+u_-(\gamma)+1}},$$

where γ goes over all the periodic orbits of f.

From the definitions of $l(f^m)$ and $Z_f(t)$ we get the following well-known formal relation

$$Z_f(t) = \prod_{m=1}^{+\infty} (1 - t^m)^{-\frac{l(f^m)}{m}}, \tag{2}$$

for more details see, for instance [BB].

From Proposition 2.1, the Lefschetz zeta function has a factor $(1 \pm t^m)^{\pm 1}$ from every periodic orbit of period m. Substituting the factors $(1 + t^k)$ by $(1 - t^{2k})/(1 - t^k)$ one obtains that in $Z_f(t)$, $(1 - t^m)$ can appear either from $(1 - t^m)$ or from $(1 + t^{\frac{m}{2}})$ if m is even. So, by using (2) $l(f^m) \neq 0$ implies $m \in \operatorname{Per}(f)$ if m is odd, and $\{m/2, m\} \cap \operatorname{Per}(f) \neq \varnothing$ if m is even. Hence Theorem A is proved.

3. Proof of Theorem B

Let $f: M \to M$ be a transversal map and suppose that the rational homology of M satisfies

$$H_0(M;\mathbb{Q}) \approx \mathbb{Q},\ H_1(M;\mathbb{Q}) \approx \mathbb{Q} \oplus \mathbb{Q},\ H_k(M;\mathbb{Q}) \approx \{0\} \text{ for } k \neq 0, 1.$$

Let λ_1 and λ_2 be the two eigenvalues of the first induced homology endomorphism $f_{*1}: H_1(M;\mathbb{Q}) \to H_1(M;\mathbb{Q})$. Since $H_0(M;\mathbb{Q}) \approx \mathbb{Q}$, M is connected, and consequently f_{*0} is the identity. Then $L(f^m) = 1 - (\lambda_1^m + \lambda_2^m)$ for all $m \in \mathbb{N}$. Notice that

$$\begin{aligned} \sum_{r|m} \mu(r) &= 1 - \left(\sum_{1 \le i \le n} 1\right) + \left(\sum_{1 \le i < j \le n} 1\right) - \ldots + (-1)^n \\ &= 1 - \binom{n}{1} + \binom{n}{2} - \ldots + (-1)^n \binom{n}{n} \\ &= (1-1)^n = 0 \end{aligned} \tag{3}$$

where $m = p_1^{\alpha_1} \cdots p_n^{\alpha_n} > 1$ with $p_1, \dots, p_n$ distinct primes. Therefore, if $m > 1$ the Lefschetz number of period m will be

$$l(f^m) = -\sum_{r|m} \mu(r)(\lambda_1^{\frac{m}{r}} + \lambda_2^{\frac{m}{r}}).$$

For each $m \in \mathbb{N}$ we define the polynomial

$$Q_m(x) = \sum_{r|m} \mu(r) x^{\frac{m}{r}}.$$

Then, if $m > 1$ we can write

$$-l(f^m) = Q_m(\lambda_1) + Q_m(\lambda_2). \tag{4}$$

Hence we will study when $l(f^m)$ is zero or not by analysing the polynomials $Q_m(x)$ and evaluating them at λ_1 and λ_2.

We start with a technical lemma and, later on, we will focus on two different cases: in Lemma 3.2 we will study the behaviour of these polynomials when $|x| \le 1$, and in Lemmas 3.3, 3.4, 3.5 and 3.6 we will consider the polynomials when $|x| \ge 1$.

Figure 3.1 displays how the polynomials behave, depending on the parity of their degree $m = p_1^{\alpha_1} \dots p_n^{\alpha_n}$.

Lemma 3.1. *Let $m \in \mathbb{N}$.*

(a) *If $m = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ with $p_1, \dots, p_n$ distinct primes, then $Q_m(x) = Q_{p_1 \cdots p_n}(x^{\frac{m}{p_1 \cdots p_n}})$.*

(b) *If $m = p_1 \cdots p_n$ with $p_1, \dots, p_n$ distinct primes, then $Q_m(x) = Q_{\frac{m}{p_k}}(x^{p_k}) - Q_{\frac{m}{p_k}}(x)$ for any $k \in \{1, \dots, n\}$.*

(c) *If m is odd, then Q_m is an odd function, i.e., $Q_m(x) = -Q_m(-x)$.*

(d) *If $4|m$, then Q_m is an even function, i.e., $Q_m(x) = Q_m(-x)$.*

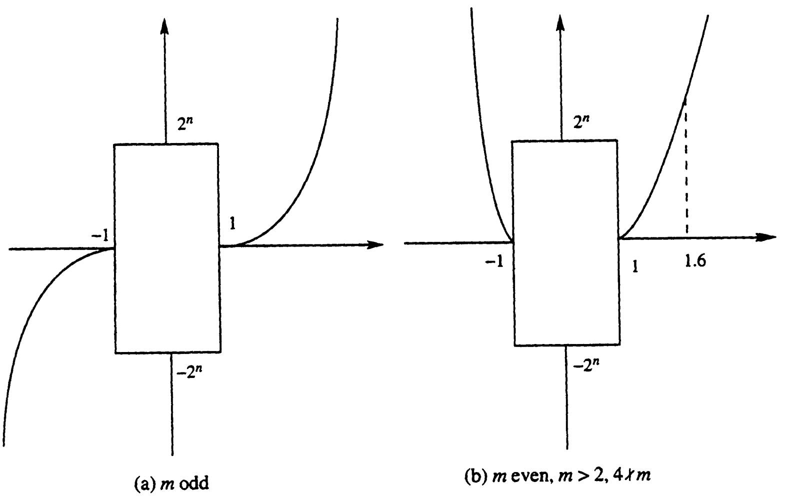

FIGURE 3.1. The qualitative graph of the polynomial $Q_m(x)$

(e) *If* $2|m$ *and* $4\not| m$, *then* $Q_m(x) = Q_{\frac{m}{2}}(x^2) - Q_{\frac{m}{2}}(x)$.
(f) $Q_m(0) = 0$.
(g) *If* $m > 1$, *then* $Q_m(1) = 0$.
(h) *If* $m > 2$, *then* $Q_m(-1) = 0$.

Proof. Suppose that $m = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ with $p_1, \ldots, p_n$ distinct primes. From the definition of $Q_{p_1 \cdots p_n}(x)$ we have that

$$Q_{p_1\cdots p_n}(x) = x^{p_1\cdots p_n} - \sum_{1\le i\le n} x^{\frac{p_1\cdots p_n}{p_i}} + \sum_{1\le i<j\le n} x^{\frac{p_1\cdots p_n}{p_ip_j}} - \ldots + (-1)^n x.$$

Then

$$Q_{p_1\cdots p_n}(x^{\frac{m}{p_1\cdots p_n}}) = x^m - \sum_{1\le i\le n} x^{\frac{m}{p_i}} + \sum_{1\le i<j\le n} x^{\frac{m}{p_ip_j}} - \ldots + (-1)^n x^{\frac{m}{p_1\cdots p_n}}.$$

Hence, since the unique divisors r of m such that $\mu(r) \neq 0$ are 1, $\{p_i\}_{1\le i\le n}$, $\{p_ip_j\}_{1\le i<j\le n}, \ldots, \{p_1\cdots p_n\}$, it follows (a).

Now assume $m = p_1 \cdots p_n$ with $p_1, \ldots, p_n$ distinct primes. Then

$$\begin{aligned}
Q_m(x) =& x^m - \sum_{\substack{1\le i\le n\\ i\neq k}} x^{\frac{m}{p_i}} + \sum_{\substack{1\le i<j\le n\\ i,j\neq k}} x^{\frac{m}{p_ip_j}} - \ldots + (-1)^{n-1} x^{p_k}\\
&- \left(x^{\frac{m}{p_k}} - \sum_{\substack{1\le i\le n\\ i\neq k}} x^{\frac{m}{p_kp_i}} + \ldots - (-1)^{n-1} \sum_{\substack{1\le i\le n\\ i\neq k}} x^{p_i} - (-1)^n x \right)\\
=& (x^{p_k})^{\frac{m}{p_k}} - \sum_{\substack{1\le i\le n\\ i\neq k}} (x^{p_k})^{\frac{m}{p_kp_i}} + \sum_{\substack{1\le i<j\le n\\ i,j\neq k}} (x^{p_k})^{\frac{m}{p_kp_ip_j}} - \ldots + (-1)^{n-1} x^{p_k}\\
&- \left(x^{\frac{m}{p_k}} - \sum_{\substack{1\le i\le n\\ i\neq k}} x^{\frac{m}{p_kp_i}} + \sum_{\substack{1\le i<j\le n\\ i,j\neq k}} x^{\frac{m}{p_kp_ip_j}} - \ldots + (-1)^{n-1} x \right)\\
=& Q_{\frac{m}{p_k}}(x^{p_k}) - Q_{\frac{m}{p_k}}(x).
\end{aligned}$$

Therefore, we have proved (b).

If m is odd, then all the degrees of all monomials of the polynomial $Q_m(x)$ are odd. Therefore $Q_m(x)$ is an odd function, and (c) is shown.

If $4|m$, then all the degrees of all monomials of the polynomial $Q_m(x)$ are even. Therefore $Q_m(x)$ is an even function and we obtain (d).

If $2|m$ and $4\not| m$ then, we can write $m = 2p_2^{\alpha_2} \cdots p_n^{\alpha_n}$ with $p_2, \ldots, p_n$ distinct primes. From statements (a) and (b) of Lemma 3.1, we obtain

$$\begin{aligned}
Q_m(x) &= Q_{2p_2\cdots p_n}(x^{\frac{m}{2p_2\cdots p_n}})\\
&= Q_{p_2\cdots p_n}(x^{\frac{m}{p_2\cdots p_n}}) - Q_{p_2\cdots p_n}(x^{\frac{m}{2p_2\cdots p_n}})\\
&= Q_{\frac{m}{2}}(x^2) - Q_{\frac{m}{2}}(x).
\end{aligned}$$

So (e) is proved.

From the definition of the polynomial $Q_m(x)$ it follows immediately (f), and from (3) we get (g).

If m is odd then, from (c) and (g), $Q_m(-1) = -Q_m(1) = 0$. If $4|m$ then, from (d) and (g), $Q_m(-1) = Q_m(1) = 0$. Assume that $m = 2p_2^{\alpha_2} \cdots p_n^{\alpha_n}$ with with $p_2, \ldots, p_n$ distinct primes. Then, from (a) and (e), we get $Q_m(-1) = Q_{2p_2\cdots p_n}(-1) = Q_{p_2\cdots p_n}((-1)^2) - Q_{p_2\cdots p_n}(-1) = 0$. Hence (h) is proved. □

As the next theorem states,the values of $Q_m(x)$ remain bounded for $|x| \leq 1$.

Lemma 3.2. *If $m = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ with $p_1, \ldots, p_n$ distinct primes, then $|Q_m(x)| \leq 2^n$ if $|x| \leq 1$.*

Proof. From the definition of $Q_m(x)$, (3) and since $|x| \leq 1$, we get

$$|Q_m(x)| = \left|\sum_{r|m} \mu(r) x^{\frac{m}{r}}\right| \leq \sum_{r|m} |\mu(r)| \left|x^{\frac{m}{r}}\right| \leq \sum_{r|m} |\mu(r)| = \sum_{k=0}^{n} \binom{n}{k} = 2^n. \quad \square$$

While in Lemma 3.1 we have studied the values of the polynomials $Q_m(x)$ at ± 1, in the next lemma we will do the same for all their derivatives. We denote by $Q_m^{(i)}(x)$ the i-th derivative of the polynomial $Q_m(x)$ with respect to the variable x.

In the following four results, the behaviour of $Q_m(x)$ for $|x| \geq 1$ is studied.

Lemma 3.3. *For all $i \in \mathbb{N}$ we have $Q_m^{(i)}(1) \geq 0$.*

Proof. First we will show that if $p_1, \ldots, p_n$ are distinct prime numbers, then $Q_{p_1\cdots p_n}^{(i)}(1) \geq 0$ for all $i \in \mathbb{N}$. We will prove this by using induction with respect to n.

If $n = 1$ then $Q_{p_1}(x) = x^{p_1} - x$. Consequently, $Q_{p_1}'(x) = p_1 x^{p_1-1} - 1$, $Q_{p_1}^{(i)}(x) = p_1! x^{p_1-i}/(p_1 - i)!$ if $1 < i \leq p_1$ (of course $0! = 1$), and $Q_{p_1}^{(i)}(x) = 0$ if $i > p_1$. Hence $Q_{p_1}^{(i)}(1) \geq 0$ for all $i \in \mathbb{N}$. So the lemma is true for $n = 1$.

Assume that the lemma is true for $n-1$. Now we will prove it for n. From Lemma 3.1(b) it follows that $Q_{p_1\cdots p_n}(x) = Q_{p_2\cdots p_n}(x^{p_1}) - Q_{p_2\cdots p_n}(x)$. Then it is easy to show that

$$Q_{p_1\cdots p_n}^{(i)}(x) = Q_{p_2\cdots p_n}^{(i)}(x^{p_1})(p_1 x^{p_1-1})^i - Q_{p_2\cdots p_n}^{(i)}(x) + P(x), \tag{5}$$

where

$$P(x) = \sum_{1\leq j<i} A_j(x) Q_{p_2\cdots p_n}^{(j)}(x), \tag{6}$$

and $A_j(x)$ is a polynomial in x with positive coefficients. Then, from (5), (6) and since the lemma is true for $n-1$, it follows that

$$Q_{p_1\cdots p_n}^{(i)}(1) \geq 0. \tag{7}$$

Now suppose that $m = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ with $p_1, \ldots, p_n$ distinct primes. By Lemma 3.1(a) we have $Q_m(x) = Q_{p_1\cdots p_n}(x^{\frac{m}{p_1\cdots p_n}})$. Then

$$Q_m^{(i)}(x) = \left(\frac{d}{dx}\right)^i Q_{p_1\cdots p_n}(x^{\frac{m}{p_1\cdots p_n}}).$$

Clearly the right-hand side of the last equality can be written as

$$\sum_{1\leq j\leq i} B_j(x) Q_{p_1\cdots p_n}^{(j)}(x^{\frac{m}{p_1\cdots p_n}}),$$

where the $B_j(x)$ are polynomials in x with positive coefficients. Hence, from (7) it follows that $Q_m^{(i)}(1) \geq 0$. □

Proposition 3.4. *The following statements hold.*

(a) *For all $m \in \mathbb{N}$ the function $Q_m(x)$ is positive and increasing in $(1, \infty)$.*
(b) *For all odd $m \in \mathbb{N}$ the function $Q_m(x)$ is negative and increasing in $(-\infty, -1)$.*
(c) *For all even $m \in \mathbb{N}$ the function $Q_m(x)$ is positive and decreasing in $(-\infty, -1)$.*

Proof. From the expression of $Q_m(x)$ in Taylor series at $x = 1$ and Lemma 3.3 it follows (a).

From (a) and Lemma 3.1(c) we get (b).

If $4|m$ then from (a) and Lemma 3.1(d), we obtain (c) when $4|m$. Now we consider $2|m$ and $4\not|m$. From Lemma 3.1(e), we get $Q_m(x) = Q_{\frac{m}{2}}(x^2) - Q_{\frac{m}{2}}(x)$. So, by Lemma 3.1(c), $Q_m(-x) = Q_{\frac{m}{2}}(x^2) + Q_{\frac{m}{2}}(x)$. Consequently, from (a) we get that $Q_m(x)$ is positive and decreasing in $(-\infty, -1)$. □

Lemma 3.5. *For all $x \in [1, \infty)$ the following statements hold.*

(a) *For all $m \in \mathbb{N}$ we have $|Q_m(x)| \leq |Q_m(-x)|$.*
(b) *For all $m \in \mathbb{N}$ such that $2|m$ and $4\not|m$ we have $Q_m(x) \leq Q_m(-x)$.*
(c) *If $m = p_1^{\alpha_1} \cdots p_n^{\alpha_n} > 1$ with $p_1, \ldots, p_n$ distinct primes, then $Q_{p_1\cdots p_n}(x) \leq Q_m(x)$.*

Proof. If m is odd, from Lemma 3.1(c), $Q_m(x) = -Q_m(-x)$. So (a) is shown when m is odd. If $4|m$, from Lemma 3.1(d), $Q_m(x) = Q_m(-x)$. Therefore (a) is also proved when $4|m$. Assume $2|m$ and $4\not|m$. From Lemma 3.1(e), $Q_m(x) = Q_{\frac{m}{2}}(x^2) - Q_{\frac{m}{2}}(x)$. So, by Lemma 3.1(c), $Q_m(-x) = Q_{\frac{m}{2}}(x^2) + Q_{\frac{m}{2}}(x)$. By subtracting the previous two equalities we get $Q_m(x) - Q_m(-x) = -2Q_{\frac{m}{2}}(x)$. Therefore, if $x \in [1, \infty)$ from Proposition 3.4(a) it follows that $Q_m(x) \leq Q_m(-x)$. Hence, we have proved (a) and (b).

From Lemma 3.1(a), Proposition 3.4(a) and since $x \in [1, \infty)$, it follows immediately (c). □

Lemma 3.6. *Assume that $p_1, \ldots, p_n$ are distinct primes.*

(a) $Q'_{p_1\cdots p_n}(1) = \prod_{i=1}^n (p_i - 1)$.
(b) $Q''_{p_1\cdots p_n}(1) = \prod_{i=1}^n (p_i^2 - 1) - \prod_{i=1}^n (p_i - 1)$.
(c) *If $m = p_1^{\alpha_1} \cdots p_n^{\alpha_n} > 2$ then $Q_m(1.6) \geq 2^n$.*

Proof. Assume that $m = p_1 \cdots p_n$. We will prove (a) and (b) by induction with respect to n. If $n = 1$ then $Q_{p_1}(x) = x^{p_1} - x$. Consequently $Q'_{p_1}(x) = p_1 x^{p_1 - 1} - 1$ and $Q''_{p_1}(x) = p_1(p_1 - 1)x^{p_1 - 2}$. Then $Q'_{p_1}(1) = p_1 - 1$ and $Q''_{p_1}(1) = p_1(p_1 - 1) = (p_1^2 - 1) - (p_1 - 1)$. So (a) and (b) are true for $n = 1$.

Assume that (a) and (b) are true up to $n - 1$. By Lemma 3.1(b), $Q_m(x) = Q_{\frac{m}{p_n}}(x^{p_n}) - Q_{\frac{m}{p_n}}(x)$. Then $Q'_m(x) = Q'_{\frac{m}{p_n}}(x^{p_n}) p_n x^{p_n - 1} - Q'_{\frac{m}{p_n}}(x)$. So, by the induction hypotheses,

$$Q'_m(1) = (p_n - 1) Q'_{\frac{m}{p_n}}(1) = (p_n - 1) \prod_{i=1}^{n-1} (p_i - 1) = \prod_{i=1}^{n} (p_i - 1).$$

Hence (a) is proved.

From $Q''_m(x) = Q''_{\frac{m}{p_n}}(x^{p_n})(p_n x^{p_n-1})^2 + Q'_{\frac{m}{p_n}}(x^{p_n})p_n(p_n-1)x^{p_n-2} - Q''_{\frac{m}{p_n}}(x)$, the induction hypothesis, and (a) we get

$$\begin{aligned} Q''_m(1) &= (p_n^2-1)Q''_{\frac{m}{p_n}}(1) + p_n(p_n-1)Q'_{\frac{m}{p_n}}(1) \\ &= (p_n^2-1)\left[\prod_{i=1}^{n-1}(p_i^2-1) - \prod_{i=1}^{n-1}(p_i-1)\right] \\ &\quad + p_n(p_n-1)\prod_{i=1}^{n-1}(p_i-1) \\ &= \prod_{i=1}^{n}(p_i^2-1) - \prod_{i=1}^{n}(p_i-1). \end{aligned}$$

Hence (b) is proved.

Now assume that $m = p_1^{\alpha_1}\cdots p_n^{\alpha_n} > 2$. By Lemma 3.1(a) and Proposition 3.4(a), we have $Q_m(1.6) = Q_{p_1\cdots p_n}(1.6^{\frac{m}{p_1\cdots p_n}}) \geq Q_{p_1\cdots p_n}(1.6)$. So, in order to prove (c) it suffices to show $Q_{p_1\cdots p_n}(1.6) \geq 2^n$.

From the Taylor series of $Q_{p_1\cdots p_n}(x)$ at $x=1$, Lemma 3.1(g), and since $Q^{(i)}_{p_1\cdots p_n}(1) \geq 0$ for all $i \geq 1$ (see Lemma 3.3 or 3.6(a)), for $x \geq 1$ we have $Q_{p_1\cdots p_n}(x) \geq Q'_{p_1\cdots p_n}(1)(x-1) + \frac{1}{2}Q''_{p_1\cdots p_n}(1)(x-1)^2$. By using (a) and (b), for $x \in [1, 3]$ we get

$$\begin{aligned} Q_{p_1\cdots p_n}(x) &\geq \frac{1}{2}\left[\left(\prod_{i=1}^{n}(p_i-1)\right)(x-1)(3-x) + \left(\prod_{i=1}^{n}(p_i^2-1)\right)(x-1)^2\right] \\ &\geq \frac{1}{2}\left(\prod_{i=1}^{n}(p_i^2-1)\right)(x-1)^2. \end{aligned}$$

Therefore, if $n \geq 2$ we have $Q_{p_1\cdots p_n}(1.6) \geq (9/50)\prod_{i=1}^{n}(p_i^2-1) \geq (9/50)\cdot 3 \cdot (2^3)^{n-1} \geq 2^{3n-4} \geq 2^n$.

Assume $n=1$. If $p_1 > 3$ then $Q_{p_1}(1.6) \geq (9/50)(p_1^2-1) > 2$. If $p_1 = 3$ then $Q_3(1.6) = 1.6^3 - 1.6 > 2$. Hence (c) is proved. □

Now we use all these results in order to prove the statements of Theorem B, that is, we characterize the zeroes of $l(f^m)$ for all natural m in case that the eigenvalues are real.

Proof of statement (a) *of Theorem* B. Let λ_1 and λ_2 be the two real eigenvalues of f_{*1}. Without loss of generality we can assume that $|\lambda_1| \geq |\lambda_2|$. From (4) we have $-l(f^m) = Q_m(\lambda_1) + Q_m(\lambda_2)$. Since m is odd, $Q_m(-\lambda_1) + Q_m(-\lambda_2) = -[Q_m(\lambda_1)+Q_m(\lambda_2)]$. So, in order to study when $l(f^m) \neq 0$ it suffices to consider $\lambda_1 \geq 0$. Therefore we can restrict the analysis to the values of (λ_1, λ_2) which belong to the set

$$R = \{(\lambda_1, \lambda_2) \in \mathbb{R}^2 : \lambda_1 \geq 0 \text{ and } -\lambda_1 \leq \lambda_2 \leq \lambda_1\}.$$

We divide R into five subsets (see Figure 3.2):

$$R_2 = \{(\lambda_1, \lambda_2) \in R : \lambda_1 > 1 \text{ and } \lambda_2 > 1\},$$
$$R_3 = \{(\lambda_1, \lambda_2) \in R : \lambda_1 > 1.6 \text{ and } -1 \le \lambda_2 \le 1\},$$
$$R_4 = \{(\lambda_1, \lambda_2) \in R : \lambda_1 > 1 \text{ and } -\lambda_1 < \lambda_2 < -1\},$$
$$R_5 = \{(\lambda_1, \lambda_2) \in R : \lambda_1 = -\lambda_2\},$$
$$R_1 = R \setminus \bigcup_{i=2}^{5} R_i.$$

If $(\lambda_1, \lambda_2) \in R_2$ then, from Proposition 3.4(a) we get $-l(f^m) = Q_m(\lambda_1) + Q_m(\lambda_2) > 0$.

If $(\lambda_1, \lambda_2) \in R_3$ then, from Lemmas 3.2 and 3.6(c), and Proposition 3.4(a), we get $Q_m(\lambda_1) > 2^n$ and $|Q_m(\lambda_2)| \le 2^n$. Hence $-l(f^m) > 0$.

If $(\lambda_1, \lambda_2) \in R_4$ then, from Lemma 3.1(c) and Proposition 3.4(b), we obtain $Q_m(\lambda_1) = -Q_m(-\lambda_1) \neq -Q_m(\lambda_2)$. So $l(f^m) \neq 0$.

If $(\lambda_1, \lambda_2) \in R_5$ then, from Lemma 3.1(c), $Q_m(\lambda_1) + Q_m(\lambda_2) = 0$. Therefore $l(f^m) = 0$.

Now we will study $l(f^m)$ on the set R_1. Let t and d be the trace and the determinant of f_{*1} respectively. We consider the set R_1 in the variables $(t = \lambda_1 + \lambda_2, d = \lambda_1\lambda_2)$. The straight lines $\lambda_1 = 1.6$, $\lambda_2 = 1$, $\lambda_2 = -1$, $\lambda_1 + \lambda_2 = 0$ and $\lambda_1 - \lambda_2 = 0$ become $d = 1.6(t - 1.6)$, $d = t - 1$, $d = -t - 1$, $t = 0$ and $d = t^2/4$ respectively. In Figure 3.3 we show the set R_1 in the variables (t, d). So the unique points (t, d) in R_1 with integer coordinates are $(1, 0)$ and $(2, 1)$; or equivalently in coordinates (λ_1, λ_2) are $(1, 0)$ and $(1, 1)$. In both points, from statements (f) and (g) of Lemma 3.1, we get $l(f^m) = 0$.

In short, if m is odd then $l(f^m) = 0$ if and only $t = 0$ and $d \le 0$, $(t, d) \in \{(\pm 1, 0), (\pm 2, 1)\}$ (use the symmetry $(\lambda_1, \lambda_2) \to (-\lambda_1, -\lambda_2)$). Hence Theorem B(a) is proved. □

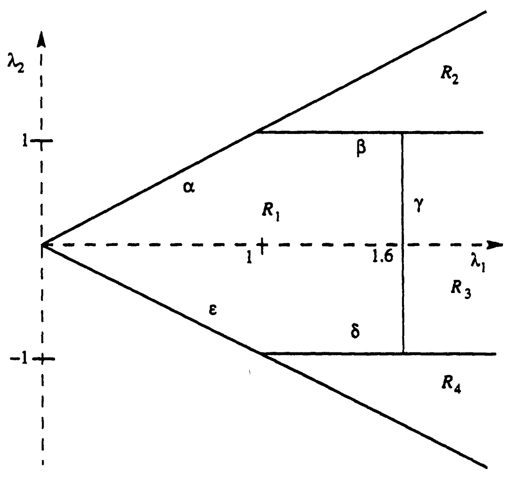

FIGURE 3.2. The partition of R into $\bigcup_{i=1}^{5} R_i$.

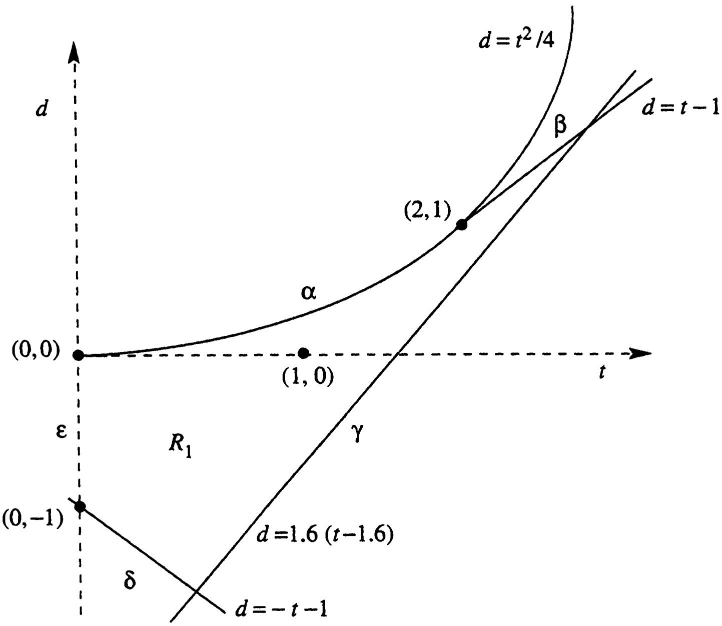

FIGURE 3.3. The set R_1 in the variables (t, d).

Proof of statement (b) *of Theorem* B. From the definition of $l(f)$ it follows that $l(f) = L(f) = 1 - t$. $\square$

Proof of statement (c) *of Theorem* B. As above we denote by λ_1 and λ_2 the two real eigenvalues of f_{*1}. We can assume that $|\lambda_1| \geq |\lambda_2|$, and $-l(f^m) = Q_m(\lambda_1) + Q_m(\lambda_2)$.

First we assume that $4|m$. By Lemma 3.1(d) $Q_m(x)$ is an even function. Then the value of $l(f^m)$ is the same in the four points $(\pm\lambda_1, \pm\lambda_2)$. Consequently we can restrict the analysis to the values (λ_1, λ_2) which belong to the set

$$R = \{(\lambda_1, \lambda_2) \in \mathbb{R}^2 : \lambda_1 \geq 0 \text{ and } -\lambda_1 \leq \lambda_2 \leq 0\}.$$

We divide R into three subsets (see Figure 3.4):

$$R_2 = \{(\lambda_1, \lambda_2) \in R : \lambda_1 > 1 \text{ and } \lambda_2 < -1\},$$
$$R_3 = \{(\lambda_1, \lambda_2) \in R : \lambda_1 > 1.6 \text{ and } -1 \leq \lambda_2 \leq 0\},$$
$$R_1 = R \setminus \bigcup_{i=2}^{3} R_i.$$

If $(\lambda_1, \lambda_2) \in R_2$ then, from Lemma 3.1(d) and Proposition 3.4(a), we get $-l(f^m) = Q_m(\lambda_1) + Q_m(\lambda_2) > 0$.

If $(\lambda_1, \lambda_2) \in R_3$ then, from Lemmas 3.2 and 3.6(c), and Proposition 3.4(a), we get $Q_m(\lambda_1) > 2^n$ and $|Q_m(\lambda_2)| \leq 2^n$. Hence $-l(f^m) > 0$.

From the last two paragraphs it follows that $l(f^m)$ only will be able to be zero in the set R_1. We will consider the set R_1 in the variables (t, d). The straight lines $\lambda_2 = 0$, $\lambda_1 = 1.6$, $\lambda_2 = -1$ and $\lambda_1 + \lambda_2 = 0$ become $d = 0$, $d = 1.6(t - 1.6)$, $d = -t - 1$ and $t = 0$ respectively. In Figure 3.5 we show the

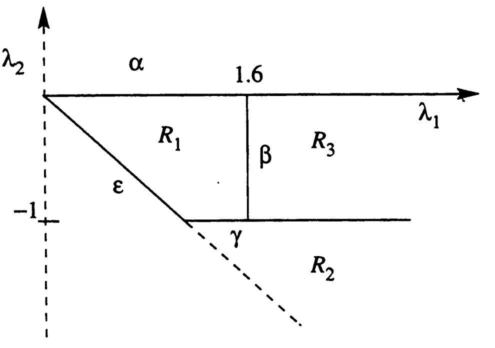

FIGURE 3.4. The partition of R into $\bigcup_{i=1}^{3} R_i$.

set R_1 in the variables (t, d). So the unique points (t, d) in R_1 with integer coordinates are $(0, 0)$, $(0, -1)$ and $(1, 0)$; or equivalently in coordinates (λ_1, λ_2) are $(0, 0)$, $(1, -1)$ and $(1, 0)$. In these three points $l(f^m) = 0$ due to statements (f), (g) and (h) of Lemma 3.1.

In short, taking into account the four symmetries, $(\pm\lambda_1, \pm\lambda_2)$, if $4|m$ then $l(f^m) = 0$ if and only if $(t, d) \in \{(0, 0), (0, -1), (\pm 1, 0), (\pm 2, 1)\}$.

Now we assume that $2|m$, $4\nmid m$ and $m \neq 2$. We must analyse the values of $l(f^m)$ in the points of the set

$$R = \{(\lambda_1, \lambda_2) \in \mathbb{R}^2 : |\lambda_1| \geq |\lambda_2|\}.$$

We divide R into three subsets (see Figure 3.6):

$$R_2 = \{(\lambda_1, \lambda_2) \in R : |\lambda_1| > 1 \text{ and } |\lambda_2| > 1\},$$
$$R_3 = \{(\lambda_1, \lambda_2) \in R : |\lambda_1| > 1.6 \text{ and } -1 \leq \lambda_2 \leq 1\},$$
$$R_1 = R \setminus \bigcup_{i=2}^{3} R_i.$$

If $(\lambda_1, \lambda_2) \in R_2$ then, from Proposition 3.4(a), we get $-l(f^m) = Q_m(\lambda_1) + Q_m(\lambda_2) > 0$.

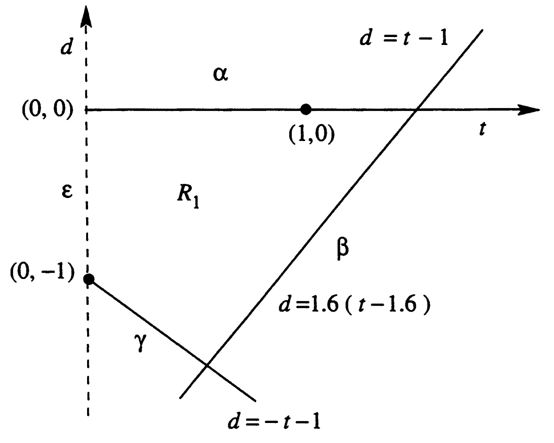

FIGURE 3.5. The set R_1 in the variables (t, d).

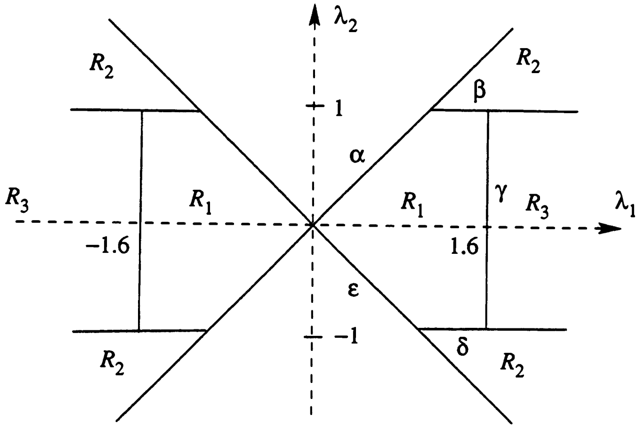

FIGURE 3.6. The partition of R into $\bigcup_{i=1}^{3} R_i$.

If $(\lambda_1, \lambda_2) \in R_3$ then, from Proposition 3.4(a) and Lemmas 3.2, 3.5(b) and 3.6(c), we get $Q_m(\lambda_1) > 2^n$ and $|Q_m(\lambda_2)| \leq 2^n$. Hence we obtain $-l(f^m) > 0$.

Then $l(f^m)$ only will be able to be zero in the set R_1. Again we will consider the set R_1 in the variables (t, d). The straight lines $\lambda_1 - \lambda_2 = 0$, $\lambda_2 = 1$, $\lambda_1 = 1.6$, $\lambda_2 = -1$, $\lambda_1 + \lambda_2 = 0$ and $\lambda_1 = -1.6$ become $d = t^2/4$, $d = t - 1$, $d = 1.6(t - 1.6)$, $d = -t - 1$, $t = 0$ and $d = -1.6(t + 1.6)$ respectively. In Figure 3.7 we show the set R_1 in the variables (t, d). Then, as in the above case for $2|m$, $4\not| m$ and $m \neq 2$ we obtain that $l(f^m) = 0$ if and only if $(t, d) \in \{(0, 0), (0, -1), (\pm 1, 0), (\pm 2, 1)\}$. Hence we have proved Theorem B(c). $\square$

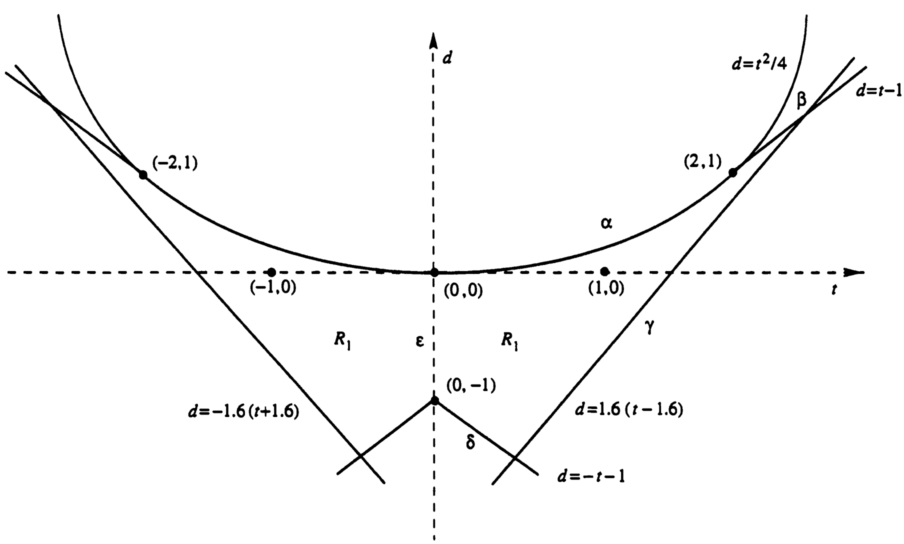

FIGURE 3.7. The set R_1 in the variables (t, d).

Proof of statement (d) *of Theorem* B. Since $Q_2(x) = x^2 - x$, the minimum

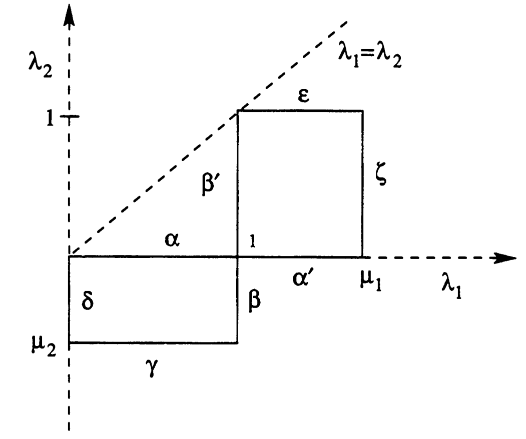

FIGURE 3.8. The set R in the variables (λ_1, λ_2).

value of $Q_2(x)$ in $\mathbb{R}$ is $Q_2(1/2) = -1/4$. Let μ_1 and μ_2 be such that $\mu_2 < 0$, $\mu_1 > 1$ and $Q_2(\mu_1) = Q_2(\mu_2) = 1/4$. Since we can consider $\lambda_1 \geq \lambda_2$, $-l(f^2) = Q_2(\lambda_1) + Q_2(\lambda_2)$ only can be zero in the set

$$\begin{aligned} R =& \{(\lambda_1, \lambda_2) \in \mathbb{R}^2 : 0 \leq \lambda_1 \leq 1 \text{ and } \mu_2 \leq \lambda_2 \leq 0\} \\ &\cup \{(\lambda_1, \lambda_2) \in \mathbb{R}^2 : 1 \leq \lambda_1 \leq \mu_1 \text{ and } 0 \leq \lambda_2 \leq 1\}, \end{aligned}$$

see Figure 3.8. The straight lines $\lambda_2 = 0$, $\lambda_1 = 1$, $\lambda_2 = \mu_2$, $\lambda_1 = 0$, $\lambda_2 = 1$ and $\lambda_1 = \mu_1$ become $d = 0$, $d = t - 1$, $d = \mu_2(t - \mu_2)$, $d = 0$, $d = t - 1$ and $d = \mu_1(t - \mu_1)$ respectively. Then if we consider the set R in the variables (t, d) we get Figure 3.9. Now an easy computation shows that $l(f^2) = 0$ if and only if $(t, d) \in \{(0, 0), (1, 0), (2, 1)\}$. Consequently we get Theorem B(d). □

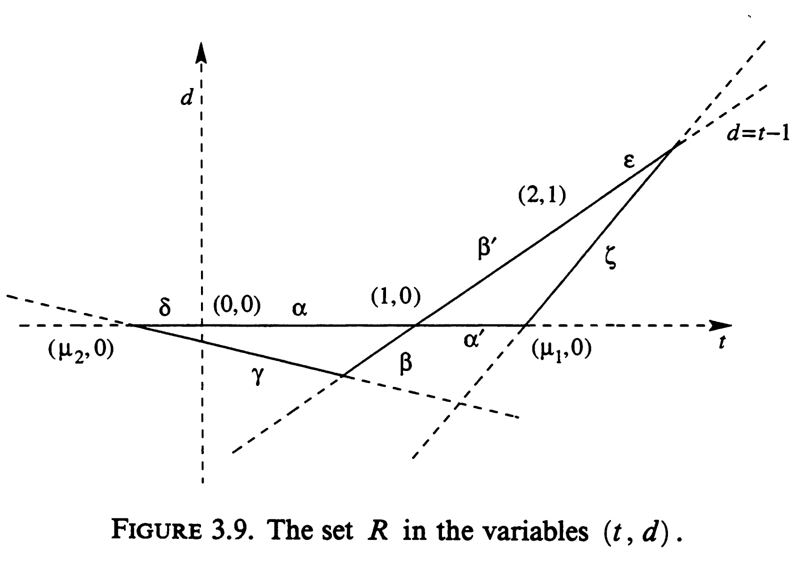

FIGURE 3.9. The set R in the variables (t, d).

4. Proof of Theorem D

In this section, the eigenvalues λ_1, λ_2 of f_{*1} can be complex. First, we want to show that this case is essentially different from the real case studied in Section 3. While in the real case we can enclose all the zeroes of $l(f^m)$ in a bounded region in the plane (t, d), this is not possible in the non-real case, where the expression of $l(f^m)$ is given by $-l(f^m) = Q_m(\lambda) + Q_m(\overline{\lambda}) = 2\mathrm{Re}(Q_m(\lambda))$ where $\lambda_1 = \lambda$, and as usual $\overline{\lambda}$ denotes the conjugate of λ and $\mathrm{Re}(\mu)$ denotes the real part of the complex μ. Recall that, if P is a polynomial map of degree m, the map $t \to P(re^{it})$ surrounds exactly m times the origin of coordinates for r sufficiently large. It means that $\mathrm{Re}(Q_m(\lambda)) = 0$, $\lambda = re^{it}$, has exactly $2m$ zeroes for each $r > r_0$ for a r_0 large enough. Therefore, we cannot enclose all the solutions of $l(f^m) = 0$ in a bounded region.

Since in general the variable λ of $\mathrm{Re}(Q_m(\lambda))$ is not real, the techniques used in Section 3 do not work. Hence the problem is to know if the algebraic curve $l(f^m) = 0$ in the (t, d)-plane has points with integer coordinates. In fact, as the following lemma shows, $l(f^m)$ is a polynomial in the variables (t, d) with integer coefficients. Then we have a diophantine problem to solve.

Lemma 4.1. *The following statements hold.*

(a) $l(f^m) \in \mathbb{Z}[t, d]$.

(b) $t | l(f^m)$ *if and only if* m *is odd.*

Proof. In Section 3 we saw that

$$l(f^m) = -\sum_{r|m} \mu\left(\frac{m}{r}\right)(\lambda_1^r + \lambda_2^r). \tag{8}$$

We will prove by induction that $\tau_r := \lambda_1^r + \lambda_2^r$ is a polynomial with integer coefficients in the variables t, d, for all $r \in \mathbb{N}$. It is easy to see that $\tau_0 = 2$ and, from the relation $\lambda_i = \left(t + (-1)^i\sqrt{t^2 - 4d}\right)/2$, that $\tau_1 = t$. On the other hand,

$$(\lambda_1^r + \lambda_2^r)(\lambda_1 + \lambda_2) = \lambda_1^{r+1} + \lambda_2^{r+1} + \lambda_1\lambda_2(\lambda_1^{r-1} + \lambda_2^{r-1}),$$

and so,

$$\tau_{r+1} = t\tau_r - d\tau_{r-1}. \tag{9}$$

This recurrence allows to end the inductive proof. Therefore, $\tau_r \in \mathbb{Z}[t, d]$ for all $r \in \mathbb{N}$ and, from the expression (8) of $l(f^m)$ and the fact that $\mu(n) \in \{-1, 0, 1\}$, (a) is proved.

Expression (9) shows that if $t|\tau_{r-1}$, then $t|\tau_{r+1}$. Since $\tau_1 = t$, it follows that $t|\tau_k$ for all k odd. Then, if m is odd, since $l(f^m)$ is the sum of factors τ_k with k odd, t divides $l(f^m)$.

If m is even, evaluating $l(f^m)$ in $t = 0$, and using that $\tau_r = -d\tau_{r-2}$ if $r \geq 2$ is even, we get

$$l(f^m)|_{t=0} = -\sum_{\substack{r|m \\ r \text{ even}}} 2\mu\left(\frac{m}{r}\right)(-d)^{r/2}.$$

This polynomial cannot be identically zero and so, (b) is proved. □

Recall that $P_m(t, d)$ is the polynomial $l(f^m)$ in the variables (t, d), $T = \{(t, d) \in \mathbb{Z}^2 : t = 0\}$, $V = \{(t, d) \in \mathbb{Z}^2 : t = 3k, d = 3k^2 \text{ for all } k \in \mathbb{Z}\}$ and

$Z_m = \{(t, d) \in \mathbb{Z}^2 : P_m(t, d) = 0\}$. We study essentially two cases. First of all, in Proposition 4.2, we describe the set Z_m for $m = p$, where p is prime. Later on, the statements 4.3–4.8 extend this result to the case $m = p^n$, where p is prime, and n a natural number.

Proposition 4.2. *The following statements hold.*

(a) $Z_2 = \{(t, \frac{t(t-1)}{2}) : t \in \mathbb{Z}\}$.

(b) $Z_3 = \{(t, \frac{t^2-1}{3})$: *for all* $t \in \mathbb{Z}$ *such that* $t \equiv 1, 2 \pmod 3\} \cup T$.

(c) $\mathrm{Card}(Z_p \setminus T)$ *is finite if* $p \geq 5$ *is a prime number. Moreover,* $Z_5 = \{(\pm 1, 1), (\pm 1, 0), (\pm 2, 1), (\pm 2, 3)\} \cup T$.

Proof. (a) $P_2(t, d) = 2d + t - t^2$. Clearly, its integer solutions satisfy $d = \frac{t(t-1)}{2}$ with $t \in \mathbb{Z}$.

(b) $P_3(t, d) = t(1 + 3d - t^2)$. So, the points $(0, d)$ for all $d \in \mathbb{Z}$, and $(t, \frac{t^2-1}{3})$ for all t such that $t \equiv 1, 2 \pmod 3$ are its integer zeroes.

(c) Substituting (λ_1, λ_2) by (t, d) in (8) and using the Newton's binomial formula, we get

$$\lambda_1{}^r + \lambda_2{}^r = \frac{1}{2^r} \sum_{k=0}^{r} \binom{r}{k} t^k \left((-1)^{r-k}(t^2 - 4d)^{\frac{r-k}{2}} + (t^2 - 4d)^{\frac{r-k}{2}}\right).$$

The factor between parentheses either will vanish if $\frac{r-k}{2} \notin \mathbb{Z}$ or will be $2(t^2 - 4d)^{\frac{r-k}{2}}$ if $\frac{r-k}{2} \in \mathbb{Z}$. Then, changing $s = \frac{r-k}{2}$, $P_m(t, d)$ can be written as

$$P_m(t, d) = -\sum_{r|m} \frac{\mu(\frac{m}{r})}{2^{r-1}} \sum_{s=0}^{[\frac{r}{2}]} \binom{r}{r-2s} t^{r-2s}(t^2 - 4d)^s.$$

When $m = p > 3$ is a prime number, this expression becomes

$$-P_p(t, d) = -t + \frac{1}{2^{p-1}} \sum_{s=0}^{\frac{p-1}{2}} \binom{p}{p-2s} t^{p-2s}(t^2 - 4d)^s.$$

Since p is odd, the last expression can be factorized by t, obtaining

$$\begin{aligned}
-\frac{P_p(t, d)}{t} &= -1 + \frac{1}{2^{p-1}} \sum_{s=0}^{\frac{p-1}{2}} \binom{p}{p-2s} t^{p-2s-1}(t^2 - 4d)^s \\
&= -1 + \frac{1}{2^{p-1}} \sum_{s=0}^{\frac{p-1}{2}} \binom{p}{p-2s} (t^2)^{\frac{p-1}{2}-s} \sum_{k=0}^{s} \binom{s}{k} (t^2)^k d^{s-k}(-4)^{s-k} \\
&= -1 + \frac{1}{2^{p-1}} \sum_{s=0}^{\frac{p-1}{2}} \binom{p}{p-2s} \sum_{k=0}^{s} \binom{s}{k} (-4)^{s-k}(t^2)^{\frac{p-1}{2}-(s-k)} d^{s-k}.
\end{aligned}$$

We remark that

$$H(t, d) := \sum_{s=0}^{\frac{p-1}{2}} \sum_{k=0}^{s} (-4)^{s-k} \binom{p}{p-2s} \binom{s}{k} (t^2)^{\frac{p-1}{2}-(s-k)} d^{s-k}$$

is a homogeneous polynomial of degree $\frac{p-1}{2}$ in the variables t^2 and d. In order to apply a theorem on diophantine equations, we will need this polynomial

If m is odd then, from (c) and (g), $Q_m(-1) = -Q_m(1) = 0$. If $4|m$ then, from (d) and (g), $Q_m(-1) = Q_m(1) = 0$. Assume that $m = 2p_2^{\alpha_2} \cdots p_n^{\alpha_n}$ with with $p_2, \dots, p_n$ distinct primes. Then, from (a) and (e), we get $Q_m(-1) = Q_{2p_2\cdots p_n}(-1) = Q_{p_2\cdots p_n}((-1)^2) - Q_{p_2\cdots p_n}(-1) = 0$. Hence (h) is proved. □

As the next theorem states,the values of $Q_m(x)$ remain bounded for $|x| \leq 1$.

Lemma 3.2. *If $m = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ with $p_1, \dots, p_n$ distinct primes, then $|Q_m(x)| \leq 2^n$ if $|x| \leq 1$.*

Proof. From the definition of $Q_m(x)$, (3) and since $|x| \leq 1$, we get

$$|Q_m(x)| = \left|\sum_{r|m} \mu(r) x^{\frac{m}{r}}\right| \leq \sum_{r|m} |\mu(r)| \left|x^{\frac{m}{r}}\right| \leq \sum_{r|m} |\mu(r)| = \sum_{k=0}^{n} \binom{n}{k} = 2^n. \quad \square$$

While in Lemma 3.1 we have studied the values of the polynomials $Q_m(x)$ at ± 1, in the next lemma we will do the same for all their derivatives. We denote by $Q_m^{(i)}(x)$ the i-th derivative of the polynomial $Q_m(x)$ with respect to the variable x.

In the following four results, the behaviour of $Q_m(x)$ for $|x| \geq 1$ is studied.

Lemma 3.3. *For all $i \in \mathbb{N}$ we have $Q_m^{(i)}(1) \geq 0$.*

Proof. First we will show that if $p_1, \dots, p_n$ are distinct prime numbers, then $Q_{p_1\cdots p_n}^{(i)}(1) \geq 0$ for all $i \in \mathbb{N}$. We will prove this by using induction with respect to n.

If $n = 1$ then $Q_{p_1}(x) = x^{p_1} - x$. Consequently, $Q_{p_1}'(x) = p_1 x^{p_1 - 1} - 1$, $Q_{p_1}^{(i)}(x) = p_1! x^{p_1 - i}/(p_1 - i)!$ if $1 < i \leq p_1$ (of course $0! = 1$), and $Q_{p_1}^{(i)}(x) = 0$ if $i > p_1$. Hence $Q_{p_1}^{(i)}(1) \geq 0$ for all $i \in \mathbb{N}$. So the lemma is true for $n = 1$.

Assume that the lemma is true for $n - 1$. Now we will prove it for n. From Lemma 3.1(b) it follows that $Q_{p_1\cdots p_n}(x) = Q_{p_2\cdots p_n}(x^{p_1}) - Q_{p_2\cdots p_n}(x)$. Then it is easy to show that

$$Q_{p_1\cdots p_n}^{(i)}(x) = Q_{p_2\cdots p_n}^{(i)}(x^{p_1})(p_1 x^{p_1 - 1})^i - Q_{p_2\cdots p_n}^{(i)}(x) + P(x), \tag{5}$$

where

$$P(x) = \sum_{1 \leq j < i} A_j(x) Q_{p_2\cdots p_n}^{(j)}(x), \tag{6}$$

and $A_j(x)$ is a polynomial in x with positive coefficients. Then, from (5), (6) and since the lemma is true for $n - 1$, it follows that

$$Q_{p_1\cdots p_n}^{(i)}(1) \geq 0. \tag{7}$$

Now suppose that $m = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ with $p_1, \dots, p_n$ distinct primes. By Lemma 3.1(a) we have $Q_m(x) = Q_{p_1\cdots p_n}(x^{\frac{m}{p_1 \cdots p_n}})$. Then

$$Q_m^{(i)}(x) = \left(\frac{d}{dx}\right)^i Q_{p_1\cdots p_n}(x^{\frac{m}{p_1\cdots p_n}}).$$

Clearly the right-hand side of the last equality can be written as

$$\sum_{1 \leq j \leq i} B_j(x) Q_{p_1\cdots p_n}^{(j)}(x^{\frac{m}{p_1\cdots p_n}}),$$

where $\eta_1 = \mu_1^{p^{n-1}}$ and $\eta_2 = \mu_2^{p^{n-1}}$. Set $x = \eta_1 + \eta_2$ and $y = \eta_1\eta_2$. It is clear that $P_p(x, y) = 0$. Taking into account the relation $\mu_i = \frac{z+(-1)^i\sqrt{z^2-4w}}{2}$, for $i = 1, 2$, the first part of statement (a) follows.

We note that expression (9) can be adapted to this case. If we consider $\tau_r = \mu_1^r + \mu_2^r$, relation (9) writes as:

$$\tau_{r+1} = z\tau_r - w\tau_{r-1},$$

with $\tau_0 = 2$ and $\tau_1 = z$. On the other hand, we remark that $x = \tau_{p^{n-1}}$. As in Lemma 4.1(a), we can conclude that $x = F(z, w)$, where F is a polynomial with integer coefficients. We have also $y = w^{p^{n-1}}$. Then, if z and w are integers, so x and y are, and the second part of (a) is proved.

Conversely, if $P_p(x, y)$ vanishes and $\eta_i = \frac{x+(-1)^i\sqrt{x^2-4y}}{2}$ for $i = 1, 2$, then

$$Q_p(\eta_1) + Q_p(\eta_2) = Q_{p^n}(\mu_1) + Q_{p^n}(\mu_2) = 0,$$

where $\eta_i = \mu_i^{p^{n-1}}$ for $i = 1, 2$. Denoting by $z = \mu_1 + \mu_2$ and $w = \mu_1\mu_2$, we have that $P_{p^n}(z, w) = 0$. From the above relations, z and w can be written as:

$$z = \sqrt[p^{n-1}]{\frac{x + \sqrt{x^2 - 4y}}{2}} + \sqrt[p^{n-1}]{\frac{x - \sqrt{x^2 - 4y}}{2}}; \quad \text{and } w = \sqrt[p^{n-1}]{y}.$$

Then, statement (b) is proved. □

We note that the formula given in Lemma 4.3(b) shows that $(x, y) \in \mathbb{Z}^2$ does not imply $(z, w) \in \mathbb{Z}^2$. Furthermore, the p^{n-1}-roots that appear in the expression of z may not take the same determination as complex numbers.

On the other hand, Lemma 4.3(a) induces a map g_{p^n} from the integer zeroes of P_{p^n} to the integer zeroes of P_p.

Corollary 4.4. *Let (t, d) be an integer zero of P_p and g_{p^n} be the map defined above. Then,* $\mathrm{Card}(\{g_{p^n}^{-1}(t, d)\})$ *is finite.*

Proof. We have that $P_p(t, d) = 0$ and $\{g_{p^n}^{-1}(t, d)\} \subset S = \{(T, D) : D = \sqrt[p^{n-1}]{d}\}$. By Theorem B, there is a finite number of elements (T, D) of S such that $T^2 - 4D > 0$. So, we only have to prove the finiteness in the case $T^2 - 4D < 0$. We note that for each d the number of $D = \sqrt[p^{n-1}]{d}$ is finite and, also, for each D the number of T such that $T^2 - 4D < 0$ is finite. So, the corollary is proved. □

However, in the statement of Proposition 4.2 we can see that, for p a prime number, some Z_p contain the infinite sets T, V, $\{(t, \frac{t(t-1)}{2}) : t \in \mathbb{Z}\}$ and $\{(t, \frac{t^2-1}{3}) :$ for all $t \in \mathbb{Z}$ such that $t \equiv 1, 2 \pmod 3\}$. The three following results are devoted to analyse how these sets generate integer solutions of $P_m(t, d) = 0$ when $m = p^n$, by means of the action of $g_{p^n}^{-1}$.

Lemma 4.5. *Assume that $p \geq 3$ is a prime number and $n \in \mathbb{N}$. Suppose that d is an integer number.*

(a) *If $p = 3$ and $n \geq 2$, then $\{g_{p^n}^{-1}(T)\} \cap \mathbb{Z}^2 = V \cup T$.*
(b) *If $p > 3$ and $n \geq 2$, then $\{g_{p^n}^{-1}(T)\} \cap \mathbb{Z}^2 = T$.*
(c) *$V \subset Z_{9n}$ for all n.*

Proof. We take an integer solution $(0, d) \in T$ of P_p. From Lemma 4.3(b), this solution gives a finite number of solutions of P_{p^n}. We are interested in knowing which of them are integer. The solution $(0, d)$ can be written in (λ_1, λ_2) coordinates as $(\sqrt{-d}, -\sqrt{-d})$. Assume that $d > 0$. Otherwise, the proof is similar. If we call $(\lambda_1^*, \lambda_2^*) = (\sqrt[p^{n-1}]{\sqrt{-d}}, \sqrt[p^{n-1}]{-\sqrt{-d}})$ by Lemma 3.1(a), we have that $P_{p^n}(\lambda_1^*, \lambda_2^*) = P_p(\sqrt{-d}, -\sqrt{-d}) = 0$. Recall that the different p^{n-1}-roots do not need to have the same determination.

We remark that we are looking for λ_1^*, λ_2^* satisfying $\lambda_1^* + \lambda_2^* \in \mathbb{Z}$ and $\lambda_1^*\lambda_2^* \in \mathbb{Z}$. Using polar coordinates,

$$\begin{aligned}(\lambda_1^*, \lambda_2^*) &= \left(\sqrt[p^{n-1}]{(\sqrt{d})_{\frac{\pi}{2}+2k\pi}}, \sqrt[p^{n-1}]{(\sqrt{d})_{\frac{3\pi}{2}+2k\pi}}\right) \\ &= \left(\left(\sqrt[p^{n-1}]{\sqrt{d}}\right)_{\frac{\frac{\pi}{2}+2k\pi}{p^{n-1}}}, \left(\sqrt[p^{n-1}]{\sqrt{d}}\right)_{\frac{\frac{3\pi}{2}+2k\pi+2l\pi}{p^{n-1}}}\right)\end{aligned}$$

Setting $\alpha_1 = \frac{\frac{\pi}{2}+2k\pi}{p^{n-1}}$ and $\alpha_2 = \frac{\frac{3\pi}{2}+2k\pi+2l\pi}{p^{n-1}}$, then

$$\lambda_1^* + \lambda_2^* = \sqrt[p^{n-1}]{\sqrt{d}}\,((\cos\alpha_1 + \cos\alpha_2) + i(\sin\alpha_1 + \sin\alpha_2)).$$

In order to have $\lambda_1^* + \lambda_2^* \in \mathbb{R}$, we need that $\sin\alpha_1 + \sin\alpha_2 = 0$. So,

$$\cos\alpha_1 + \cos\alpha_2 = \pm\cos\left(\frac{\pi + 2l\pi}{2p^{n-1}}\right).$$

Hence, $(\lambda_1^* + \lambda_2^*)$ in (t, d) coordinates writes as

$$\left(\pm 2\cos\left(\frac{\pi + 2l\pi}{2p^{n-1}}\right)\sqrt[p^{n-1}]{\sqrt{d}}, \sqrt[p^{n-1}]{\sqrt{d}}\right),$$

where $l \in \mathbb{Z}$. We want these two coordinates be integer. Let $s = \sqrt[p^{n-1}]{\sqrt{d}} \in \mathbb{Z}$. We wonder when $2\sqrt{s}\cos\left(\frac{\pi+2l\pi}{2p^{n-1}}\right) \in \mathbb{Z}$. Using the basic relation $2\cos^2\alpha - 1 = \cos 2\alpha$, this last condition can be thought as

$$\cos\left(\frac{1+2l}{p^{n-1}}\pi\right) \in \mathbb{Q}.$$

For $d < 0$, one gets the same condition.

By [N, p.41], the only rational values of $\cos(r\pi)$ with $r \in \mathbb{Q}$ are as follows: 0, $\pm\frac{1}{2}$, ± 1. These values can only be achieved if $\frac{1+2l}{p^{n-1}} \in \{\frac{1}{2}, \frac{3}{2}, \frac{1}{3}, \frac{2}{3}, \frac{4}{3}, \frac{5}{3}, 0, 1\}$. Since $1+2l$ is odd and $p \neq 2$ is a prime number, we can remove $\frac{1}{2}$, $\frac{3}{2}$, $\frac{2}{3}$, $\frac{4}{3}$ and 0. There remain three values to analyse: $\frac{1}{3}$, $\frac{5}{3}$ and 1. The first and the second ones are only possible when $p = 3$ and the last one, for all prime number $p > 2$.

TABLE 1

$\frac{1+2l}{p^{n-1}}$	$(t, d) = \left(\pm 2\cos\left(\frac{\pi+2l\pi}{2p^{n-1}}\right) \sqrt[p^{n-1}]{\sqrt{d}}, \sqrt[p^{n-1}]{d}\right)$	valid for
$\frac{1}{3}$	$(\sqrt{3s}, s)$	$p = 3$
$\frac{5}{3}$	$(-\sqrt{3s}, s)$	$p = 3$
1	$(0, s)$	$p \neq 2$

From Table 1, if $p = 3$, the integer zeroes of P_{3^n} coming from $(0, d)$ can be $\{(3q, 3q^2) : q \in \mathbb{Z}\}$ or $\{(0, q) : q \in \mathbb{Z}\}$ (that is to say, belonging to $T \cup V$).

In the case $p > 3$, there only can appear integer zeroes in T.

We know from Lemma 4.1(b) that $P_{p^n}(0, q) = 0$ for all $q \in \mathbb{Z}$, $p > 2$ and $n \in \mathbb{N}$.

We only need to show that $P_{3^n}(3q, 3q^2) = 0$ for all $q \in \mathbb{Z}$ and $n \in \mathbb{N}$. The pair $(3q, 3q^2)$ becomes in polar coordinates as $\lambda_1 = (\sqrt{3}q)_{\frac{\pi}{6}}$, $\lambda_2 = (\sqrt{3}q)_{-\frac{\pi}{6}}$. We observe that

$$\lambda_1^{3j} + \lambda_2^{3j} = (\sqrt{3}q)^{3j}{}_{\frac{\pi}{2}j} + (\sqrt{3}q)^{3j}{}_{-\frac{\pi}{2}j} = 0, \tag{10}$$

for all $j \in \mathbb{N}$.

Since $l(f^{3^n}) = (\lambda_1^{3^n} + \lambda_2^{3^n}) - (\lambda_1^{3^{n-1}} + \lambda_2^{3^{n-1}})$, by (10) $P_{3^n}(3q, 3q^2) = 0$ for all $q \in \mathbb{Z}$. So, statement (a) and (b) are proved.

In addition, we remark that $l(f^{9n})$ can be written as the sum of factors of type $\lambda_1^{3j} + \lambda_2^{3j}$ with $j \in \mathbb{Z}$. So (c) follows. □

We also need to control the other infinite sets that appear in Z_m when m is a prime number (see Proposition 4.2). Before stating the next result, we give the following lemma:

Lemma 4.6 (see [Mo, p. 265]). *If α, β, γ and δ are integers, and $\alpha\delta \neq 0$, $\beta^2 - 4\alpha\gamma \neq 0$, $s \geq 3$, then the equation $\alpha t^2 + \beta t + \gamma = \delta D^s$, has only a finite number of integer solutions (t, D).*

Proposition 4.7. *The following statements hold.*

(a) *If $p = 2$ and $n \geq 3$, then* $\mathrm{Card}(\{g_{p^n}^{-1}(t, \frac{t(t-1)}{2}) : t \in \mathbb{Z}\} \cap \mathbb{Z}^2) < \infty$.

(b) *If $p = 3$ and $n \geq 2$, then* $\mathrm{Card}(\{g_{p^n}^{-1}(t, \frac{t(t^2-1)}{3}) : t \in \mathbb{Z}, t \equiv 0, 1 \pmod 3)\} \cap \mathbb{Z}^2) < \infty$.

Proof. By Lemma 4.3(a) we know that an integer zero (T, D) of P_{2^n} gives one integer zero $(t, D^{2^{n-1}})$ of P_2. Since we look for $g_{p^n}^{-1}(t, \frac{t(t-1)}{2})$, by Proposition 4.2(a), the equality $t(t-1) = 2D^{2^{n-1}}$ must be satisfied.

Using Lemma 4.6 with $\alpha = 1$, $\beta = -1$, $\gamma = 0$, $\delta = 2$, this equation has a finite number of integer solutions if $2^{n-1} \geq 3$. Then, (a) is proved.

By similar arguments, from Proposition 4.2(b) and Lemma 4.3(a), if (T, D) is an integer zero of P_{3^n}, it gives an integer zero $(t, D^{3^{n-1}})$ of P_3. If this zero belongs to $\{(t, \frac{t^2-1}{3}) : t \in \mathbb{Z}, t \equiv 1, 2 \pmod 3)\}$, then $t^2 - 1 = 3D^{3^{n-1}}$. Using again Lemma 4.6 with $\alpha = 1$, $\beta = 0$, $\gamma = -1$, $\delta = 3$, we finish the proof. □

In the previous result, the power $m = 2^2$ is not covered. We give the study of this particular case in the next proposition.

Proposition 4.8. $Z_4 = \{(\pm 1, 1), (\pm 1, 0), (0, -1), (0, 0), (\pm 2, 1), (\pm 2, 6)\}$.

Proof. It can be seen that $-P_4(t, d) = 2d^2 + (2-4t^2)d + t^4 - t^2$. So we are finding pairs (t, d) such that $t \in \mathbb{Z}$ and $d = (2t^2 - 1 \pm \sqrt{(t^2)^2 + (t^2-1)^2})/2 \in \mathbb{Z}$. A necessary condition is that $(t^2)^2 + (t^2-1)^2 = s^2$, with $s \in \mathbb{Z}$. If $t^2 = 0$ then $d = 0, -1$. If $t^2 - 1 = 0$ then $d = 0, 1$. Otherwise, when $(X, Y) = 1$ the solutions of the equation $X^2 + Y^2 = Z^2$ can be written as (see [Mo, p. 13]) $X = 2uv$, $Y = u^2 - v^2$ and $Z = u^2 + v^2$, where $(u, v) = 1$. Since in our case, X and Y are consecutive, we have $u^2 - v^2 = 2uv \pm 1$.

By the change $\overline{u} = u - v$, $\overline{v} = u + v$, this equation becomes $\overline{u}^2 - 2v^2 = \pm 1$. Since X or Y must be equal to t^2, we distinguish the two following cases.

Case (i). $X = t^2$. Then, since $(u, v) = 1$, either

$$u = 2a_1^2 \text{ and } v = b_1^2, \quad \text{or} \quad u = a_2^2 \text{ and } v = 2b_2^2,$$

for some integer numbers a_i, b_i, $i = 1, 2$. These cases are respectively equivalent to the following two systems:

$$(11^{\pm}) \qquad \begin{cases} \overline{u}^2 - 2b_1^4 = \pm 1, \\ \overline{u} + b_1^2 = 2a_1^2; \end{cases}$$

$$(12^{\pm}) \qquad \begin{cases} \overline{u}^2 - 8b_2^4 = \pm 1, \\ \overline{u} + 2b_2^2 = a_2^2. \end{cases}$$

Case (ii). $Y = t^2$. Then, $\overline{u} = a_3^2$ and $\overline{v} = b_3^2$ with a_3 and b_3 integer numbers. As in the previous case, this situation can be expressed in terms of a system:

$$(13^{\pm}) \qquad \begin{cases} a_3^4 - 2v^2 = \pm 1, \\ a_3^2 + 2v = b_3^2. \end{cases}$$

Hence the problem has been divided into three particular diophantine equations. In fact, due to the term ± 1, we have six different systems to solve. Each one of them is studied using known results that only refer to that concrete case.

By [Mo, p. 269] and taking into account that $(u, v) = 1$, system (11^+) has no integer solutions.

By [Mo, p. 271], $\overline{u}^2 - 2b_1^4 = -1$ has two integer solutions $(\overline{u}, b_1)$: $(1, 1)$ and $(239, 13)$. But only the first one satisfies $\overline{u} + b_1^2 = 2a_1^2$. In the coordinates (X, Y) it corresponds to the point $(4, 3)$, which implies $(t, d) = (\pm 2, 1)$ and $(t, d) = (\pm 2, 6)$.

By [Mo, p. 270], the first equation of system (12^+) has at most two solutions, which must satisfy that $\overline{u} + 2b_2^2\sqrt{2} \in \{\epsilon, \epsilon^2, \epsilon^4\}$, where $\epsilon = 1 + \sqrt{2}$. In fact, only $(\overline{u}, b_2) = (3, 1)$ arises. But, it does not satisfy the second equation of (12^+).

System (12^-) has no solutions because $\overline{u}^2 \not\equiv -1 \pmod 8$.

By [C2], system (13^+) has no integer solutions.

By [L], system (13^-) has only one integer solution, which is $(\overline{u}, b_2) = (1, 1)$. As in (11^-), it implies $(X, Y) = (4, 3)$ and so, it does not provide new solutions.

After this analysis, we have proved that only the pairs $(\pm 1, 0)$, $(\pm 1, 1)$, $(0, 0)$, $(0, -1)$, $(\pm 2, 1)$ and $(\pm 2, 6)$ can vanish the polynomial $P_4(t, d)$. It is easy to check that they actually vanish it. So, the proposition follows. □

Proof of statement (a) *of Theorem* D. Both claims follow immediately from Lemmas 4.1(b) and 4.5(c), respectively. □

Proof of statement (b) *of Theorem* D. It follows easily from Propositions 4.2(a), 4.8 and 4.7(a), respectively. □

Proof of statement (c) *of Theorem* D. By Proposition 4.2(b), $Z_3 = \{(t, \frac{t^2-1}{3}) :$ for all $t \in \mathbb{Z}$ such that $t \equiv 1, 2 \pmod 3\} \cup T$ and, by Lemma 4.5(a) we get that $V \subset Z_{3^n}$. Finally, if $m = 3^n$ and $n \geq 2$, from Proposition 4.2(b), Lemma 4.5(a) and Proposition 4.7(b), we obtain that $\operatorname{Card}(Z_m \setminus \{T \cup V\}) < \infty$. □

Proof of statement (d) *of Theorem* D. By Proposition 4.2(c) if $p \geq 5$ then $\operatorname{Card}(Z_p \setminus T)$ is finite. So, by Corollary 4.4, $\operatorname{Card}(Z_{p^n} \setminus T)$ is also finite. Proposition 4.2(c) gives also the description of $Z_5 \setminus T$. We only have to see that $Z_{5^n} \setminus T = \{(\pm 1, 1), (\pm 1, 0), (\pm 2, 1)\}$.

We have obtained $Z_5 = \{(\pm 1, 1), (\pm 1, 0), (\pm 2, 1), (\pm 2, 3)\} \cup T$. From Lemma 4.5(b), $g_{p^n}^{-1}(T) = T$. By Lemma 4.3(b), $g_{p^n}^{-1}(\pm 2, 3) \notin \mathbb{Z}^2$ for all $n \geq 2$. Putting $(\pm 1, 1), (\pm 1, 0), (\pm 2, 1)$ in polar coordinates we can see that $g_{p^n}^{-1}(\{(\pm 1, 1), (\pm 1, 0), (\pm 2, 1)\}) = \{(\pm 1, 1), (\pm 1, 0), (\pm 2, 1)\}$. So (d) is proved. □

Proof of statement (e) *of Theorem* D. If $p > 5$, from Lemma 4.5(b), $g_{p^n}^{-1}(T) = T$. In (d) we state that $Z_p \setminus T$ is finite. As in the above case,

$$g_{p^n}^{-1}(\{(\pm 1, 1), (\pm 1, 0), (\pm 2, 1)\}) = \{(\pm 1, 1), (\pm 1, 0), (\pm 2, 1)\}.$$

If there exist other points of $Z_p \setminus T$, it is sure that $d > 1$. Let $d_0 = \max\{|d| : (t, d) \in (Z_p \setminus T)\}$. For each p, there exists a $n_0(p)$ such that the complex modulus of $\sqrt[p^{n-1}]{d_0} \in (1, 2)$. By Lemma 4.3(b), the elements of $\{g_{p^n}^{-1}(t, d)\}$, with $(t, d) \in (Z_p \setminus \{T \cup \{(\pm 1, 1), (\pm 1, 0), (\pm 2, 1)\}\})$ cannot have integer coordinates. So (e) follows. □

Proof of statement (f) *of Theorem* D. Recall that $\tau_r = \lambda_1^r + \lambda_2^r$. We observe from (8) and the definition of τ_r that $l(f^m) = -\sum_{r|m} \mu(\frac{m}{r})\tau_r$.

If $(t, d) = (-1, 1)$ we can check easily from (9) that $\tau_r = 2$ if $r \equiv 0 \pmod 3$, and $\tau_r = -1$ if $r \equiv 1, 2 \pmod 3$. We distinguish the three following cases.

Case (i). If $3 \nmid m$, r never is a multiple of 3. So $\tau_r = -1$ and $l(f^m) = \sum_{r|m} \mu(\frac{m}{r})$. Therefore, $l(f^m) = 1$ if $m = 1$, and $l(f^m) = 0$ if $m \neq 1$.

Case (ii). If $3^2 | m$, r is always a multiple of 3. So $\tau_r = 2$ and $l(f^m) = -2\sum_{r|m} \mu(\frac{m}{r})$. Therefore, $l(f^m) = -2$ if $m = 1$, and $l(f^m) = 0$ if $m \neq 1$.

Case (iii). If $3|m$ and $3^2 \nmid m$, we take $\overline{m} = m/3$ (obviously, $3 \nmid \overline{m}$). Applying similar arguments to those of Lemma 3.1(b) we can write

$$\begin{aligned} l(f^m) &= -\sum_{r|\overline{m}} \mu\left(\frac{\overline{m}}{r}\right)\tau_{3r} + \sum_{r|\overline{m}} \mu\left(\frac{\overline{m}}{r}\right)\tau_r \\ &= -2\sum_{r|\overline{m}} \mu\left(\frac{\overline{m}}{r}\right) - \sum_{r|\overline{m}} \mu\left(\frac{\overline{m}}{r}\right). \end{aligned}$$

So $l(f^m) = 0$ except for the case when $\overline{m} = 1$. Then, $m = 3$ and $l(f^m) = 3$.

If $(t, d) = (1, 1)$, we get other values of τ_r according to the congruences of r with respect to 3 and we have to deal with more cases. However, the ideas and the scheme of the proof are the same that we have used in the case $(t, d) = (-1, 1)$. □

Appendix. One 3-dimensional compact manifold with homology given by (1)

Let X be the three-dimensional compact manifold $S^3 \setminus V$ where V is the connected sum of two open solid tori, one of them knotted, see Figure 1.1. The space X can be retracted to Y where Y is $S^3 \setminus W$ and W is homeomorphic to $S^1 \vee S^1$ with one of the S^1 knotted, see Figure A.1.

The spaces X and Y have the same homologic groups. Since W and S^3 are compact we can apply Alexander's duality theorem [G, Theorem 27.5] which under our assumptions states that

$$\check{H}^q(W) \simeq H_{3-q}(S^3, S^3 \setminus W), \qquad q = 0, \dots, 3,$$

where $\check{H}^q(W)$ is the Alexander-Čech cohomology of W and $H_{3-q}(S^3, S^3 \setminus W)$ are the relative homology groups. Since the homology sequence

$$\cdots \to H_q(S^3 \setminus W) \to H_q(S^3) \to H_q(S^3, S^3 \setminus W) \to H_{q-1}(S^3 \setminus W) \to \cdots$$

is exact (see [G, Theorem 14.1]) we can compute $H_q(S^3 \setminus W)$ if we know $H_q(S^3, S^3 \setminus W)$ which is isomorphic to $\check{H}^q(W)$ as we have already seen. But this cohomologic group is intrinsic to W, so if instead of W we consider $W^* = S^1 \vee S^1$, see Figure A.2, we see that $\check{H}^q(W) \simeq \check{H}^q(W^*)$ because W is homeomorphic to W^*.

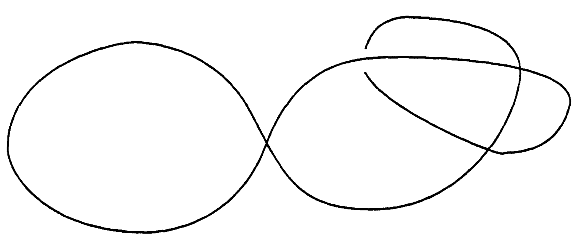

Figure A.1. The space W.

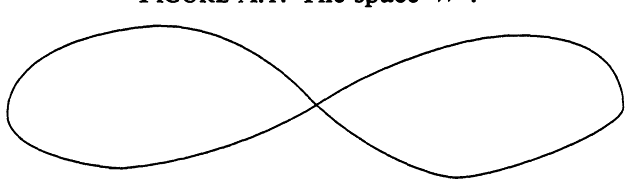

Figure A.2. The space W^*.

Now if we consider the homology sequence

$$\cdots \to H_q(S^3 \setminus W^*) \to H_q(S^3) \to H_q(S^3, S^3 \setminus W^*) \to H_{q-1}(S^3 \setminus W^*) \to \cdots,$$

since $H_q(S^3, S^3 \setminus W) \simeq H_q(S^3, S^3 \setminus W^*)$ it follows that $S^3 \setminus W$ has the same homology groups as $S^3 \setminus W^*$, i.e., the homology does not "see" the knot. As $S^3 \setminus W^*$ is homeomorphic to $R^3 \setminus \{r_1 \cup r_2\}$, r_1, r_2 being two straight lines that do not cross, one concludes that

$$\begin{aligned} H_0(X) &\simeq H_0(S^3 \setminus W^*) = \mathbb{Q}, \\ H_1(X) &\simeq H_1(S^3 \setminus W^*) = \mathbb{Q} \oplus \mathbb{Q}, \\ H_q(X) &\simeq H_q(S^3 \setminus W^*) = 0, \quad q \geq 2. \end{aligned}$$

Acknowledgment

We want to thank Enric Nart and Xavier Xarles for their useful comments.

References

[ALM] L. Alsedà, J. Llibre and M. Misiurewicz, *Combinatorial dynamics and entropy in dimension one*, Advanced Series in Nonlinear Dynamics, Vol. 5, World Scientific, Singapore, 1993.

[BB] I.K. Babenko and S.A. Bogatyi, *The behavior of the index of periodic points under iterations of a mapping*, Math. USSR Izv. **38** (1992), 1–26.

[B] R.F. Brown, *The Lefschetz fixed point theorem*, Scott, Foresman and Company, Glenview, IL, 1971.

[C1] J.H.E. Cohn, *Eight diophantine equations*, Proc. London Math. Soc. **16** (1966), 153–166.

[C2] ——, *The diophantine equation* $x^4 - Dy^2 = 1$, J. Math. Oxford Ser. **26** (1975), 279–281.

[CLN1] J. Casasayas, J. Llibre and A. Nunes, *Periodic orbits of transversal maps*, preprint, Univ. Autònoma de Barcelona, 1991.

[CLN2] ——, *Periods and Lefschetz zeta functions*, Pacific J. Math. **165** (1994), 51–66.

[D] A. Dold, *Fixed point indices of iterated maps*, Invent. Math. **74** (1983), 419–435.

[F1] J. Franks, *Some smooth maps with infinitely many hyperbolic periodic points*, Trans. Amer. Math. Soc. **226** (1977), 175–179.

[F2] J. Franks, *Homology and dynamical systems*, CBMS Regional Conf. Ser. in Math., no. 49, Amer. Math. Soc., Providence, R.I., 1982.

[F3] J. Franks, *Period doubling and the Lefschetz formula*, Trans. Amer. Math. Soc. **287** (1985), 275–283.

[G] M. Greenberg, *Lectures on algebraic topology*, Benjamin, Menlo Park, CA, 1971.

[H] B. Halpern, *Nielsen type numbers for periodic points* (unpublished).

[HPY] P. Heath, R. Piccinini and C.Y. You, *Nielsen type numbers for periodic points* I, Lecture Notes in Math., vol. 1411, Springer, 1989, pp. 88–106.

[L] W. Ljunggren, *Ein Satz über die diophantische Gleichung* $Ax^2 - By^4 = C$ $(C = 1, 2, 4)$, Tolfte Skandinaviska Metematikerkongressen, Lund, 1953, pp. 188–194.

[Ll] J. Llibre, *Lefschetz numbers for periodic points*, Contemporary Math., vol. 152, Amer. Math. Soc., Providence, RI, 1993, pp. 215–227.

[M] T. Matsuoka, *The number of periodic points of smooth maps*, Ergodic Theory Dynamical Systems **9** (1989), 153–163.

[Mo] L.J. Mordell, *Diophantine equations*, Pure and Applied Mathematics, vol. 30, Academic Press, London, 1969.

[MS] T. Matsuoka and H. Shiraki, *Smooth maps with finitely many periodic points*, Mem. Fac. Sci. Kochi. Univ. (Math.) **11** (1990), 1–6.

[N] I. Niven, *Irrational numbers*, The Carus Math. Monographs, 11, The Math. Assoc. of America, 1956.

[NZ] I. Niven and H.S. Zuckerman, *An introduction to the theory of numbers*, 4th ed., Wiley, New York, 1980.

[S] A. N. Sharkovskii, *Co-existence of a cycles of a continuous map mapping of the line into itself*, Ukrain. Math. Zh. **16** (1964), 61–67. (Russian)

Departament de Matemàtiques, Universitat Autònoma de Barcelona, Bellaterra, 08193 Barcelona, Spain

Current address (A. Guillamon): Departament de Matemàtica Aplicada I, E.U.P.B, Universitat Politècnica de Catalunya, 08028 Barcelona, Spain

Departament d'Economia i Història Econòmica, Universitat Autònoma de Barcelona, Bellaterra, 08193 Barcelona, Spain

Current address (X. Jarque): Departament d'Economia i Història Econòmica, Universitat Autònoma de Barcelona, Bellaterra, 08193 Barcelona, Spain

Current address (J. LLibre, J. Torregrosa): Departament de Matemàtiques, Universitat Autònoma de Barcelona, Bellaterra, 08193 Barcelona, Spain

Current address (J. Ortega): Departament de Matemàtica Aplicada I, E.T.S.E.I.B, Universitat Politècnica de Catalunya, 08028 Barcelona, Spain