Publ. Math. Debrecen
84/3-4 (2014), 399–414
DOI: 10.5486/PMD.2013.5755

An algorithm determining cycles of polynomial mappings in integral domains

By TADEUSZ PEZDA (Wrocław)

Abstract. In the first part of this paper we show how all normalized cycles could be found in a domain R, provided all nontrivial solutions in units of $u+v=1$ and $u+v+w=1$ are given. Then we give an effective method to find all normalized cycles in the ring of integers Z_K in any algebraic number field K. Finally, we deal with polynomial orbits.

For a commutative ring S with unity a tuple $(x_0, x_1, \dots, x_{n-1})$ of distinct elements from S is called a *(polynomial) cycle* if for some $f \in S[X]$ we have $f(x_0) = x_1,\ f(x_1) = x_2, \dots, f(x_{n-2}) = x_{n-1},\ f(x_{n-1}) = x_0$. The number n is called the *length* of this cycle. A cycle $x_0, x_1, \dots$ is called *normalized* provided $x_0 = 0$, $x_1 = 1$.

In the first section we show how all normalized cycles could be found in a domain R, provided all nontrivial solutions in units of $u+v=1$ and $u+v+w=1$ are given. In the second section we give an effective method to find all normalized cycles in the ring of integers Z_K in any algebraic number field K. In the last section we deal with polynomial orbits.

1. A usefulness of $u+v=1$ and $u+v+w=1$ in units

In [H-KNa2] the following theorem was established:

Mathematics Subject Classification: 11R04, 11R21, 11R27.
Key words and phrases: polynomial cycles, Dedekind rings, 2-unit equations.
Supported by the MNiSW Grant N N201 366636.

Theorem 0. *Let R be an integral domain and assume that for every nonzero $b \in R$ each of the equations: $x_1 + bx_2 = 1$, $b(x_1 + x_2) + x_3 = 1$, $x_1 + x_2 + x_3 + x_4 + x_5 = 1$ has only finitely many nontrivial solutions $x_i \in R^\times$. Then there are only finitely many normalized cycles in R of a given length.*

Let R be a commutative domain in which the equations $u + v = 1$ and $u + v + w = 1$ have only finitely many solutions in units $\neq 1$ (this assumption is satisfied for finitely generated domains of 0 characteristics). Let us define $\mathcal{A}$ as the set of all solutions $(\alpha_i, \beta_i, \gamma_i)$, $i = 1, \dots, m$ of $\alpha + \beta + \gamma = 1$ with invertible α, β, γ distinct from 1, and $|\mathcal{A}| = m$. We also define $\mathcal{B}$ as the set of all solutions (δ_j, ϵ_j), $j = 1, \dots, m_1$ of $\delta + \epsilon = 1$ with invertible δ, ϵ, and $|\mathcal{B}| = m_1$. In the following theorem we improve Theorem 0.

Theorem 1. *Let $R, \mathcal{A}, \mathcal{B}$ be as above.*

(i) *The lengths of cycles in R are bounded by $6(m+2)^2$.*

(ii) *Fix $n \leq 6(m+2)^2$ and $n \neq 4$. We define a family of sets $\mathcal{X}_j$ as follows.*
Put $\mathcal{X}_1 = \{1\}$. For odd n we put $\mathcal{X}_2 = \{1 - \delta_j : j = 1, \dots, m_1\}$. For even $n \neq 6, 12$ we put $\mathcal{X}_2 = \{1 - \alpha_i : i = 1, \dots, m\}$. For $n = 12$ we put $\mathcal{X}_2 = \{1 - \alpha_i, 1 + \alpha_i : i = 1, \dots, m\}$. For $n = 6$ we put $\mathcal{X}_2 = \{1 - \alpha_i : i = 1, \dots, m\} \cup \{1 - \xi, 1 - \xi^2\}$, where $\xi \in R$ is a primitive third root of unity (if it exists in R, otherwise we skip the second component).
Having defined $\mathcal{X}_1, \mathcal{X}_2$, we define inductively $\mathcal{X}_i$ for $i \geq 3$ by
$\mathcal{X}_i = \{a(x-y) + y : a \in \mathcal{X}_2,\ x \in \mathcal{X}_{i-1},\ y \in \mathcal{X}_{i-2}, x - y \text{ is invertible}\}$.
Then for $n \neq 4, 6$ any normalized cycle $(x_0 = 0, x_1 = 1, x_2, \dots, x_{n-1})$ of length n satisfies $x_i \in \mathcal{X}_i$.
Any normalized cycle $(x_0 = 0, x_1 = 1, x_2, \dots, x_5)$ of length 6 satisfies $x_i \in \mathcal{X}_i$, except for $\operatorname{char} R = 3$, where, in addition, $(0, 1, 1-u, 2-u, u-1, u)$ is a cycle for any invertible $u \neq 1, 2$.

(iii) *Any normalized cycle in R of length 4 is of one of the following forms:*
   (a) *$(0, 1, 1-\alpha_i, \beta_i)$, where $1 \leq i \leq m$ and the ratio $(1-\alpha_i)/(1-\beta_i)$ is invertible;*
   (b) *$(0, 1, 1+\alpha_i, \alpha_i)$, where $1 \leq i \leq m$ and the ratio $(1+\alpha_i)/(1-\alpha_i)$ is invertible;*
   (c) *$(0, 1, 1+\epsilon, \epsilon)$, where ϵ satisfies $\epsilon^2 + 1 = 0$;*
   (d) *(only for $\operatorname{char} R = 2$) $(0, 1, 1+v, v)$, where v is any unit $\neq 1$.*

Proof. (i) Let $(0, 1, x_2, \dots, x_{n-1})$ be a cycle. Lemma 1 from [Na1] gives that for any $1 \leq k \leq n-1$ satisfying $(k(k-2), n) = 1$ the elements x_k, $x_1 - x_2 = 1 - x_2$

and $x_2 - x_k$ are invertible. Thus for such k the triples $(\alpha, \beta, \gamma) = (1 - x_2, x_2 - x_k, x_k)$ are distinct solutions of the 3-unit equation $\alpha + \beta + \gamma = 1$. Among them there are at most two trivial solutions, i.e. when $k = 1$ or $x_2 - x_k = 1$. Thus the number l of integers $k \in [1, n-1]$ satisfying $(k(k-2), n) = 1$ cannot exceed $m + 2$. Since

$$l = \begin{cases} n \prod_{p|n} \left(1 - \dfrac{2}{p}\right) & \text{if } 2 \nmid n, \\ \dfrac{n}{2} \prod_{2 \neq p|n} \left(1 - \dfrac{2}{p}\right) & \text{if } 2 \mid n, \end{cases} \tag{1}$$

and $p^\alpha(1 - 2/p) \geq \sqrt{p^\alpha}$ for prime $p \geq 5$ and $\alpha \geq 1$, we get $m + 2 \geq l \geq \sqrt{n}/\sqrt{6}$. Thus $n \leq 6(m+2)^2$.

(ii) Let $n \geq 3$ and let $(0, 1, x_2, \ldots, x_{n-1})$ be a cycle in R. Our first aim is to prove that $x_2 \in \mathcal{X}_2$.

If n is odd, then $1 - x_2 = x_1 - x_2$ and x_2 are invertible. Thus $x_2 = 1 - \delta_j$ for some $1 \leq j \leq m_1$. Hence $x_2 \in \mathcal{X}_2$.

Assume now that $n \neq 4, 6, 12$ is even. Then the number l from (1) satisfies $l \geq 3$. So there exists $k \in [2, n-1]$ such that $(k(k-2), n) = 1$ and $x_2 - x_k \neq 1$. Hence $(1 - x_2, x_2 - x_k, x_k) = (\alpha_i, \beta_i, \gamma_i)$ for some $1 \leq i \leq m$, and $x_2 \in \mathcal{X}_2$ follows.

For $n = 12$ the triples $(1 - x_2, x_2 - x_7, x_7)$ and $(1 - x_6, x_6 - x_7, x_7)$ are solutions of the 3-unit equation $\alpha + \beta + \gamma = 1$. If the first solution is not trivial, then $1 - x_2 = \alpha_i,\ x_2 = 1 - \alpha_i$ for some $1 \leq i \leq m$. Otherwise $x_2 - x_7 = 1$, but then the second solution is not trivial, and $x_7 = \alpha_i$, $x_2 = 1 + \alpha_i$ for some i. Hence $x_2 \in \mathcal{X}_2$.

Assume that $n = 6$. Put $x_6 = 0$, $x_7 = 1$ and $y_i = x_i - x_{i-1}$ for $i \in [2, 7]$. Hence $y_2, \ldots, y_7$ are invertible. Put $y_2 = -u$. Assume that $x_2 \neq 1 - \alpha_i$ (i.e. $u \neq \alpha_i$) for $1 \leq i \leq m$.

Take any $i \in [3, 7]$. Then $x_2 \sim x_i - x_{i-2} = y_{i-1} + y_i$, and $1 - u = x_2 = \delta(y_{i-1} + y_i)$ for some invertible δ. Thus $(u, \delta y_{i-1}, \delta y_i)$ is the trivial solution of the equation $\alpha + \beta + \gamma = 1$ in units. Since $u \neq 1$, we get $\delta y_{i-1} = 1$ or $\delta y_i = 1$, and $y_i / y_{i-1} \in \{-u, -u^{-1}\}$ follows. Since $y_7 = 1$, we get $y_6 \in \{-u, -u^{-1}\}$.

If $u = -1$, then $x_2 = 2$, $x_3 = 3$ and $0 = x_6 = 2 \cdot 3$. This gives $2 = 0$ or $3 = 0$, i.e. $x_2 = 0$ or $x_3 = 0$, a contradiction. Thus we get $u \neq \pm 1$.

For $i = 2, \ldots, 6$ put $y_i = (-u)^{a_i}$, with $a_2 = 1$ and $|a_i - a_{i-1}| = 1$ for $i = 3, \ldots, 6$.

In this way we obtain 16 possibilities for the quadruple (a_3, a_4, a_5, a_6).

There are 9 possibilities for (a_3, a_4, a_5, a_6) such that $(a_3, a_4, a_5, a_6) \neq (0, 1, 0, 1)$ and $a_6 \in \{\pm 1\}$. In each of these possibilities the condition that $0, 1, x_2, \ldots, x_5$ are distinct is not satisfied. A typical such possibility is $(a_3, a_4, a_5, a_6) = (0, 1, 0, -1)$.

In this case $0 = x_6 = 1 - u + 1 - u + 1 - u^{-1} = (1 - u)(1 + 1 - u^{-1})$, and $1+1-u^{-1} = 0$ follows. This gives $x_4 - x_1 = -u + 1 - u = -u(1+1-u^{-1}) = 0$, a contradiction.

There are 5 possibilities for (a_3, a_4, a_5, a_6) such that $a_6 \in \{\pm 3\}$. In any such possibility $y_6 \in \{-u, -u^{-1}\}$ gives $(-u)^2 = 1$ or $(-u)^4 = 1$. Since we have already excluded $u = \pm 1$, we must have $u^2+1 = 0$, and this gives a contradiction. Take for example $(a_3, a_4, a_5, a_6) = (0, -1, -2, -3)$. Since $0 = x_6 = 1 - u + 1 - u^{-1} + u^{-2} - u^{-3} = (1-u)(1-u^{-1}-u^{-3})$, we obtain $0 = 1-u^{-1}-u^{-3} = 1-u^{-3}(1+u^2) = 1$, a contradiction. In other four cases we proceed in a similar manner.

Let us consider $(a_3, a_4, a_5, a_6) = (2, 3, 4, 5)$. Since $0 = x_6 = 1 - u + u^2 - u^3 + u^4 - u^5 = (1 - u)(1 - u + u^2)(1 + u + u^2)$ and $x_3 = 1 - u + u^2 \neq 0$, we obtain $1 + u + u^2 = 0$. Hence u is a primitive third root of unity and $x_2 = 1 - u \in \mathcal{X}_2$.

Finally, let $(a_3, a_4, a_5, a_6) = (0, 1, 0, 1)$. Then $0 = x_6 = 3(1-u)$ and $\operatorname{char} R = 3$ follows. If an invertible $u \neq 1, 2$ and $\operatorname{char} R = 3$, then $(0, 1, 1-u, 2-u, 2-2u, -2u)$ is a cycle for $f(X) = 1 - uX - (u+1)/uX(X-1) + 1/uX(X-1)(X-(1-u))$.

Lemma 1. *For $n \geq 3$, $n \neq 4$ let $(0, 1, x_2, \ldots, x_{n-1})$ be a cycle in R for $f(X) \in R[X]$. We extend the indices putting $x_n = x_0 = 0$, $x_{n+1} = x_1 = 1$, $x_{n+2} = x_2$, $x_{n+3} = x_3$ and so on. Assume that for some $2 \leq r \leq n+1$ we have $1 - y := (x_r - x_{r-2})/(x_{r-1} - x_{r-2}) \notin \mathcal{X}_2$. Then $x_2 \notin \mathcal{X}_2$.*

Proof. We have that $(0, 1, 1 - y, (x_{r+1} - x_{r-2})/(x_{r-1} - x_{r-2}), \ldots, (x_{r+n-3} - x_{r-2})/(x_{r-1} - x_{r-2}))$ is a cycle for $g(X) = (x_{r-1} - x_{r-2})^{-1}(f((x_{r-1} - x_{r-2})X + x_{r-2}) - x_{r-2}) \in R[X]$. By what we have already proved, we have $n = 6$, $\operatorname{char} R = 3$ and $(x_{r+1} - x_{r-2})/(x_{r-1} - x_{r-2}) = 2 - y, \ldots, (x_{r-3} - x_{r-2})/(x_{r-1} - x_{r-2}) = y$. In particular the triple $((x_0-x_{r-2})/(x_{r-1}-x_{r-2}), (x_1-x_{r-2})/(x_{r-1}-x_{r-2}), (x_2-x_{r-2})/(x_{r-1}-x_{r-2}))$ is of one of the following forms $(0, 1, 1-y), (1, 1-y, 2-y), \ldots, (y-1, y, 0), (y, 0, 1)$. This easily gives $x_2 \in \{1-y, 1-1/y\}$. Since $1-y \in \mathcal{X}_2$ if and only if $1-1/y \in \mathcal{X}_2$, we are done. $\square$

Summing up, for $n \geq 3$, $n \neq 4$ we showed that $x_2 \in \mathcal{X}_2$, except for one family of exceptions in $\operatorname{char} R = 3$. Using Lemma 1, by simple induction we obtain $x_j \in \mathcal{X}_j$ for $j \geq 2$ provided $x_2 \in \mathcal{X}_2$. If $x_2 \notin \mathcal{X}_2$, then $\operatorname{char} R = 3$ and $(0, 1, x_2, \ldots, x_5)$ is of the form $(0, 1, 1 - u, 2 - u, 2 - 2u, -2u)$, with invertible $u \neq 1, 2$.

(iii) Let $(0, 1, x_2, x_3)$ be a normalized cycle. We see that $1-x_2, x_3$ and x_3-x_2 are invertible and $(1 - x_2, x_3, x_2 - x_3)$ is a solution of the 3-unit equation. If this solution is not trivial, then $(1 - x_2, x_3, x_2 - x_3) = (\alpha_i, \beta_i, \gamma_i)$ for some $1 \leq i \leq m$, and $(0, 1, x_2, x_3) = (0, 1, 1 - \alpha_i, \beta_i)$ follows.

Otherwise $x_2 - x_3 = 1$, and $(0, 1, x_2, x_3) = (0, 1, 1 + v, v)$ for some unit v. Since $x_3 - 1 \sim x_2$, we obtain that $1 - v = \delta(1 + v)$ for some invertible δ. We see that $(v, \delta, \delta v)$ is a solution of the 3-unit equation. If this solution is not trivial, then $(0, 1, x_2, x_3) = (0, 1, 1 + \alpha_i, \alpha_i)$ for some $1 \leq i \leq m$. If this solution is trivial, then $\delta = 1$, char $R = 2$ or $\delta = 1/v$, $v^2 + 1 = 0$. One easily sees that $(0, 1, 1 + v, v)$ is a cycle if char $R = 2$ and $v \neq 1$ is invertible. $\square$

Remark 1. Theorem 1 gives (except for two families of cycles if char R equals 2 or 3) a finite list of tuples which may be cycles. To check whether a given $(0, 1, x_2, \dots, x_{n-1})$ is a cycle we should calculate the Lagrange interpolation polynomial realizing this cycle, and check whether its coefficients lie in R.

Remark 2. Generally speaking, the numbers of elements of $\mathcal{X}_2, \mathcal{X}_3, \dots$ grow quite rapidly. In some cases one can shrink quite a lot the sets of possible values for x_j's. For example if n is odd, $(0, 1, x_2, \dots, x_{n-1})$ is a cycle and $1 \leq j \leq n - 1$ satisfies $(j(j-1), n) = 1$, then $(x_j, 1 - x_j) \in \mathcal{B}$. One may also restrict the possible values for x_j's taking into account for example that $x_2 \sim x_3 - x_1 \sim x_4 - x_2$ and some other similar relations.

Remark 3. If $(x_0, x_1, \dots, x_{n-1})$ is a cycle, then $(0, 1, (x_2 - x_0)/(x_1 - x_0), (x_3 - x_0)/(x_1 - x_0), \dots, (x_{n-1} - x_0)/(x_1 - x_0))$ is a normalized cycle of the same length. Thus having found all normalized cycles we find the set $\mathcal{CYCL}(R)$ of all cycle lengths in R.

Remark 4. From the proof of Theorem 1 we infer that for odd n all normalized cycles of length n can be found using solely the solutions of the 2-unit equation $u + v = 1$. Using the ideas from the proof of Theorem 1(i), we may show that the odd lengths of cycles are bounded by $C(m_1 + 1)(\log\log(m_1 + 3))^2$ for some constant C. Thus finding all normalized cycles of even lengths is much complicated than those of odd lengths.

Remark 5. Theorem 1 does not lead directly to the determination of $\mathcal{CYCL}(R)$ in the case when $R = Z_K$ is the ring of integers of an algebraic number field K, as there is no known procedure to find all solutions of the equation $u + v + w = 1$ in units $\neq 1$. An exception is formed by fields with unit rank ≤ 1, where all cycle lengths were determined ([Bo] and [Ba]) for quadratic fields, [Na2] for complex cubic fields, and [Pe2] for totally complex quartic fields.

2. An algorithm determining all normalized cycles

Nevertheless, we have found a finitary procedure working in all number fields K, which finds all normalized cycles in Z_K, and therefore also $\mathcal{CYCL}(Z_K)$. It is based on some known algorithms from algebraic number theory. In the proof of Theorem 2 below we propose such a procedure.

Theorem 2. *There is an effective procedure, which for a given number field K finds all normalized cycles in Z_K. This procedure also finds $\mathcal{CYCL}(Z_K)$.*

Proof. For any number field K the following things can be effectively calculated:

(A) the degree $[K:Q]$, the discriminant $\operatorname{disc}(K)$, the regulator $\operatorname{reg}(K)$, the class number h_K, an integral basis, a fundamental system of units, all roots of unity lying in K. One may effectively check whether a given element from K lies in Z_K.

(B) For any nonzero $\alpha,\beta,\gamma\in Z_K$ let us define $\mathcal{T}_K(\alpha,\beta;\gamma)=\{(u,v): \alpha u+\beta v=\gamma$, and u, v are invertible$\}$. Then $\mathcal{T}_K(\alpha,\beta;\gamma)$ is finite and may be effectively found (see [S], [Gy], [EGST]).

(C) For any nonzero $a\in Z_K$ one can effectively find the set of all (up to associates) divisors of a. Since for any $b\mid a$ one has $N_{K/Q}(b)\mid N_{K/Q}(a)$, this may be completed by solving a suitable norm form equation. For the solvability of norm form equations in an effective way see [BSh], [Ga].

Lemma 2. *Let K be a number field. Let $a_1,a_2,b_1,b_2,c_1,c_2\in Z_K$ be given and satisfy $a_1,a_2,c_1,c_2,b_1a_2-b_2a_1\neq 0$. Then one can effectively determine a finite set $\mathcal{A}_1$, depending on K and $a_1,a_2,\dots,c_2$, consisting of all integers $u\in Z_K$ satisfying $a_iu+b_i\mid c_i$ for $i=1,2$.*

Proof. For $i=1,2$ one effectively finds a finite set $\mathcal{D}_i$ of all (up to associates) divisors of c_i. Hence $a_1u+b_1=d_1\delta_1$, $a_2u+b_2=d_2\delta_2$ for some $d_i\in\mathcal{D}_i$ and invertible δ_1,δ_2. This gives $(\delta_1,\delta_2)\in\mathcal{T}_K(d_1a_2,-d_2a_1;b_1a_2-b_2a_1)$, so for fixed d_1,d_2 we effectively find possible u. Since d_i lies in the finite set $\mathcal{D}_i$, we are done. □

Let K be a fixed number field. Put $N=[K:Q]$. Let (r,s) be the signature of K. Let $\zeta_M=\exp(2\pi i/M)$ be the generator of the group of roots of unity lying in K and let $\eta_1,\dots,\eta_{r+s-1}$ be any fundamental system of units in K.

Let us define $\mathcal{S}(n)$ as the set of all normalized cycles in Z_K of length n. In order to prove the assertion it suffices to bound effectively the n's such that $\mathcal{S}(n)$ is non-empty, and for n less than this bound to find effectively $\mathcal{S}(n)$. According to Remark 1, in order to check whether $(0, 1, x_2, \ldots, x_{n-1})$ is a cycle it suffices to check whether the (unique) polynomial $h(X)$ of degree $\leq n-1$ realizing this cycle, with coefficients in K, has all its coefficients in Z_K. The polynomial $h(X)$ is calculated by the Lagrange interpolation formula, and one may effectively check whether all its coefficients lie in Z_K.

Remark 6. Let $B(R)$ be the biggest element of $\mathcal{CYCL}(R)$. It is known that $B(Z_K)$ is bounded from above by some explicit expression depending on $N = [K : Q]$. The first such estimation was given in [Na1], where $B(Z_K)$ is bounded from above by some double exponential function in N. It was improved in [Pe1], where $B(Z_K) \leq 2^{N+1}(2^N - 1)$ was established.

For any odd $n \leq 2^{N+1}(2^N - 1)$ we can find effectively all elements from $\mathcal{S}(n)$, as explained in Remark 4, since by (B) all solutions of the 2-unit equation $u + v = 1$ in Z_K can be effectively computed.

The procedure of finding all $\mathcal{S}(k)$ will be completed provided for all $n \leq 2^N(2^N - 1)$ we can effectively find $\mathcal{S}(2n)$ having at our disposal the finite set $\mathcal{S}(n)$.

Remark 7. Assume that $(0, 1, x_2, \ldots, x_{n-1})$ is a cycle in a domain R for a polynomial $f(X) = c_0 + c_1X + \cdots + c_{n-1}X^{n-1}$. Take any nonzero $a \in R$. The Lagrange interpolation polynomial for the sequence $\xi_a = (0, a, ax_2, \ldots, ax_{n-1})$ equals $af((1/a)X)$. Thus ξ_a is a cycle in R if and only if $a \mid c_2$, $a^2 \mid c_3, \ldots$, $a^{n-2} \mid c_{n-1}$.

Remark 8. If $(0, 1, y_2, y_3, \ldots, y_{2n-1}) \in \mathcal{S}(2n)$ is a cycle for $F(X)$, then $(0, 1, y_4/y_2, y_6/y_2, \ldots, y_{2n-2}/y_2)$ is a cycle of length n for $(1/y_2)(F \circ F)(y_2X) \in R[X]$.

Owing to the last remark in order to find $\mathcal{S}(2n)$ it suffices to find effectively for a fixed $(0, 1, x_2, \ldots, x_{n-1}) \in \mathcal{S}(n)$ all $(0, 1, y_2, \ldots, y_{2n-1}) \in \mathcal{S}(2n)$ such that $y_{2k}/y_2 = x_k$ for all $2 \leq k \leq n-1$ (informally speaking $(0, 1, x_2, \ldots, x_{n-1})$ is proportional to $(0, y_2, y_4, \ldots, y_{2n-2})$). Let us call such $(0, 1, y_2, \ldots, y_{2n-1})$ *connected* to $(0, 1, x_2, \ldots, x_{n-1})$.

Lemma 3. *Let n be given and assume that the set $\mathcal{S}(n)$ is explicitly known. If for each sequence $\xi = (0, 1, x_2, \ldots, x_{n-1}) \in \mathcal{S}(n)$ one can effectively construct a finite set $\mathcal{Y} = \mathcal{Y}(\xi, K)$ such that every cycle $\eta = (0, 1, y_2, \ldots, y_{2n-1})$, connected to ξ satisfies $y_2 \in \mathcal{Y}$, then there exists an effective procedure to determine $\mathcal{S}(2n)$.*

Such a construction exists, provided one can either effectively find a nonzero $b \in Z_K$ such that each cycle η connected to ξ satisfies $y_2 \mid b$, or one can find *effectively nonzero $b, c \in Z_K$ with $b \neq 1$ such that each cycle η connected to ξ satisfies $y_2 b - 1 \mid c$.*

Proof. Suppose that we found such $\mathcal{Y}$. Fix any $a \in \mathcal{Y}$. If η is a cycle with $y_2 = a$, connected to ξ, then $y_{2k} = a x_k$ for all $2 \leq k \leq n-1$. Thus $y_2, y_4, y_6, \dots, y_{2n-2}$ are uniquely determined by a and ξ. Let $\mathcal{T}_K(1,1;a) = \{(u_1, v_1), \dots, (u_t, v_t)\}$.

Take any $1 \leq k \leq n-1$, and consider y_{2k+1}. Then $y_{2k+2} - y_{2k+1}, y_{2k+1} - y_{2k}, x_{k+1} - x_k$ are units, and $((y_{2k+2} - y_{2k+1})/(x_{k+1} - x_k), (y_{2k+1} - y_{2k})/(x_{k+1} - x_k)) \in \mathcal{T}_K(1,1;a)$. This gives $y_{2k+1} = a x_k + (x_{k+1} - x_k) v_i$ for some $1 \leq i \leq t$. Thus we have only finitely many and effectively computable possibilities for the values $y_3, y_5, \dots, y_{2n-1}$. Having a finite number of possibilities for cycles connected to $(0, 1, x_2, \dots, x_{n-1})$ we pick those which are in fact cycles.

Let $b \neq 0$ be effectively computable and suppose that for all cycles η connected to $(0, 1, \dots, x_{n-1})$ we have $y_2 \mid b$. Such a set $\mathcal{Y}$ exists by Lemma 2 in view of $y_2 - 1 \mid 1$.

Let $b \neq 0, 1$; $c \neq 0$ be effectively computable and suppose that for all cycles η connected to ξ we have $y_2 b - 1 \mid c$. Such a set $\mathcal{Y}$ exists by Lemma 2 in view of $y_2 - 1 \mid 1$. $\square$

Let $\xi = (0, 1, x_2, \dots, x_{n-1}) \in \mathcal{S}(n)$ be fixed. Let $\eta = (0, 1, y_2, y_3, \dots, y_{2n-1})$ be connected to ξ. Put $y_2 = a$. We will show two ways of finding a set $\mathcal{Y}$ fulfilling the condition of Lemma 3. The sets $\mathcal{Y}$ obtained in the two ways below may differ.

First way. Let $f(X) = c_0 + c_1 X + c_2 X^2 + \cdots + c_{n-1} X^{n-1}$ be the unique polynomial of degree $\leq n-1$ realizing ξ. Since $(0, y_2, y_4, \dots, y_{2n-2}) = (0, a, a x_2, \dots, a x_{n-1})$ is a cycle for $(f \circ f)(X)$, by Remark 7 we get $a \mid c_2, a^2 \mid c_3, \dots, a^{n-2} \mid c_{n-1}$. If at least one number from $c_2, c_3, \dots, c_{n-1}$ is nonzero we are done by Lemma 3.

Second way. We have $y_4 - y_1 = y_4 - 1 \mid y_6 - y_0 = y_6$, and equivalently $a x_2 - 1 \mid a x_3$. Hence $a x_2 - 1 \mid a x_3 x_2$ and $a x_2 - 1 \mid x_3$ follows. If $n > 3$, then $x_2 \neq 0, 1$; $x_3 \neq 0$, and we are done by Lemma 3.

For $n \geq 4$ the set $\mathcal{Y}$ may be established by the second way.

Let $n = 3$. If the Lagrange interpolation polynomial $f(X)$ realizing $\xi = (0, 1, x_2)$ is of degree 2, then we establish $\mathcal{Y}$ using the first way. Assume that $f(X) = c_0 + c_1 X$ realizes the cycle ξ. Then $c_0 = 1$ and (since $f^{\circ 3}(0) = 0$) $1 + c_1 + c_1^2 = 0$. Thus c_1 is a primitive third root of unity.

It remains therefore to consider ξ of the form $\xi = (0, 1, 1 + \zeta)$, where in what follows ζ is a primitive third root of unity. Let $\eta = (0, 1, y_2, \dots, y_5)$ be a cycle connected to $(0, 1, 1 + \zeta)$. We may write η in the form $(0, 1, a, 1 + b, a(1 + \zeta), 1 + bz)$ for some $a, b, z \in Z_K$. Let $g(X)$ be a polynomial realizing the cycle η.

We see that $(0, 1, z)$ is a cycle for $1/b\ (g^{\circ 2}(bX + 1) - 1) \in Z_K[X]$. Thus $(0, 1, z) \in \mathcal{S}(3)$.

Fix $z \neq 1 + \zeta, 1 + \zeta^2$ such that $(0, 1, z) \in \mathcal{S}(3)$. Owing to the invertibility of $a-1$ we obtain that $\eta_1 = (0, 1, b/(a-1), (a(1+\zeta)-1)/(a-1), bz/(a-1), -1/(a-1))$ is a cycle (for $1/(a - 1)\ (g((a - 1)X + 1) - 1) \in Z_K[X]$) connected to $(0, 1, z)$. Since $z - 1$ is not a primitive third root of unity, by the previous part of the proof we conclude that η_1 can be effectively found, and therefore also a, b can be effectively found.

It remains therefore to consider the cases $z = 1 + \zeta$ and $z = 1 + \zeta^2$.

First, let $z = 1+\zeta^2$, and consider $(0, 1, a, 1+b, a(1+\zeta), 1+b(1+\zeta^2)) \in \mathcal{S}(6)$. Since $y_4 - 1 \mid y_3, y_5 - y_2$ we have $a(1+\zeta) - 1 \mid 1+b, 1+b(1+\zeta^2) - a$. This easily gives $a(1 + \zeta) - 1 \mid 2 + \zeta^2 \neq 0$, which together with $a - 1 \mid 1$ shows by Lemma 2 that a belongs to an effectively computable and finite set.

Secondly, let $z = 1+\zeta$, and consider $(0, 1, a, 1+b, a(1+\zeta), 1+b(1+\zeta)) \in \mathcal{S}(6)$ with $a \sim b$. Since $y_2 - y_3$ and $y_4 - y_5$ are units, we get that $a - 1 - b$ and $a(1+\zeta)-(1+b(1+\zeta))$ are units. This gives that $(a-1-b, a(1+\zeta)-(1+b(1+\zeta)))$ lies in the finite and effectively computable set $\mathcal{T}_K(1, \zeta; \zeta^2) = \{(u_1, v_1), \dots, (u_t, v_t)\}$. Put $a - 1 - b = u_i$ for some $i \leq t$.

If $u_i \neq -1$, then $a \mid a - b = u_i + 1$, which together with $a - 1 \mid 1$ shows by Lemma 2 that a belongs to an effectively computable and finite set.

Let $u_i = -1$, or equivalently $a = b$, and consider $(0, 1, a, 1 + a, a(1 + \zeta), 1 + a(1 + \zeta)) \in \mathcal{S}(6)$. Then $a - 1$ and $1 + a(1 + \zeta)$ are units, and $(a - 1, 1 + a(1 + \zeta))$ belongs to the finite and effectively computable set $\mathcal{T}_K(1, \zeta; \zeta - 1)$.

In this way we showed for any $n \geq 3$ that having at our disposal $\mathcal{S}(n)$ we can effectively find $\mathcal{S}(2n)$. It remains to find effectively $\mathcal{S}(4)$, and this case requires a slightly different approach.

Let us arbitrary order the units of the form $\zeta_M^{i_0} \eta_1^{i_1} \cdot \ldots \cdot \eta_{r+s-1}^{i_{r+s-1}}$, with $0 \leq i_0, i_1, \dots, i_{r+s-1} \leq 1$ and denote them as $\sigma_1, \sigma_2, \dots, \sigma_{2^{r+s}}$. Any unit δ may be uniquely written in the form $\sigma_i \epsilon^2$ for a unit ϵ and some $i \in [1, 2^{r+s}]$.

Let $(0, 1, x_2, x_3)$ be a cycle. Since $x_2 - 1$ and x_3 are units, we may write $x_2 = 1 + \delta$, $x_3 = \epsilon$ for some invertible δ, ϵ. Thus $(0, 1, x_2, x_3) = (0, 1, 1 + \delta, \epsilon)$. Since $x_2 \sim 1 - x_3$, we may write $1 - \epsilon = \psi(1 + \delta)$ for some unit ψ. Since $x_2 - x_3$ is invertible, $(x_2 - x_3)/\psi = 1 + \delta + \delta/\psi$ is invertible as well. In view of $\delta + \delta^2 - \delta/\psi = -\delta\epsilon/\psi$, we then obtain that

$$\tau_1 := 1 + \delta + \frac{\delta}{\psi}; \quad \tau_2 := \delta + \delta^2 - \frac{\delta}{\psi}$$

are units. Write $\tau_1 = \sigma_i \rho^2$, for some $1 \le i \le 2^{r+s}$ and a unit ρ.

We see that $\tau_2 = (\delta+1)^2 - \tau_1 = (\delta+1)^2 - \sigma_i\rho^2 = (\delta+1+\sqrt{\sigma_i}\rho)(\delta+1-\sqrt{\sigma_i}\rho)$ is invertible. Thus $\delta+1+\sqrt{\sigma_i}\rho$ and $\delta+1-\sqrt{\sigma_i}\rho$ are units in $Z_{K(\sqrt{\sigma_i})}$. Hence

$$\left(\frac{\delta+1}{\sqrt{\sigma_i}\rho}+1, \frac{\delta+1}{\sqrt{\sigma_i}\rho}-1\right) \in \mathcal{T}_{K(\sqrt{\sigma_i})}(1,-1;2).$$

For $i = 1, \dots, 2^{r+s}$ the sets $\mathcal{T}_{K(\sqrt{\sigma_i})}(1,-1;2)$ are finite and effectively computable. Moreover, having K we may effectively find all $K(\sqrt{\sigma_i})$.

Let $\mathcal{T}_{K(\sqrt{\sigma_i})}(1,-1;2) = \{(u_{i_1}, v_{i_1}), \dots, (u_{i_{j(i)}}, v_{i_{j(i)}})\}$. Hence $(\delta+1)/(\sqrt{\sigma_i}\rho)+1 = u_{i_j}$ for some $j \le j(i)$. Thus $(u_{i_j}-1)\sqrt{\sigma_i} \in K$, and therefore $(\delta,\rho) \in \mathcal{T}_K(1, \sqrt{\sigma_i}(1-u_{i_j}); -1)$.

For any $i \le 2^{r+s}$ and u_{i_j} satisfying $(u_{i_j}-1)\sqrt{\sigma_i} \in K$ we effectively find $\mathcal{T}_K(1, \sqrt{\sigma_i}(1-u_{i_j}); -1)$, and this gives that all possible $x_2 - 1 = \delta$ belong to a finite and effectively computable set.

Having found possibilities for δ and observing that $(\tau_1, -\delta/\psi) \in \mathcal{T}_K(1,1;1+\delta)$, we finally obtain that $x_3 = \epsilon = 1 - \psi(1+\delta)$ also belongs to some finite and effectively computable set. The proof of Theorem 2 is thus completed. $\square$

3. Finite orbits

In a domain R a tuple $(y_k, y_{k-1}, \dots, \underline{y_0 = x_0, x_1, \dots, x_{n-1}})$ of distinct elements from R is called a *(finite) orbit* provided there exists a polynomial $f(X) \in R[X]$ realizing this orbit, i.e. $f(y_k) = y_{k-1}$, $f(y_{k-1}) = y_{k-2}, \dots, f(y_1) = y_0 = x_0$, $f(x_0) = x_1$, $f(x_1) = x_2, \dots, f(x_{n-1}) = x_0$. We underlined the unique cycle contained in the orbit.

The counterpart of the second part of Remark 1 holds also for orbits.

The number $n+k$ is called the *length* of this orbit, the cycle $(x_0, x_1, \dots, x_{n-1})$ will be called the *head* of this orbit (of length n), $(y_k, y_{k-1}, \dots, y_0)$ will be called the *tail* of this orbit (of length k (not $k+1$)), and finally (n,k) will be called the *type* of this orbit.

A cycle $(x_0, x_1, \dots, x_{n-1})$ in R is called *linear*, provided it is realized by some polynomial $f(X) \in R[X]$ of degree ≤ 1. We call an orbit *linear* provided its head is linear.

If $(y_k, \dots, \underline{y_0 = x_0, \dots, x_{n-1}})$ is an orbit in R, then clearly for any invertible $a \in R$ and any $b \in R$ the tuple $(ay_k + b, \dots, \underline{ay_0 + b = ax_0 + b, \dots, ax_{n-1} + b})$ is also an orbit in R. Two such orbits will be called *equivalent*.

In [H-KNa2] it was established that in any finitely generated domain of characteristic zero there is only finitely many inequivalent nonlinear orbits.

Theorem 3. *Let K be an algebraic number field of degree N. Then for polynomial orbits in Z_K the following holds.*

(i) *The lengths of orbits are bounded by some quantity depending solely on N.*

(ii) *There are only finitely many inequivalent nonlinear orbits and all of them can be effectively found.*

(iii) *Any linear orbit with tail of length 0 is equivalent to $(\underline{0, a, a(1+\zeta_n), \ldots, a(1+\zeta_n+\zeta_n^2+\cdots+\zeta_n^{n-2})})$ for some nonzero $a \in Z_K$ and some primitive n-th root of unity $\zeta_n \in Z_K$.*

(iv) *There are only finitely many inequivalent linear orbits with head of length ≥ 4 and tail of length ≥ 1 and all of them can be effectively found.*

(v) *Any linear orbit of type $(3,1)$ is equivalent to $(1, \underline{0, 1+\epsilon, (1+\epsilon)(1+\zeta_3)})$ (this is the orbit for $f(X) = (X-1)(X-(1+\epsilon)(1+\zeta_3))(-\zeta_3+(\zeta_3/\epsilon)X)$, and ζ_3 is a primitive third root of unity) for any unit $\epsilon \neq -1$.*

(vi) *There are only finitely many inequivalent linear orbits of type $(3,k)$ with $k \geq 2$, and all of them can be effectively found.*

(vii) *Any orbit of type $(2,1)$ is equivalent to $(1, \underline{0, d})$ for some $d \in Z_K, d \neq 0, 1$ (this is the orbit for $f(X) = (d-X)(1-X)$).*

(viii) *Any orbit of type $(2,2)$ is equivalent to $(1+\epsilon, 1, \underline{0, 1+\epsilon+\delta})$ for some invertible $\epsilon, \delta \in Z_K$, $\epsilon \neq -1$, $\delta \neq -\epsilon, -1-\epsilon$; $(1+\epsilon) \mid \delta - 1$ (this is the orbit for $f(X) = (1+\epsilon+\delta-X)(1-X)-(1+\epsilon\delta)/(\epsilon\delta(1+\epsilon))X(X-1)(X-(1+\epsilon+\delta)))$.*

(ix) *$(a, \underline{b})$ is the orbit of type $(1,1)$ for any $a \neq b$ (for $f(X) = b$).*

(x) *Any orbit of type $(1,2)$ is equivalent to $(d, \underline{d(1-\epsilon), 0})$ for some nonzero $d \in Z_K$ and invertible ϵ satisfying $d \mid 1-\epsilon$ (this is the orbit for $f(X) = (1-\epsilon)/(\epsilon d)(X - d(1-\epsilon))X$).*

(xi) *There are only finitely many inequivalent orbits with head of length 1 or 2 and tail of length ≥ 3. One can effectively (up to equivalence) find all of them if and only if one finds an effective procedure for determining all solutions of $u+v+w=1$, $1-u \mid 1-v$, with invertible $u, v, w \in Z_K$, $u, v, w \neq 1$.*

Proof. Any orbit is equivalent to $(y_k, \ldots, y_1, \underline{y_0 = 0, a, ax_2, \ldots, ax_{n-1}})$, where $(0, 1, x_2, \ldots, x_{n-1})$ is a normalized cycle, and we may restrict considerations to orbits of this form.

(i) In [NaPe] it was emphasized that the lengths of orbits in Z_K are bounded by some quantity depending solely on $B(Z_K)$ and the number of nontrivial solutions of $u+v+w=1$ in units (the latter number is bounded by some expression depending solely on $[K:Q]$ (see [EG])).

Lemma 4. *Fix $a, b \in Z_K$, $a \neq 0$, $b \neq 0$, $a \neq b$.*

(α) *There are only finitely many orbits with head of length ≥ 3 of the form $(y_k, \dots, \underline{y_0 = 0, a, \dots})$, and all of them can be effectively found.*

(β) *There are only finitely many orbits of the form $(y_k, \dots, y_1 = b, \underline{y_0 = 0, a})$, and all of them can be effectively found.*

(γ) *There are only finitely many orbits of the form $(y_k, \dots, y_1 = a, \underline{y_0 = 0})$, and all of them can be effectively found.*

Proof. (α) Put $(x_0, x_1, \dots, x_{n-1}) = (0, a, \dots)$. Then $(0, 1, x_2/x_1, x_3/x_1, \dots)$ is a normalized cycle. By Theorem 2 there is only finitely many possibilities for $n \geq 3$, then for $x_2, \dots, x_{n-1}$ and they can be effectively computed. It suffices then to deal with tails, which have bounded lengths by (i) of Theorem 3.

Since for x_2 there is only finitely many possibilities, we may fix $x_2 = c$. The assertion follows then from Theorem 4 of [H-KNa2], as all solutions of the unit equations $a_1 u + b_1 v = c_1$ (with nonzero a_1, b_1, c_1) can be found in an effective way. One may also use Lemma 2.

(β) and (γ) follow immediately from Theorem 3(i) and Theorem 4 of [H-KNa2]. □

(ii) Since we are considering orbits up to equivalence, by Theorem 2, Remark 7 and (C) we may assume that the element a from a nonlinear orbit $(y_k, \dots, y_1, \underline{y_0 = 0, a, ax_2, \dots, ax_{n-1}})$ belongs to some effectively computable and finite set $\mathcal{Y}$. By Lemma 4(α) we are done.

(iii) It is clear.

(iv), (v) Let $(b, \underline{0, a, a(1+\zeta_n), \dots, a(1+\zeta_n+\dots+\zeta_n^{n-2})})$ be a linear orbit (for a polynomial $f(X) \in Z_K[X]$) with head of length $n \geq 3$, and ζ_n is a primitive n-th root of unity. Thus $f(X)$ is of the form $f(X) = \zeta_n X + a + h(X)X(X-a)\cdot \dots \cdot (X - a(1+\zeta_n+\dots+\zeta_n^{n-2}))$ for some $h(X) \in Z_K[X]$. Since $b - 0 \mid f(b) - f(0) = 0 - a$ we may write $a = bd$, for some $d \in Z_K$.In view of $h(b) \in Z_K$ we get $b^{n-1}(1-d)(1-d(1+\zeta_n)) \cdot \dots \cdot (1 - d(1+\zeta_n+\dots+\zeta_n^{n-2})) \mid \zeta_n + d \neq 0$ (otherwise $y_1 = x_{n-1}$).

For $n \geq 4$ we then get $1 - d \mid d + \zeta_n$ and $(1 - d(1+\zeta_n)) \mid d + \zeta_n$, which gives $1 - d \mid \zeta_n + 1$ and $(1 - d(1+\zeta_n)) \mid \zeta_n(1+\zeta_n) + 1 \neq 0$. Lemma 2 gives $d \in \mathcal{Y}$ for some finite and effectively computable $\mathcal{Y}$. Fix any $d \in \mathcal{Y}$, and we obtain $b \mid b^{n-1} \mid \zeta_n + d$. By (C), b is associated to an element of some finite and effectively computable $\mathcal{Y}_1$. Thus our orbit is equivalent to some orbit of the form $(b_1, \underline{0, b_1 d, \dots})$ with $b_1 \in \mathcal{Y}_1, d \in \mathcal{Y}$. Since there is only finitely many possibilities for $b_1 d$, (iv) follows from Lemma 4(α).

Let $n = 3$. Then $b^2(1-d)(1-d(1+\zeta_3)) \mid d+\zeta_3$, which gives that $b^2(1-d)$ is invertible. So our orbit is equivalent to $(1, \underline{0, d, d(1+\zeta_3)})$ with invertible $d-1$. This settles (v).

(vi) Consider a linear orbit $(y_k, \ldots, y_1, \underline{0, x_1, x_2})$ of type $(3, k)$ with some $k \geq 2$. By (v) we may assume that $y_1 = 1$, $x_1 = d$, $x_2 = d(1+\zeta_3)$, with $d = 1+\epsilon$ for some invertible $\epsilon \neq -1$. So $(y_2, 1, \underline{0, d, d(1+\zeta_3)})$ is an orbit. This gives $y_2 - 1 \mid 1 - 0 = 1$; $y_2 = y_2 - 0 \mid 1 - (1+\epsilon) \mid 1$. By Lemma 2, we obtain $y_2 \in \mathcal{Y}$, for some finite and effectively computable $\mathcal{Y}$.

Fix $y_2 \in \mathcal{Y} \setminus \{-\zeta_3\}$. Then $y_2 - d \mid d(1+\zeta_3) - 1$, and $y_2 - d \mid \zeta_3 + y_2$ follows. This together with $d - 1 \mid 1$, by Lemma 2, gives that d belongs to some finite and effectively computable set. Lemma $4(\alpha)$ gives the assertion for such y_2.

Assume now that $y_2 = -\zeta_3$. Then $d(1+\zeta_3) - (-\zeta_3) \mid 1 - 0 = 1$. This together with $d - 1 \mid 1$, by Lemma 2, gives that d belongs to some finite and effectively computable set. Lemma $4(\alpha\ )$ gives the assertion for $y_2 = -\zeta_3$. This settles (vi).

(vii) Let $(c, \underline{0, b})$ be an orbit for $f(X)$. So $f(X) = b - X + h(X)X(X-b)$ for some $h(X) \in Z_K[X]$. This gives $c(c-b) \mid b - c$, and c is invertible. We may thus assume that $c = 1$.

(viii) By (vii) any orbit of type $(2,2)$ is equivalent to $(m, 1, \underline{0, d})$. This gives $m - 1 \mid 1$; $m - d \mid 1$ and $m \mid d - 1$.

(ix) It is obvious.

(x) Let $(d, c, \underline{0})$ be an orbit for $f(X)$. So $f(X) = X(X-c)h(X)$ for some $h(X) \in Z_K[X]$. This gives $d(d-c) \mid c$, and $d \sim d - c$ follows. Put $d - c = d\epsilon$. The rest is obvious.

(xi) Let us first deal with orbits with head of length 1.

Suppose, for the time being, that we have at our disposal all orbits of the form $(1, a, b, \underline{0})$*, and there is only finitely many of them.* $(*)$

Let $(m, c, d, \underline{0})$ be an orbit for some $f(X)$. We see that $(1, c/m, d/m, \underline{0})$ is the orbit for $(1/m)f(mX) \in Z_K[X]$. Thus $(1, c/m, d/m, \underline{0}) = (1, a, b, \underline{0})$, with specified possible values for a, b. Since $(c, d, \underline{0})$ is the orbit, by (x), we have $m \mid c \mid (d/c) = (b/a)$. This gives $d = m(d/m) \mid (b/a)b = (b^2)/a$. Thus in any orbit of the form $(y_k, \ldots, y_1, \underline{0})$ (with $k \geq 3$) the number y_1 (still under our assumption $(*)$) may assume (up to associates) only finitely many known values. By Lemma $4(\gamma)$ we then would be able to find effectively (up to equivalence) all orbits with head of length 1 and tail of length ≥ 3.

So let $(1, a, b, \underline{0})$ be an orbit. We easily obtain $1 - a \mid a$; $a \mid b$; $a - b \mid b$; $1 - b \mid b$. This gives $a = 1 - \delta$, $b = a(1-\epsilon)$, $b = 1 - \psi$ for some invertible $\delta, \epsilon, \psi \neq 1$, and by (x) we get $1 - \delta \mid 1 - \epsilon$. This gives $\psi = \delta + \epsilon - \delta\epsilon$ and

$1/\delta + 1/\epsilon - \psi/(\delta\epsilon) = 1$ follows. Hence $(1/\delta, 1/\epsilon, -\psi/(\delta\epsilon))$ is the solution of the 3-unit equation $u + v + w = 1$ satisfying $(1 - 1/\delta) \mid (1 - 1/\epsilon)$.

If this solution is trivial, then $\delta = -\epsilon$ and we obtain $1 - \delta \mid 1 + \delta$, i.e. $1 - \delta \mid 2$. By Lemma 2, we may effectively find all such δ, and there is only finitely many of them.

Conversely, suppose that (u, v, w) is a nontrivial solution of the 3-unit equation $u + v + w = 1$ with $u - 1 \mid v - 1$. Then $(1, 1 - 1/u, (1 - 1/u)(1 - 1/v), \underline{0})$ is the orbit for

$$X\left(X - \left(1 - \frac{1}{u}\right)\left(1 - \frac{1}{v}\right)\right) \times \left(\frac{u(v-1)}{u-1} + \frac{u(v - uv^2 + u^2 - u)}{(u+v-1)(u-1)}\left(X - \left(1 - \frac{1}{u}\right)\right)\right) \in Z_K[X].$$

Notice that if $(u_1, v_1, w_1) \neq (u_2, v_2, w_2)$, then $(1, 1 - 1/u_1, (1 - 1/u_1)(1 - 1/v_1), \underline{0})$ is not equivalent to $(1, 1 - 1/u_2, (1 - 1/u_2)(1 - 1/v_2), \underline{0})$.

In this way we obtained the one-to-one correspondence between the set of all nontrivial solutions of the 3-unit equation $u + v + w = 1$ satisfying $u - 1 \mid v - 1$ and a certain subset $\mathcal{S}$ of orbits of the form $(1, a, b, \underline{0})$. Since any orbit of the form $(1, a, b, \underline{0})$ lying out of $\mathcal{S}$ is effectively computable we are done in the case of orbits with head of length 1.

Now we deal with orbits with head of length 2.

By (viii) and Lemma 4(β) it suffices to find all orbits of the form $(t, m, 1, \underline{0, d})$ provided we have all nontrivial solutions of the 3-unit equation $u + v + w = 1$ with $u - 1 \mid v - 1$.

Assume that we have all such solutions of this 3-unit equation at our disposal. $(**)$

Since $t - m \mid m - 1 \mid 1 - 0 = 1$; $t - d \mid m - 0 = m$; $t - 1 \mid m - 0 = m$; $t = t - 0 \mid m - d \mid 1 - 0 = 1$, we obtain that t, $t - m$, $m - 1$, $m - d$ are invertible and $1 - t \mid m$. Hence $(t, 1 - m, m - t)$ is the solution of the 3-unit equation $u + v + w = 1$ satisfying $t - 1 \mid (1 - m) - 1 = -m$.

If this solution is nontrivial, then by $(**)$ the numbers t, m belong to some finite and explicitly given set.

If this solution is trivial, then $t = m - 1$. This gives $m - 2 \mid m$, i.e. $m - 2 \mid 2$ and $m - 1 \mid 1$. By Lemma 2 we obtain that for such m there is only finitely many possibilities, and they can be effectively computed.

All in all, there is only finitely many possibilities for t, m, and all these possibilities can be effectively computed assuming $(**)$. Fix any possible t, m.

Then $t - d \mid m$; $m - d \mid 1$ and by Lemma 2 we may compute all possible values for d. This settles (xi). $\square$

Remark 9. In the proof of Theorem 3(xi) we showed that in terms of effective computability finding (up to equivalence) all orbits of type $(1, k)$ (with $k \geq 3$) in an effective way is equivalent to finding in an effective way all nontrivial solutions of $u + v + w = 1$ satisfying $u - 1 \mid v - 1$. One sees that finding in an effective way all orbits (up to equivalence) of type $(2, k)$ (with $k \geq 3$) is equivalent to finding in an effective way all nontrivial solutions of $u + v + w = 1$ satisfying $u - 1 \mid v - 1$ and some other condition.

Acknowledgements. I would like to express my gratitude to Prof. I. Gaál for explaining to me some aspects of algorithms in algebraic number theory.

The author thanks the referee for recommending various improvements in exposition.

References

[Ba] G. Baron, Polynomiteration in algebraischen Zahlkörpern, *preprint*, 1991.

[Bo] J. Boduch, Polynomial cycles in rings of algebraic integers, M. A. Thesis, *Wrocław University*, 1990 (in *Polish*).

[BSh] Z. I. Borevich and I. R. Shafarevich, Number Theory, *Academic Press*, 1967.

[EG] J. H. Evertse and K. Győry, On the number of solutions of weighted unit equations, *Compos. Math.* **66** (1988), 329–354.

[EGST] J. H. Evertse, K. Győry, C. L. Stewart and R. Tijdeman, S-unit equations and their applications, New Advances in Transcendence Theory, (A. Baker, ed.), *Cambridge University Press*, 1988, 110–174.

[Ga] I. Gaál, An efficient algorithm for the explicit resolution of norm form equations, *Publ. Math. Debrecen* **56** (2000), 375–390.

[Gy] K. Győry, On the number of solutions of linear equations in units of an algebraic number field, *Comment. Math. Helv.* **54** (1979), 583–600.

[H-KNa1] F. Halter-Koch and W. Narkiewicz, Polynomial cycles and dynamical units, *Proc. Conf. Analytic and Elementary Number Theory*, Wien 1997, 70–80.

[H-KNa2] F. Halter-Koch and W. Narkiewicz, Scarcity of polynomial orbits, *Publ. Math. Debrecen* **56** (2000), 405–414.

[Na1] W. Narkiewicz, Polynomial cycles in algebraic number fields, *Colloq. Math.* **58** (1989), 149–153.

[Na2] W. Narkiewicz, Polynomial cycles in cubic fields of negative discriminant, *Funct. Approx. Comment. Math.* **35** (2006), 261–269.

[NaPe] W. Narkiewicz and T. Pezda, Finite polynomial orbits in finitely generated domains, *Monatshefte für Mathematik* **124** (1997), 309–316.

[Pe1] T. Pezda, Polynomial cycles in certain local domains, *Acta Arith.* **66** (1994), 11–22.

[Pe2] T. Pezda, Polynomial cycles in rings of integers in fields of signature $(0, 2)$, *Funct. Approx. Comment. Math.*, accepted for publication.

[S] V. G. Sprindzhuk, Effective estimates in 'ternary' exponential diophantine equations, *Dokl. Akad. Nauk BSSR* **13** (1969), 777–780 (in *Russian*).

TADEUSZ PEZDA
DEPARTMENT OF MATHEMATICS
UNIVERSITY OF WROCŁAW
PL.GRUNWALDZKI 2/4, 50-384 WROCŁAW
POLAND

E-mail: pezda@math.uni.wroc.pl

(Received January 14, 2013; revised June 4, 2013)