POLYNOMIAL CYCLES IN CUBIC FIELDS OF NEGATIVE DISCRIMINANT

Władysław Narkiewicz

To Professor Eduard Wirsing on his 75th birthday

Abstract: Cycle lengths of polynomial maps in one variable in rings of integers of cubic fields of negative discriminants are determined.

Keywords: cycle lengths, polynomial mappings, cubic fields.

1. A finite sequence

$$\bar{x} = \{x_0, x_1, \dots, x_n\} \tag{1}$$

of elements x_i of a domain R is called a polynomial sequence of length n if there exists a polynomial $f \in R[X]$ such that for i = 0, 1, 2, ..., n-1 one has

$$f(x_i) = x_{i+1}. (2)$$

Such sequence is called a polynomial cycle of length n, or an n-cycle, if the elements $x_0, x_1, \ldots, x_{n-1}$ are all distinct, and $x_n = x_0$ holds. Two polynomial sequences (x_0, x_1, \ldots, x_n) and (y_0, y_1, \ldots, y_m) are called equivalent, if m = n and there exists $a \in R$ and an invertible element $u \in R$ such that for $j = 0, 1, \ldots, n$ one has

$$y_j = a + ux_j.$$

Obviously every polynomial sequence is equivalent to a sequence containing 0.

A cycle $\xi = (x_0, x_1, \dots, x_{n-1}, x_0)$ will be called *normalized*, if $x_0 = 0$ and $x_1 = 1$. While studying cycle-lengths it suffices to consider only normalized cycles, since if a polynomial $f \in R[X]$ realizes the cycle ξ , and for $i = 0, 1, \dots, n-1$ we put

$$y_i = (x_i - x_0)/(x_1 - x_0),$$

then $y_0 = 0$, $y_1 = 1$, $y_i \in R$ (i = 2, 3, ..., n - 1), and $\eta = (0, 1, y_2, ..., y_{n-1}, 0)$ is a normalized cycle of length n, realized by the polynomial

$$g(X) = \frac{f(X(x_1 - x_0) + x_0)}{x_1 - x_0} \in R[X].$$

Denote by C(R) the set of all lengths of polynomial cycles in R.

We shall denote by U(R) the group of units, i.e., invertible elements of R. If $u \in U(R)$ satisfies $1 - u \in U(R)$, then u is called an *exceptional unit of* R. The set of exceptional units in R we shall denote by Ex(R).

We shall also consider unit solutions of the equation

$$u + v + w = 1. (3)$$

Such a solution will be called trivial, if one of the units u, v, w equals unity, and will be called non-trivial otherwise.

It is easy to see that the length of a polynomial cycle in the ring of rational integers equals 1 or 2, and the possible cycle-lengths in rings of integers of quadratic extensions of the rationals were determined in [1] and [2] (see also [5]). The purpose of this paper is to settle the same question for rings of integers in cubic fields of negative discriminants.

Theorem 1. Let \mathbf{Z}_K be the ring of integers in a cubic field K of discriminant d = d(K) < 0. Then

$$\mathcal{C}(\mathbf{Z}_K) = \begin{cases} \{1, 2, 3, 4, 5\} & \text{if } d = -23, \\ \{1, 2, 3, 4, 6\} & \text{if } d = -31, \\ \{1, 2, 4\} & \text{if } d = -44, -59, \\ \{1, 2\} & \text{otherwise.} \end{cases}$$

2. In the next proposition we collect some simple auxiliary results needed in the sequel:

Proposition 1. Let R be an integral domain.

- (i) If $(x_0 = 0, x_1 = 1, x_2, \dots, x_{n-1}, 0)$ is a normalized cycle in R, and we extend x_j by putting $x_j = x_{j-n}$ for j > n, then $x_{i+1} x_i \in U(R)$ holds for $i = 1, 2, \dots$. Moreover for every i and $j \neq 0$ the elements $x_{i+j} x_i$ and x_j are associated, i.e., differ by a unit factor, and if (j, n) = 1 then $x_j \in U(R)$.
- (ii) If R contains an ideal I of finite norm N=#(R/I)>1, then the prime divisors of cycle-lengths in R cannot exceed N.
- (iii) If there is a polynomial cycle of odd length in R, then the set Ex(R) is non-empty.
- (iv) If $(0, 1, x_2, \ldots, x_{n-1}, 0)$ is a normalized cycle of length $n \ge 3$ in R, and I is an ideal in R of norm N(I) < n, then some non-zero element of that cycle lies in I.

(v) If $(0, x_1, x_2, \ldots, x_{n-1}, 0)$ is an n-cycle in R, then x_1 divides x_j for $j = 2, 3, \ldots, n-1$, and if the polynomial $f(X) = A_m X^m + \cdots + 1$ realizes the corresponding normalized cycle $(0, 1, x_2/x_1, \ldots, x_{n-1}/x_1, 0)$, then A_m is divisible by x_1^{m-1} .

Proof. For the assertions (i), (ii) see Lemma 12.8 and its Corollary 1 in [7], (iii) is a consequence of (i), and (iv) appears in [8] (Corollary 2 to Lemma 1). Finally, for assertion (v) see the proof of Theorem 2 in [4].

In the next proposition we collect certain results concerning cycle lengths:

Proposition 2. (i) If ε is an exceptional unit, then $(0, 1, \varepsilon, 0)$ is a 3-cycle, and every normalized 3-cycle arises in this way.

- (ii) If $\alpha, \beta \in R$, then $(0,1,\alpha,\beta,0)$ is a normalized 4-cycle for a polynomial in R[X] if and only if $\beta \neq 1$, the elements $\beta, 1-\alpha$, $\alpha-\beta$ are units of R, and the elements α and $1-\beta$ are associated. If R does not contain the fourth primitive root of unity, and the equation u+v+w=1 has no solutions in units $\neq 1$, then there are no 4-cycles in R.
- (iii) Let R be a finitely generated integral domain and assume that we have a complete list, say

$$(0, \alpha_i, \beta_i, 0)$$
 $(j = 1, 2, \dots, N)$

of pairwise non-equivalent 3-cycles in R. Without restriction we may assume, multiplying, if necessary, all elements of a cycle by a unit, that if α_j and α_k are associated then they are equal.

If now

$$\xi = (0, 1, x_2, x_3, x_4, x_5, 0)$$

is a normalized 6-cycle in R, then there exists j and k such that $\alpha_j = \alpha_k$ and

$$x_2 = \varepsilon \alpha_i$$
, $x_3 = 1 + \beta \alpha_i$, $x_4 = \varepsilon \beta_i$, $x_5 = 1 + \eta \beta_k$,

where $\varepsilon = 1/u$, $\eta = -1/z$, u is a solution of the unit equation $u + v = \alpha_j$, and z is a solution of the unit equation $z + w = \beta_k$.

(iv) Let p be a prime, and denote by \mathbf{Z}_p the ring of integers of the p-adic field \mathbf{Q}_p . Then

$$C(\mathbf{Z}_p) = \begin{cases} \{1, 2, 4\} & \text{if } p = 2, \\ \{1, 2, 3, 4, 6, 9\} & \text{if } p = 3, \\ \{ab : 1 \le a \le p, b|p-1\} & \text{if } p \ge 5. \end{cases}$$

Proof. The assertion (i) is a direct consequence of Proposition 1 (i), for (ii) see Lemma 5 of [3], and for (iii) see Lemma 9 (i) in [8]. The last assertion has been proved in [10].

Corollary. Let R be a finitely generated domain of zero characteristics, and assume that it does not contain a primitive fourth root of unity. The following procedure leads to a complete list of all normalized 4-cycles in R:

Let (u_j, v_j, w_j) (j = 1, 2, ..., N) be the complete list of all non-trivial solutions of the equation u + v + w = 1 in units of R.

- (i) If $1 u_j$ and $1 + u_j$ are associated, then $(0, 1, 1 u_j, 1 + u_j, 0)$ is a 4-cycle, and the same applies if one replaces u_j by v_j , or w_j .
- (ii) If $1 v_j$ and $1 u_j$ are associated, then $(0, 1, 1 v_j, u_j, 0)$ is a 4-cycle, and the same applies if one replaces the pair u_j, v_j by u_j, w_j , or by w_j, v_j .

Proof. Part (ii) of the Proposition shows that every 4-cycle $(0, 1, \alpha, \beta, 0)$ leads to a solution of the equation (3), due to

$$(1 - \alpha) + (\alpha - \beta) + \beta = 1.$$

If this solution is trivial, then one sees easily that $\alpha - \beta = 1$, since otherwise we would have $1 + \beta^2 = 0$. This corresponds to the case (i). If it is non-trivial, then we arrive at the case (ii).

3. We need also certain results concerning unit equations, but first we recall certain well-known properties of cubic fields with negative discriminants of small absolute values:

Proposition 3. Let K be a real cubic field of discriminant d(K).

- (i) If d(K) = -23, then $K = Q(\theta_1)$ with $\theta_1^3 \theta_1 1 = 0$. The smallest prime ideal norms equal 5 and 7, and $\theta_1 = 1.3247...$
- (ii) If d(K) = -31, then $K = Q(\theta_2)$ with $\theta_2^3 \theta_2^2 1 = 0$. The minimal ideal norm equals 3, and $\theta_2 = 1.4655...$
- (iii) If d(K) = -44, then $K = Q(\theta_3)$ with $\theta_3^3 \theta_3^2 \theta_3 1 = 0$. The minimal ideal norm equals 7, and $\theta_3 = 1.8392...$
- (iv) If d(K) = -59, then $K = Q(\theta_4)$ with $\theta_4^3 2\theta_4^2 1 = 0$. The minimal ideal norm equals 2, and $\theta_4 = 2.2055...$

In all cases the generating element θ_i is the unique fundamental unit exceeding 1.

Proposition 4. ([6]) Let K be a cubic field of negative discriminant d(K).

- (i) If $d(K) \neq -23, -31$ then $Ex(K) = \emptyset$.
- (ii) If d(K) = -23, then

$$Ex(K) = \{ \pm \theta_1, \theta_1^2, \pm (1 - \theta_1^2), 1 \pm \theta_1, -\theta_1 \pm \theta_1^2, 2 - \theta_1^2, 1 + \theta_1 \pm \theta_1^2 \}.$$

(iii) If d = -31, then

$$Ex(K) = \{\theta_2, 1 - \theta_2, -\theta_2^2, 1 + \theta_2 - \theta_2^2, -\theta_2 + \theta_2^2, 1 + \theta_2^2\}.$$

We need also a complete list of non-trivial unit solutions $\neq 1$ of the equation (3) in the considered cubic fields. Note that if we have such a solution, then dividing both sides of the equation consecutively by u, v and w we obtain again its solutions. Since all units in the considered fields are of the form $\pm \varepsilon^k$, where $\varepsilon > 1$ is the fundamental unit and k is a rational integer, therefore its suffices to find all solutions $u, v, w \neq 1$ of (3) satisfying $u = \pm \varepsilon^a$, $v = \pm \varepsilon^b$, $w = \pm \varepsilon^c$ with $a, b, c \geqslant 0$. Such solutions will be called fundamental.

Lemma 1. Let K be a real cubic field of discriminant d(K) < 0.

- (i) ([9]) If $d(K) \notin \{-23, -31, -44, -59\}$ then the equation (3) has no non-trivial solutions in units $\neq 1$ of K.
 - (ii) If d(K) = -23, then all fundamental solutions of (3) are given by

$$\begin{split} 1 &= \theta_1^{10} - \theta_1^9 - \theta_1^4 = \theta_1^8 - \theta_1^7 - \theta_1^1 = \theta_1^8 - \theta_1^6 - \theta_1^4 = \theta_1^6 - \theta_1^4 - \theta_1^1, \\ 1 &= \theta_1^5 - \theta_1^2 - \theta_1^1 = \theta_1^7 - \theta_1^4 - \theta_1^4 = -\theta_1^4 + \theta_1^3 + \theta_1^2 = -\theta_1^6 + \theta_1^5 + \theta_1^3, \\ 1 &= -\theta_1^9 + \theta_1^8 + \theta_1^5 = -\theta_1^7 + \theta_1^5 + \theta_1^5. \end{split}$$

(iii) If d(K) = -31, then all fundamental solutions of (3) are given by

$$1 = \theta_2^7 + (-\theta_2^5) + (-\theta_2^5) = \theta_2^6 + (-\theta_2^5) + (-\theta_2^5) + (-\theta_2^5) + (\theta_2^5) +$$

(iv) If d(K) = -44, then all fundamental solutions of (3) are given by $1 = \theta_3^3 + (-\theta_3^2) + (-\theta_3) = -\theta_3^4 + \theta_3^3 + \theta_3^3.$

(v) If d(K) = -59, then the only fundamental solution of (3) is given by

$$1 = \theta_4^3 + (-\theta_4^2) + (-\theta_4^2).$$

Proof. Let u be a fixed real number larger than 1, and let G be the group consisting of all elements of the form $\pm u^k$ with rational integral k.

We outline now a very simple elementary approach to find all solutions of the equation x+y+z=1 with x,y,z being elements of G not equal to 1. This equation can be written in the form

$$\eta_1 u^a + \eta_2 u^b + \eta_3 u^c = 1, (4)$$

with $a, b, c \in \mathbf{Z}$ and $\eta_i = \pm 1$. We may assume that the inequalities $a \geqslant b \geqslant c$ hold.

Consider first the case $c \ge 1$. It is clear that $\eta_1 = \eta_2 = \eta_3$ is impossible, and moreover the cases

$$[\eta_1, \eta_2, \eta_3] \in \{[1, 1, -1], [1, -1, 1], [-1, 1, -1], [-1, -1, 1]\}$$

are also excluded, because in these cases we would have either $u^a+u^b=1+u^c\leqslant 1+u^b$ or $u^a+u^c=1+u^b\leqslant 1+u^a$ or $u^b=1+u^a+u^c>u^b$, or $u^c=1+u^a+u^b>u^c$, respectively. Hence we have either

$$u^b + u^c = 1 + u^a, (5)$$

or

$$u^a = 1 + u^b + u^c. (6)$$

The equation (5) leads to

$$u^{a-c} - u^{b-c} = 1 - u^{-c} < 1,$$

and the equation (6) implies

$$u^{a-c} - u^{b-c} = 1 + u^{-c} < 2.$$

Our assumptions imply that a>b, and in view of $\lim_{n\to\infty}(u^{n+1}-u^n)=\infty$ this shows that in both cases there are only finitely many possibilities for a-c and b-c. It follows that c lies in a finite set, and as $u^a-u^b=u^c\pm 1$, it follows that there are only finitely many possibilities for a,b and c.

If c = 0, then our assumptions imply $\eta_3 = -1$, so our equation becomes

$$\eta_1 u^a \pm \eta_2 u^b = 2,$$

and the only possibility turns out to be

$$u^a - u^b = 2.$$

which can hold only for finitely many values of a

It is clear that for any fixed value of u the obtained bounds for a,b,c are in all cases effective, and if u is not too close to 1, then these bounds are rather small, so a simple computer search leads to all fundamental solutions of the equation (4). In our case we have

$$1.3 < \theta_i < 2.3$$

and this leads to $0 \le b-c \le a-c \le 7$, which makes the computation trivial, even by hand.

Corollary. Let K be a cubic field with d(K) < 0 and let \mathbf{Z}_K be its ring of integers.

(i) If $d(K) \not\in \{-23, -31, -44, -59\}$, then the length of any polynomial cycle in ${\bf Z}_K$ equals 1 or 2.

(ii) If $d \in \{-44, -59\}$ then every cycle length in \mathbf{Z}_K is a power of 2.

Proof. Follows from Proposition 1 (iii), Proposition 2 (ii), and the last Lemma.

4. Proof of the theorem

If $d(K) \notin \mathcal{X} = \{-23, -31, -44, -59\}$, then the assertion results from the Corollary to Lemma 1, hence we may assume that d(K) lies in \mathcal{X} . Observe now that Proposition 2 (ii) implies that if there is a non-trivial solution of (3) with $u = v \in \mathbf{Z}_K$, then there exists a 4-cycle. Using Lemma 1 we obtain thus the existence of 4-cycles in every of the four fields considered.

Let now d=-23. In this case there is an ideal P of norm 5, hence $\mathbf{Z}_K\subset\mathbf{Z}_5$, and using Proposition 2 (iv) we obtain that the possible cycle lengths are contained in $\{1,2,3,4,5,6,8,10,12,16,20\}$. Moreover, there is an unramified prime ideal of norm 7, hence, using again that Proposition, we eliminate 16 and 20 from this list. Since the polynomial

$$(2\theta_1^2 - 3)X^4 + (7 - 5\theta_1)X^3 - (7\theta_1^2 - 9\theta_1 + 1)X^2 + (5\theta_1^2 - 5\theta_1 - 4)X + 1$$

realizes the 5-cycle

$$(0, 1, \theta_1, -\theta_1, \theta_1^2, -\theta_1 + \theta_1^2, 0),$$

hence it remains to consider possible cycles of length 6, 8 and 10.

Proposition 2 (i) and Proposition 4 (ii) were used to make a list of all normalized 3-cycles. It turned out that the leading coefficients of the relevant interpolation polynomials were either units, or associated to the number $2 + \theta_1$. In view of Proposition 1 (v) every 3-cycle must be equivalent to a cycle of the form (0, a, ua, 0), $u \in Ex(\mathbf{Z}_K)$, and $u \in \{1, 2 + \theta_1\}$. Now a simple computer check using PARI, and based on Proposition 2(iii) showed that there are no 6-cycles.

If $(0, 1, x_2, ..., x_7, 0)$ were an 8-cycle, then the elements x_3, x_5, x_7 would be units, and therefore, according to Proposition 1 (iv), the prime ideal P_7 of norm 7 would divide one of the elements x_2, x_4, x_6 . However $(0, x_2, x_4, x_6, 0)$ is a 4-cycle, and a simple computer search, based on a list of all 4-cycles prepared with the help of Corollary to Proposition 2, shows that no element of a 4-cycle is contained in P_7 .

To deal with cycles of length 10 we first made, with PARI, a list of all normalized 5-cycles, using the fact that they must be of the form (0,1,a,b,c), where a,b,c are exceptional units. It turned out that there are 118 such cycles, and none of their leading coefficient is divisible by a non-unit cube, so every 5-cycle differs from a normalized cycle by a unit factor. If now $(0,1,x_2,\ldots,x_9,0)$ is a normalized 10-cycle, then by Proposition 1 (i) the elements x_3,x_7 and x_9 are units, and since $(0,x_2,x_4,x_6,x_8,0)$ is a 5-cycle, the elements x_{2m} are units for m=1,2,3. It follows moreover form Proposition 1 (i) that x_2-1 is a unit, hence x_2 is an exceptional unit, and repeating this argument we see that for j=2,3,4,7,8,9 the element x_j is an exceptional unit. Therefore the only non-zero non-unit element of our cycle must be x_5 , and by Proposition 1 (iv) it must be contained in ideals of norm 5 and 7. By Proposition 1 (i) the numbers x_7-x_2 and x_5 are associated, hence $|N(x_7-x_2)|$ must be divisible by 35. This is, however, not possible, since the maximal norm of an ideal generated by the difference of two exceptional units equals 11. Therefore there are no 10-cycles in \mathbf{Z}_K .

Now let d = -31. Since there is an unramified prime ideal P of norm 3, thus $\mathbf{Z}_K \subset \mathbf{Z}_3$, and we obtain that the set of possible cycle-lengths is contained in $\{1, 2, 3, 4, 6, 9\}$. Since the polynomial

$$-(1+4\theta_2^2)X^5 + (16\theta_2^2 + 9\theta_2 + 8)X^4 - (33\theta_2^2 + 17\theta_2 + 22)X^3 + (31\theta_2^2 + 15\theta_2 + 20)X^2 - (10\theta_2^2 - 6\theta_2 - 6)X + 1$$

realizes the 6-cycle $(0,1,\theta_2,\theta_2^2-\theta_2+1,\theta_2^2,\theta_2^2-\theta_2,0)$, it remains to show that there are no 9-cycles in this case.

Assume now that $(0,1,x_2,\ldots,x_8,0)$ is a 9-cycle. By Proposition 1 (i) x_2,x_4,x_5,x_7 and x_8 are units, and x_2,x_5 are exceptional units. According to Proposition 2 (i) every normalized 3-cycle has the form $(0,1,\varepsilon,0)$, where ε is an exceptional unit. Constructing the Lagrange interpolation polynomials realizing these cycles one sees that their leading coefficients are either units, or are associated with $1+\theta_2$, therefore (by Propositions 1 (v) and 2 (i)) every 3-cycle containing 0 has the form $(0,ua,ua\varepsilon,0)$, where u is a unit, $u\in\{1,1+\theta_2\}$ and ε is an exceptional unit. Since $(0,x_3,x_6,0)$ is a 3-cycle we see that x_3,x_6 are either units, or are associated with $1+\theta_2$. The norm of $1+\theta_2$ being equal to 3 we see that none of the elements of our cycle can be divisible by the ideal I_2 generated by 2, and since I_2 is of norm 8<9, this contradicts Proposition 1 (iv).

In the case d = -44 we have to exclude the existence of an 8-cycle. Assume thus that $(0, 1, x_2, \ldots, x_7, 0)$ is such a cycle. Then $(0, x_2, x_4, x_6, 0)$ is a 4-cycle. Using Lemma 1 (iv) and Proposition 2 (ii) we obtain that every normalized 4-cycle is of the form $(0, 1, \alpha, \beta, 0)$, where

$$(a,b) \in \{ (1 - \theta_3^3, -\theta_3), \quad (1 - \theta_3, -\theta_3^{-1}), \quad (1 - \theta_3^{-3}, \theta_3), \quad (1 + \theta_3, -\theta_3^{-1}), \\ (1 + \theta_3^{-1}, -\theta_3), \quad (1 - \theta_3^{-1}, \theta_3^{-3}), \quad (1 - \theta_3^3, \theta_3^3), \quad (1 - \theta_3^{-1}, \theta_3^{-1}) \}.$$

Note that in all cases we have $N(a) = \pm 2$ and b is a unit. Since the only principal ideal of norm 2 is generated by $1 - \theta_3$ it follows that every element a has the form $u(1 - \theta_3)$ with some unit u.

Computing the cubic polynomials realizing these cycles one finds that the norms of their leading coefficients lie in the set $\{-4,8,47\}$. Proposition 1 (v) implies that x_2^2 divides one of these coefficients. Since the prime 47 splits in our field it follows that x_2 is either a unit, or is of norm ± 2 , hence has the form $\epsilon(1-\theta_3)$ with a unit ϵ . The first case is impossible, because x_2-1 is a unit, due to Proposition 1 (i), so x_2 would be an exceptional unit, contradicting Proposition 3 (i). Thus $x_2 = \epsilon(1-\theta_3)$, and since $N(x_4/x_2) = \pm 2$, so $N(x_4) = \pm 4$. Now Proposition 1 (i) shows that x_3, x_5, x_7 are units, and since there is a prime ideal P of norm 7 we deduce by Proposition 1(iv) that x_6 is divisible by P. This is however not possible, as $N(x_6/x_2) = 2$. Therefore there is no 8-cycle in the case d = -44.

If d=-59, then Proposition 3 implies $\mathbf{Z}_K\subset\mathbf{Z}_2$, hence by [10] the possible cycle-lengths lie in $\{1,2,4\}$.

References

- [1] Baron, G., Polynomiterationen in algebraischen Zahlkörpern, preprint 1991.
- [2] Boduch, J., Polynomial cycles in rings of algebraic integers, M.A. thesis, Wrocław University 1990. (Polish)
- [3] Halter-Koch, F., Narkiewicz, W., *Polynomial cycles and dynamical units*, Proc. Conf. Analytic and Elementary Number Theory, 70–80, Wien 1997.
- [4] Halter-Koch, F., Narkiewicz, W., Scarcity of finite polynomial orbits, Publicationes Math., **56**, 2000, 405–414.
- [5] Marszałek, R., Narkiewicz, W. Finite polynomial orbits in quadratic rings, Ramanujan J., in print.
- [6] Nagell, T., Quelques problèmes relatifs aux unités algébriques, Arkiv Mat., 8, 1969, 115–127.
- [7] Narkiewicz, W., Polynomial Mappings, Lecture Notes in Math. 1600, Springer 1995.
- [8] Narkiewicz, W., Polynomial cycles in certain rings of rationals, J. Théorie des Nombres de Bordeaux, 14, 2002, 529–552.
- [9] Narkiewicz, W., Pezda, T., Finite polynomial orbits in finitely generated domains, Monatsh. Math., 124, 1997, 309–316.
- [10] Pezda, T., Polynomial cycles in certain local domains, Acta Arith., 66, 1994, 11–22.

Address: Institute of Mathematics, Wrocław University

E-mail: E-mail: narkiew@math.uni.wroc.pl Received: 21 March 2005; revised: 28 April 2005