Functiones et Approximatio
49.2 (2013), 391–409
doi: 10.7169/facm/2013.49.2.16

POLYNOMIAL CYCLES IN RINGS OF INTEGERS IN FIELDS OF SIGNATURE $(0, 2)$

Tadeusz Pezda

Abstract: We find all possible cycle-lengths of polynomial mappings in one variable over rings of integers of number fields of signature $(0, 2)$. Such fields have unit rank 1, and possible cycle-lengths for other fields having unit rank $\leqslant 1$, but other signature, were found earlier by other authors.

Keywords: polynomial cycles, Dedekind rings, 3-unit equations, quartic extensions.

1. Introduction

For a commutative ring R with unity and $f \in R[X]$, we define a *cycle* for f as a k-tuple $x_0, x_1, \ldots, x_{k-1}$ of different elements of R such that

$$f(x_0) = x_1, \qquad f(x_1) = x_2, \qquad \ldots, \qquad f(x_{k-1}) = x_0.$$

The number k is called the *length* of this cycle.

Let $\mathcal{CYCL}(R)$ be the set of all possible lengths of cycles in R of polynomials $f \in R[X]$.

For an algebraic number field K, we denote by Z_K the ring of algebraic integers in K. A field K is said to have signature (r, s) if it has r real and $2s$ non-real embeddings. By Dirichlet's theorem, the rank of the group of units in Z_K equals $r + s - 1$. Put $\zeta_n = \exp(\frac{2\pi i}{n})$. Note that $[Q(\zeta_n) : Q] = \phi(n)$, and $\phi(n) \leqslant 4$ holds only for $n = 1, 2, 3, 4, 5, 6, 8, 10, 12$. Moreover, $Q(\zeta_6) = Q(\zeta_3)$; $Q(\zeta_{10}) = Q(\zeta_5)$; $Q(\zeta_2) = Q(\zeta_1) = Q$. By $\mathrm{Disc}(K)$ we denote the discriminant of K.

One can treat as an exercise to prove that $\mathcal{CYCL}(Z) = \{1, 2\}$. Boduch ([2]) and Baron ([1]) established the following result.

The author was partially supported by the MNiSW Grant N N201 366636.
2010 Mathematics Subject Classification: primary: 11R04; secondary: 11R16, 11R27

Theorem B. *Let K be a quadratic field. Write $K = Q(\sqrt{D})$ with a square-free integer D. Then $\mathcal{CYCL}(Z_K)$ equals*

$$\begin{aligned} \{1,2,3,6\} &\quad \text{for } D=-3,\\ \{1,2,3,4\} &\quad \text{for } D=5,\\ \{1,2,4\} &\quad \text{for } D=-1,2,\\ \{1,2\} &\quad \text{for } D\neq -3,-1,2,5. \end{aligned}$$

Around 2004, Narkiewicz [3] found sets $\mathcal{CYCL}(Z_K)$ for cubic fields with negative discriminant, i.e. with signature $(1,1)$.

Theorem N. *Let K be a cubic field with negative discriminant d. Then $\mathcal{CYCL}(Z_K)$ equals $\{1,2,3,4,5\}$ for $d=-23$; $\{1,2,3,4,6\}$ for $d=-31$; $\{1,2,4\}$ for $d=-44,-59$; and $\{1,2\}$ for other d.*

In these theorems the signature is $(2,0),(0,1)$ or $(1,1)$, hence the unit group has rank $\leqslant 1$. Moreover, for all but finitely many fields K of one of these signatures one has $\mathcal{CYCL}(Z_K)=\{1,2\}$.

In this paper we extend these results to fields of signature $(0,2)$. Note that the unit rank of such fields is 1, and for all other number fields K with unit rank $\leqslant 1$ the sets $\mathcal{CYCL}(Z_K)$ were established by Theorem B and Theorem N. Let us call a number field K *trivial* if for every $k\in\mathcal{CYCL}(Z_K)$ there is a subfield L of K, $L\neq K$, such that $k\in\mathcal{CYCL}(Z_L)$.

Theorem 1. *Let K be a field of signature $(0,2)$. Then $\mathcal{CYCL}(Z_K)$ equals:*

(i) $\{1,2,3,4,5,6\}$ *for* $K\sim Q(\theta)$, $\theta^4-\theta^3+2\theta^2-2\theta+1=0$, $\operatorname{Disc}(K)=117$;
(ii) $\{1,2,3,4,5,6,8,10\}$ *for* $K=Q(\zeta_{10})$, $\operatorname{Disc}(K)=125$;
(iii) $\{1,2,3,4,6,8,12\}$ *for* $K=Q(\zeta_{12})$, $\operatorname{Disc}(K)=144$;
(iv) $\{1,2,3,4,6\}$ *for* $K\sim Q(\theta)$, $\theta^4+\theta^3-2\theta+1=0$, $\operatorname{Disc}(K)=189$;
(v) $\{1,2,3,4\}$ *for* $K\sim Q(\theta)$, $\theta^4+\theta+1=0$, $\operatorname{Disc}(K)=229$;
(vi) $\{1,2,4,8\}$ *for* $K=Q(\zeta_8)$, $\operatorname{Disc}(K)=256$;
(vii) $\{1,2,4\}$ *for* $K\sim Q(\theta)$, $\theta^4+\theta^2+\theta+1=0$, $\operatorname{Disc}(K)=257$;
(viii) $\{1,2,3,4\}$ *for* $K\sim Q(\theta)$, $\theta^4+\theta^2+2\theta+1=0$, $\operatorname{Disc}(K)=272$;
(ix) $\{1,2,4\}$ *for* $K\sim Q(\theta)$, $\theta^4+\theta^3-\theta+1=0$, $\operatorname{Disc}(K)=392$;
(x) $\{1,2,3,4,6\}$ *for* $K\sim Q(\theta)$, $\theta^4+2\theta^3+6\theta^2+2\theta+1=0$, $\operatorname{Disc}(K)=432$;
(xi) $\{1,2,3,4,6\}$ *for* $K=Q(\sqrt{-3},\sqrt{-7})$, $\operatorname{Disc}(K)=441$.

Other K of signature $(0,2)$ are trivial.

The case of signature $(0,2)$ in comparison to signature $(1,1)$ is more complicated due to the bigger degree and the abundance of roots of unity $\neq\pm1$ in many such fields.

In Section 2 we give some lemmas of general character concerning polynomial cycles. In Section 3 we determine 17 fields, up to isomorphism, where something interesting may happen. Then, in Section 4, we find all $\mathcal{CYCL}(Z_K)$ in the fields determined in Section 3. Computer calculations were made with the help of PARI

and MAPLE. The main technical tool was an analysis of solutions of 3-unit equation $x+y+z=1$. As there is no known procedure to find all solutions of 3-unit equation in any number field with unit rank $\geqslant 2$, our approach does not lead to an algorithm determining $\mathcal{CYCL}(Z_K)$ for such fields.

Quite recently, we managed to propose a finitary procedure finding $\mathcal{CYCL}(Z_K)$, working for any number field K. But the problem with unit rank $\geqslant 2$ is that the procedure for finding all solutions of 2-unit equation $x+y=1$ can be carried out effectively only in a particular finite family of such fields.

2. Auxiliary results

2.1. General lemma

In this subsection R is a commutative ring with 1, and without zero divisors. Let K be the field of fractions of R. For $x,y\in R$, $x\sim y$ means that x and y are associated.

Lemma 1.

(i) *Let $x_0,x_1,\dots,x_{k-1}$ be a cycle of length k in R for $f(X)\in R[X]$. Then $x_i-x_0 \mid x_j-x_0$ for all $1\leqslant i\mid j\leqslant k-1$.*

(ii) *If $k\in\mathcal{CYCL}(R)$, then in R there is a cycle of length k of the form $0,1,\dots$.*

(iii) *Let $x_0,x_1,\dots,x_{k-1}$ be a cycle of length k in R for $g(X)\in R[X]$. Then the unique polynomial $f\in K[X]$ of degree $\leqslant k-1$ such that $f(x_0)=x_1, f(x_1)=x_2,\dots,f(x_{k-1})=x_0$ has coefficients in R.*

(iv) *Let $x_0,x_1,\dots,x_{k-1}$ be a cycle of length k in R. Then $x_j-x_i\sim x_{(j-i,k)}-x_0$ for $0\leqslant i<j<k$. In particular, in a cycle $x_0=0,x_1=1,x_2,\dots,x_{k-1}$ of length k in R the differences x_j-x_i are invertible for $(j-i,k)=1$.*

(v) *If $k\in\mathcal{CYCL}(R)$ and $l\mid k$, then $l\in\mathcal{CYCL}(R)$.*

(vi) *If $p\in\mathcal{CYCL}(R)$ is a prime, then $\{1,2,\dots,p\}\subset\mathcal{CYCL}(R)$.*

(vii) *$0,1,x_2$ is a cycle in R if and only if x_2 and $1-x_2$ are invertible.*

(viii) *Let $\mathcal{A}=\{a_1,a_2,\dots,a_n\},\mathcal{B}=\{b_1,b_2,\dots,b_n\}$ be subsets of R such that $a_i-a_j, b_i-b_j, a_i-b_j, b_i-a_j$ are units for all $i<j$. If for all i,j one has $a_i-b_i\sim a_j-b_j$, then $\{2,4,\dots,2n\}\subset\mathcal{CYCL}(R)$.*

(ix) *$0,1,x_2,x_3$ is a cycle in R if and only if $x_2\neq 0$, $x_2\sim x_3-1$ and x_2-1, x_3-x_2, x_3 are invertible.*

(x) *Let $u,v\neq 1$ be units in R such that $1-u-v$ is a unit, and $1-u\sim 1-v$. Put $\epsilon=(v-1)/(1-u)$. Then $0,1,1-u,v$ is a cycle in R, and $0,t,t(1-u),tv$ is a cycle in R if and only if $t\mid u+\epsilon$ and $t^2\mid(1+\epsilon^2)(u(\epsilon-1)+\epsilon^2)$.*

(xi) *Let $0,1,x_2,x_3,x_4,x_5$ be a cycle for $f\in R[X]$, with $\delta=\frac{x_4}{x_2}$. Then in R there is a cycle of the form $0,1,y_2,y_3,y_4,y_5$ with $\frac{y_4}{y_2}=\gamma$, for any $\gamma\in\mathcal{A}(\delta):=\{\delta,\frac{1}{\delta},1-\delta,\frac{1}{1-\delta},\frac{\delta-1}{\delta},\frac{\delta}{\delta-1}\}$. Moreover, $\mathcal{A}(v_1)=\mathcal{A}(v_2)$ for any $v_2\in\mathcal{A}(v_1)$.*

Proof. (i) For all m we have $x_{mi}-x_{(m-1)i}=f^{\circ((m-1)i)}(x_i)-f^{\circ((m-1)i)}(x_0)$, which is divisible by x_i-x_0. The rest of the proof is clear.

(ii) Let $x_0, x_1, \dots, x_{k-1}$ be a cycle for $f(X) \in R[X]$. Then $0, 1, \frac{x_2-x_0}{x_1-x_0}, \frac{x_3-x_0}{x_1-x_0}, \dots, \frac{x_{k-1}-x_0}{x_1-x_0}$ is a cycle for $g(X) = \frac{1}{x_1-x_0}(f((x_1-x_0)X+x_0)-x_0)$. Clearly $g(X) \in R[X]$.

(iii) $f(X)$ is the remainder of the division of $g(X)$ by $(X-x_0)\cdot\ldots\cdot(X-x_{k-1})$, so $f(X) \in R[X]$.

(iv) This claim was proved in [4] for $(j-i,k)=1$. The general case requires only minor, and obvious, changes.

(v) Obvious.

(vi) In view of (ii) it is sufficient to consider a cycle $x_0 = 0, x_1 = 1, x_2, \dots, x_{p-1}$. Since (iv) shows that all the differences $x_j - x_i$ are invertible, for any $1 \leqslant k \leqslant p$ the Lagrange interpolation polynomial realizing the cycle $0, 1, \dots, x_{k-1}$ has its coefficients in R.

(vii) $0, 1, x_2$ is the cycle for $1 + (x_2-1)X - \frac{x_2^2-x_2+1}{x_2(x_2-1)}X(X-1)$.

(viii) Take any $k \leqslant n$. Let $c \sim a_i - b_i$ for all i. One sees that every coefficient of the Lagrange interpolation polynomial for the cycle $a_1, a_2, \dots, a_k, b_1, b_2, \dots, b_k$ is the ratio of two determinants. The determinant A in the denominator is associated to c^k. As the difference of l-th and $l+k$-th rows in the determinant B in the numerator is divisible by c we see that c^k divides B, thus $B/A \in R$.

(ix) It follows from (iv) that the conditions are necessary. To obtain their sufficiency it is enough to observe that the Lagrange interpolation polynomial realizing the cycle $0, 1, x_2, x_3$ has all its coefficients in R.

(x) By (ix), $0, 1, 1-u, v$ is the cycle in R. Let $f(X)$ be the unique polynomial of degree $\leqslant 3$ realizing this cycle. Then $0, t, t(1-u), tv$ is a cycle for the unique polynomial $g(X) \in K[X]$ of degree $\leqslant 3$. One sees that $g(X) = tf(\frac{1}{t}X)$. Using (iii) and calculating the coefficients of $f(X)$ we get the assertion.

(xi) We see that $0, 1, \frac{x_4-x_2}{x_3-x_2}, \frac{x_5-x_2}{x_3-x_2}, \frac{-x_2}{x_3-x_2}, \frac{1-x_2}{x_3-x_2}$ is a cycle for $g(X) = \frac{1}{x_3-x_2}(f((x_3-x_2)X+x_2)-x_2) \in R[X]$, and we have $\frac{-x_2}{x_4-x_2} = \frac{1}{1-\delta}$. In a similar manner we get the other elements from $\mathcal{A}(\delta)$. The last claim may be verified directly. ∎

2.2. Lemmas for number fields

In this section K is an algebraic number field.

Lemma 2. *Let L be a subfield of K. If $k \in \mathcal{CYCL}(Z_K) \setminus \mathcal{CYCL}(Z_L)$, then in Z_K there is a cycle of the form $0, 1, z_2, \dots, z_{k-1}$ (and clearly of length k) with $z_2 \notin L$.*

Proof. Let $t_0 = 0,\ t_1 = 1,\ t_2, \dots, t_{k-1}$ be a cycle in Z_K. Since $k \notin \mathcal{CYCL}(Z_L)$, there is the smallest $l \leqslant k-1$ such that $t_l \notin L$. Then $y_0 = t_{l-2},\ y_1 = t_{l-1},\ y_2 = t_l, \dots, y_{k-2} = t_{k+l-4 \pmod k},\ y_{k-1} = t_{k+l-3 \pmod k}$ is a cycle (for the same map as for the initial cycle). But then $0, 1, \frac{y_2-y_1}{y_1-y_0}, \dots$ is a cycle in Z_K, with $\frac{y_2-y_1}{y_1-y_0} \notin L$. ∎

Lemma 3. *Let K be a subfield of C of signature $(0,2)$. Assume that K is not trivial. Then there is a unit $d \in Z_K$ such that $K = Q(d)$ and every unit u of Z_K is of the form $u = d^m\zeta$, for some integer m and a root of unity ζ.*

Proof. Let ρ be a fundamental unit of K. If $Q(\rho) = K$, then it is sufficient to take $d = \rho$.

Assume that $Q(\rho)$ is a proper subfield of K. Then $Q(\rho)$ is quadratic and real, since in imaginary quadratic fields there are no units of infinite order. If for some $n \geqslant 3$ the number ζ_n belongs to K, then $\rho\zeta_n$ is also a fundamental unit of K. From $(\rho\zeta_n)^n = \rho^n \notin Q$, we conclude that $Q(\rho) = Q(\rho^n) \subset Q(\rho\zeta_n)$ and $Q(\rho^n) \neq Q(\rho\zeta_n)$. Consequently, $Q(\rho\zeta_n) = K$, and it is sufficient to take $d = \rho\zeta_n$.

There remains the case when all roots of unity in K are ± 1. Then every unit lies in $Q(\rho)$.

Let $k \in \mathcal{CYCL}(Z_K) \setminus \mathcal{CYCL}(Z_{Q(\rho)})$. Lemma 2 gives that in Z_K there is a cycle of the form $0, 1, z_2, \ldots$ of length k, with $z_2 \notin Q(\rho)$. Since Lemma 1(iv) shows that $z_2 - 1$ is invertible, we get a contradiction. ∎

Lemma 4.

(i) *The numbers* $\zeta_6, \zeta_6^5, \frac{3\pm\sqrt{5}}{2}, \frac{\pm 1\pm\sqrt{5}}{2}$ *are the only algebraic integers* v *of degree* 2 *such that* $0, 1, v$ *is a cycle in* Z_L *for any number field* L *containing* v.

(ii) *The numbers* $\pm i, \pm 2 \pm \sqrt{5}, \frac{\pm 1\pm\sqrt{5}}{2}, \pm 1 \pm \sqrt{2}$ *are the only algebraic integers* w *of degree* 2 *such that* $0, 1, 1 + w, w$ *is a cycle in* Z_L *for any number field* L *containing* w.

Proof. (i) Let $X^2 + aX + \epsilon$ be the minimal polynomial for v. By Lemma 1(vii), we see that $\epsilon \in \{-1, 1\}$ and $1 + a + \epsilon \in \{-1, 1\}$. In this way we get that $X^2 - X + 1$, $X^2 - 3X + 1$, $X^2 + X - 1$, $X^2 - X - 1$ are the only possible minimal polynomials for v.

(ii) Let $X^2 + aX + \epsilon$ be the minimal polynomial for w. By Lemma 1(ix) we see that w is invertible, i.e. $\epsilon \in \{-1, 1\}$. Moreover, the same lemma gives that for $\delta \in \{-1, 1\}$ we have $w + \delta \mid 2$, which in turn, considering the minimal polynomial for $\frac{2}{w+\delta}$, gives $1 + \epsilon - a\delta \mid 4$ and $1 + \epsilon - a\delta \mid 2a$. In this way we get that $X^2 + 1, X^2 \pm 4X - 1, X^2 \pm 2X - 1, X^2 \pm X - 1$ are the only possible minimal polynomials for w. ∎

2.3. Cycles of length 4 and the equation $u + v + w = 1$ in units

Let K be a number field of signature $(0, 2)$. If $0, 1, x_2, x_3$ is a cycle of length 4 in Z_K, then $u = 1 - x_2, v = x_2 - x_3, w = x_3$ are units satisfying

$$u + v + w = 1 \tag{1}$$

(we consider (u, v, w) as a solution of (1) only if $u + v + w = 1$ and u, v, w are units).

As $x_2 \sim 1 - x_3$, we have $1 - u \sim 1 - w$, and $N_{K/Q}(1 - u) = N_{K/Q}(1 - w)$ follows.

It may occur that some of u, v, w equal 1. If this happens, then in view of $x_2 \neq 0$ and $x_3 \neq 1$ we must have $v = 1$. In this case we have the cycle $0, 1, 1 + x_3, x_3$ in Z_K provided x_3 is a unit satisfying $x_3 - 1 \sim x_3 + 1$. Such cycles will require a special consideration.

If none of u, v, w equals 1, then we have so-called non-trivial solution of (1). It is known that for any number field K there is only a finite number of such solutions. For some fields K we will find them explicitly.

To each non-trivial solution of $u + v + w = 1$ in units we attach a triple $(N_{K/Q}(1-u), N_{K/Q}(1-v), N_{K/Q}(1-w))$ of integers. As we noted earlier, if a non-trivial solution (u, v, w) of (1) comes from a cycle $0, 1, x_2, x_3$, then $1 - u \sim 1 - w$ and $N_{K/Q}(1-u) = N_{K/Q}(1-w) = N_{K/Q}(x_2)$ follows.

Let us define some useful sets related to (1).

Definition 1. *Let*

- $\mathcal{D}(K)$ *be the set of attached triples to all non-trivial solutions of (1) in* Z_K*, where we neglect the order of terms in attached triples;*
- $d(K)$ *be the set consisting of all natural numbers appearing in the triples from* $\mathcal{D}(K)$*;*
- $d_1(K)$ *be the set consisting of all natural numbers* n *such that there is a non-trivial solution* (u, v, w) *of (1) satisfying* $1-u \sim 1-w$ *and* $n = N_{K/Q}(1-u) = N_{K/Q}(1-w)$*. Hence* $d_1(K)$ *is the set consisting of* $N_{K/Q}(x)$*, where in* Z_K *there is a cycle of the form* $0, 1, x, x_3$ *with* $x \neq x_3 + 1$*;*
- $\mathcal{E}(K)$ *be the set of all* $w \in Z_K$ *such that* $0, 1, 1 + w, w$ *is a cycle in* Z_K*;*
- $e(K)$ *be the set consisting of* $N_{K/Q}(1 + w)$*, where* $w \in \mathcal{E}(K)$*;*
- $g(K) = e(K) \cup d_1(K)$ *be the set consisting of* $N_{K/Q}(x)$*, where in* Z_K *there is a cycle of the form* $0, 1, x, x_3$*.*

For any natural k *put* $m(k) = m(k, K) = \prod_{\mathfrak{p} \in I(k,K)} N(\mathfrak{p})$*, where* $I(k, K)$ *is the family of all prime ideals in* Z_K *having norms* $< k$ *and* $N(\mathfrak{p})$ *is the norm of* $\mathfrak{p}$*.*

Define also $\mathcal{V}(K)$ *as the set of all* $v \in Z_K$ *such that* $0, 1, v$ *is a cycle in* Z_K*.*

We introduce an equivalence relation in the set of all non-trivial solutions of $u+v+w = 1$ as the minimal equivalence relation $\simeq$ such that $(u, v, w) \simeq (v, u, w) \simeq (u, w, v) \simeq (\frac{1}{u}, -\frac{v}{u}, -\frac{w}{u})$. We observe that equivalent solutions have the same triple attached, except for possible reordering. One sees that equivalent solutions of (1) are trivial (or non-trivial) at the same time.

When listing the non-trivial solutions of (1) or the attached triples, we will try to avoid mentioning equivalent solutions, or the attached triples differing only by the order of appearance.

2.4. Embeddings into local rings

Let K be a number field. If Z_K is embeddable into a ring S, then clearly $\mathcal{CYCL}(Z_K) \subset \mathcal{CYCL}(S)$. Let $\mathfrak{p}$ be a non-zero prime ideal of Z_K. Let S be the completion of $(Z_K)_{\mathfrak{p}}$ with respect to the natural valuation. Then S is a discrete valuation domain. Let $\mathfrak{P}$ be its maximal ideal. Put $p^f = |S/\mathfrak{P}| = |Z_K/\mathfrak{p}|$, where p is prime. So p^f is the norm of $\mathfrak{p}$. A cycle $x_0, x_1, \ldots$ in S is called a $*$-cycle if $x_i - x_j \in \mathfrak{P}$ for all i, j.

Lemma 5. *Let S be as above.*

(i) *If k is the length of a $*$-cycle in S, then k is of the form $k = a \cdot p^{\alpha}$, where $a \mid p^f - 1$.*
(ii) *If l is the length of a cycle in S, then $l = ck$, where $c \leqslant p^f$ and k is the length of a $*$-cycle.*
(iii) *The length of any cycle in Z_K is a product of primes not exceeding p^f.*
(iv) *If $x_0 = 0, x_1, \ldots, x_{k-1}$ is a cycle in S of length $k > p^f$ and $i_0 = \min\{j > 0 : x_j \in \mathfrak{P}\}$, then $i_0 \mid k$ and $i_0 \leqslant p^f$. Moreover, k/i_0 is the length of a $*$-cycle.*
(v) *$\mathcal{CYCL}(Z_2) = \{1, 2, 4\}$, where Z_2 is the ring of 2-adic integers.*

Proof. These assertions were proved in [4]. ■

2.5. Sufficient conditions for nonexistence of cycles of some specific lengths

Let K be a number field of signature $(0, 2)$.

Lemma 6. *Let $k = q^a > 4$ (with prime q) be a prime power. There are no cycles of length k in Z_K if at least one of the following conditions holds.*

(i) *The product $m(k)$ of norms of all prime ideals in Z_K having norms $< k$ does not divide*
   (a) *any element of $g(K)$, for $q = 2$;*
   (b) *any element of $d_1(K)$, for $q > 2$.*
(ii) *$d_1(K)$ is empty.*

Proof. (i) Let $x_0 = 0, x_1 = 1, x_2, \ldots, x_{q^a-1}$ be a cycle in Z_K. Let $\mathfrak{p}$ be a prime ideal of norm $< k = q^a$. By Lemma 1 and Lemma 5(iv) we get $x_{q^{a-1}} \in \mathfrak{p}$. Hence $x_{q^{a-1}}$ belongs to the product of all prime ideals $\mathfrak{p}$ of norm $< k$, and $m(k) \mid N_{K/Q}(x_{q^{a-1}})$ follows. Suppose that $a \geqslant 2$. As (by Lemma 1) $0, 1, x_{q^{a-1}}, x_{q^{a-1}+1}$ and (for $q > 2$) $0, 1, x_{q^{a-1}}, x_{2q^{a-1}+1}$ are cycles, we get the sufficiency of (i) for $a \geqslant 2$.

Let $a = 1$. Lemma 5(iii) gives $m(k) = m(q) = 1$. Since $0, 1, x_2, x_3$ and $0, 1, x_2, x_4$ are cycles in Z_K, we get $d_1(K) \neq \varnothing$. We thus obtain the sufficiency of (i) for $a = 1$.

(ii) By (i)(b), it suffices to deal with $q = 2$. Let $x_0 = 0, x_1 = 1, x_2, \ldots, x_{2^a-1}$ be a cycle in Z_K. Then Lemma 1(iv),(ix) shows that $0, 1, x_2, x_3$ and $0, 1, x_2, x_{2^a-1}$ are also cycles, and at least one of them is not of the form $0, 1, 1 + w, w$. Thus $d_1(K)$ is not empty. ■

Lemma 7. *Assume that at least one of the following conditions holds.*

(a) *$g(K)$ consists of one element;*
(b) *if $0, t, ty_2, ty_3$ is a cycle (clearly, $t, y_2, y_3 \in Z_K$), then t is invertible.*

If there is a prime ideal $\mathfrak{p}$ in Z_K such that $N(\mathfrak{p}) < 12$ and $N(\mathfrak{p})$ does not divide any element of $g(K)$, then $12 \notin \mathcal{CYCL}(Z_K)$.

Proof. Let $0, 1, x_2, \ldots, x_{11}$ be a cycle in Z_K, and let $\mathfrak{p}$ be a prime ideal satisfying $N(\mathfrak{p}) < 12$. Lemma 5 shows that $x_4 \in \mathfrak{p}$ or $x_6 \in \mathfrak{p}$. Lemma 1 gives that $0, 1, x_6, x_7$ and $0, 1, \frac{x_6}{x_3}, \frac{x_9}{x_3}$ are cycles in Z_K.

Suppose that $g(K) = \{n\}$. This gives $N_{K/Q}(\frac{x_6}{x_3}) = N_{K/Q}(x_6) = n$, and $N_{K/Q}(x_3) = 1$ follows.

Note that $0, x_3, x_6, x_9$ is a cycle. If (b) holds, then x_3 is a unit.

We may thus assume that x_3 is a unit. Lemma 1 shows then that $0, 1, x_4, x_5$ is a cycle, and $N(\mathfrak{p})$ divides some element of $g(K)$. ∎

Lemma 8.

(i) *For any different primes p, q and natural $a, b > 0$ the number n of $0 \leqslant l \leqslant p^a q^b - 1$ satisfying $(p^a q^{b-1} - l, pq) = (l, pq) = 1$ is at least 3 except for $(q, b) = (2, 1)$; $(p, q, a, b) = (2, 3, 1, 1), (2, 3, 2, 1)$.*

(ii) *Let P, p, q be distinct primes, and let $a, b > 0$. Put $k = p^a q^b$. Let $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_j$ be distinct prime ideals of norm P. Assume that*

(a) *$P < k$;*

(b) *$q \nmid p^a q^{b-1} - 1$;*

(c) *if $p \nmid P - 1$, then $j \geqslant 2$;*

(d) *if $p \mid P - 1$, then $j \geqslant 3$ and $p \nmid p^{a-1} q^b - 1$.*

Then $k \in \mathcal{CYCL}(Z_K)$ implies that P^2 divides some element from $d(K)$.

Proof. (i) The assertion easily follows from a formula for n. We see that $n = (p-1)p^{a-1}(q-1)q^{b-1}$ for $b \geqslant 2$, and $n = (p-1)p^{a-1}(q-2)q^{b-1}$ for $b = 1$.

(ii) Let $0, 1, x_2, \ldots, x_{k-1}$ be a cycle in Z_K. Let $\mathfrak{p}$ be any ideal of norm P. As $P < k$, Lemma 5 implies that $x_{p^{a-1}q^b} \in \mathfrak{p}$ or $x_{p^a q^{b-1}} \in \mathfrak{p}$.

If $p \nmid P - 1$, then $x_{p^{a-1}q^b} \in \mathfrak{p}$ would imply the existence of a $*$-cycle (namely $0, x_{p^{a-1}q^b}, x_{2p^{a-1}q^b}, \ldots$) of length p in $(Z_K)_{\mathfrak{p}}$, contradicting Lemma 5(i). Thus, in this case we obtain $x_{p^a q^{b-1}} \in \mathfrak{p}$, and $P^2 \mid P^j \mid N_{K/Q}(x_{p^a q^{b-1}})$ follows.

By pidgeonhole principle, at least one of the following possibilities holds

1-st possibility: $P^2 \mid N_{K/Q}(x_{p^a q^{b-1}})$ and $q \nmid p^a q^{b-1} - 1$;

2-nd possibility: $P^2 \mid N_{K/Q}(x_{p^{a-1}q^b})$ and $p \nmid p^{a-1} q^b - 1$.

Assume the first possibility. Using (i) we obtain that there is $0 \leqslant l \leqslant p^a q^b - 1$ such that $(p^a q^{b-1} - l, pq) = (l, pq) = 1$; $l \neq 1$ and $x_{p^a q^{b-1}} - x_l \neq 1$. Now Lemma 1 implies that $(1 - x_{p^a q^{b-1}}, x_{p^a q^{b-1}} - x_l, x_l)$ is a non-trivial solution of (1). Hence $N_{K/Q}(x_{p^a q^{b-1}}) = N_{K/Q}(1 - (1 - x_{p^a q^{b-1}})) \in d(K)$.

We deal with the second possibility in the same manner. ∎

Let $0, 1, x_2, x_3, x_4, x_5$ be a cycle in Z_K. Put $z = \frac{x_4}{x_2}$ (Lemma 1 gives $z \in \mathcal{V}(K)$). Write then $x_2 = 1 - u$; $x_3 = 1 - u + v$ for some invertible u, v. In view of $x_2 \sim x_3 - 1$, there is an invertible δ such that $1 - u = \delta(-u + v)$. Hence $(\alpha, \beta, \gamma) := (u, -\delta u, \delta v)$ is a solution of (1).

Lemma 9. *Let K of signature $(0,2)$ be such that in Z_K there are exactly $k \geqslant 1$ prime ideals of norm 5. Let $0, 1, x_2, \ldots, x_5$ be a cycle in Z_K, and $z, u, \alpha, \beta, \gamma$ be as above.*

If (α, β, γ) is the trivial solution of (1), then $x_3 = 2 - u$. Otherwise,

$$\begin{aligned} 5^k \mid N_{K/Q}(-\beta + \beta\alpha + \gamma\alpha) = N_{K/Q}(z(1-\alpha) - 1), \\ N_{K/Q}(\beta(z-1)(1-\alpha) + \gamma\alpha) = 1. \end{aligned} \tag{2}$$

Moreover, x_3 belongs to all prime ideals of norm 5.

Proof. Let $\mathfrak{p}$ be any prime ideal of norm 5. By Lemma 5 we must have $x_3 \in \mathfrak{p}$.

If the mentioned solution is trivial, then one easily gets $v = 1$ or $v = u^2$. But the second possibility would give $1 - u + u^2 \equiv 0 \mod \mathfrak{p}$, which is impossible.

The condition (2) follows by a direct calculation of x_2, x_3, x_4 in terms of α, β, γ, $x_3 \sim x_4 - 1$, $x_3 \in \mathfrak{p}$ and the invertibility of $x_4 - x_3$. ∎

3. Determining all fields of signature (0, 2) which can be non-trivial

Lemma 10. *If K is a non-trivial field of signature $(0,2)$, then it is of one of the following forms.*

(i) *$Q(\zeta_8), Q(\zeta_{10}), Q(\zeta_{12})$;*
(ii) *$Q(v)$, where v is a unit such that $1 - v$ is also a unit;*
(iii) *$Q(w)$, where w is a unit such that $w - 1 \sim w + 1$ (equivalently, $0, 1, 1 + w, w$ is a cycle in Z_K);*
(iv) *$Q(\eta)$, where η is a unit satisfying $1 < |\eta| \leqslant 1 + \sqrt{2}$.*

Proof. Let d be as in Lemma 3. We may assume that $|d| > 1$. Let n be the number of roots of unity in K. Put $\zeta = \zeta_n$. If $n \in \{8, 10, 12\}$, then $K = Q(\zeta)$ and K satisfies (i). If $\sqrt{5} \in K$ or $\sqrt{2} \in K$, then $1 < |d| \leqslant \max(\frac{1+\sqrt{5}}{2}, 1 + \sqrt{2})$ and K satisfies (iv).

From this point on we assume that $\sqrt{2}, \sqrt{5} \notin K$ and $n \in \{2, 4, 6\}$. Then a sum of two or three roots of unity in K is 0 or has the absolute value greater than 1.

Suppose that (1) has a non-trivial solution (u, v, w). We may assume that $|u| \geqslant |v| \geqslant |w| \geqslant 1$. Put $u = d^{k_1}\zeta^{j_1}, v = d^{k_2}\zeta^{j_2}, w = d^{k_3}\zeta^{j_3}$, with $k_1 \geqslant k_2 \geqslant k_3 \geqslant 0$. We easily see that $k_1 > 0$.

If $k_1 = k_2 = k_3$, then $|u + v + w| = |d|^{k_1}|\zeta^{j_1} + \zeta^{j_2} + \zeta^{j_3}| > 1$, a contradiction. If $k_1 = k_2 > k_3$, then $|d|^{k_1} \leqslant |d|^{k_1}|\zeta^{j_1} + \zeta^{j_2}| = |u + v| = |1 - w| \leqslant 2|d|^{k_1 - 1}$ and $|d| \leqslant 2$ follows. If $1 = k_1 > k_2$, then $d \in Q(\zeta)$, a contradiction. In all other cases, $|d|^{k_1} \leqslant 2|d|^{k_1 - 1} + 1$ with $k_1 \geqslant 2$, and $|d| \leqslant 1 + \sqrt{2}$ follows. Hence if (1) has a non-trivial solution, then $1 < |d| \leqslant 1 + \sqrt{2}$ and K is as in (iv).

Suppose that $3 \in \mathcal{CYCL}(Z_K)$. Then in Z_K there is a cycle of the form $0, 1, v$, with (see Lemma 1) invertible $v, v - 1$. If $[Q(v) : Q] = 4$, then $K = Q(v)$ and K is as in (ii). If $[Q(v) : Q] = 2$, then $\sqrt{5} \notin K$ and Theorem B gives $\zeta_6 \in K$.

Suppose that $4 \in \mathcal{CYCL}(Z_K)$ and (1) has no non-trivial solutions. Then by Lemma 1 in Z_K there is a cycle of the form $0, 1, 1+w, w$. If $[Q(w):Q]=4$, then $K=Q(w)$ and K is as in (iii). If $[Q(w):Q]=2$, then $\sqrt{2}, \sqrt{5} \notin K$ and Theorem B gives $i=\zeta_4 \in K$.

From this point on we assume moreover that $d(K)=d_1(K)=\varnothing$, and K is not as in (i),(ii),(iii),(iv).

Lemma 1(v) and Lemma 6(ii) show then that $\mathcal{C} := \mathcal{CYCL}(Z_K) \subseteq \{1,2,3,4,6,12\}$.

As K is not trivial, we have $\mathcal{C} \neq \{1,2\}$. If $3 \in \mathcal{C}$, then $\zeta_6 \in K$ and $\mathcal{CYCL}(Z_{Q(\zeta_6)}) = \{1,2,3,6\} \subseteq \mathcal{C}$. As K is not trivial, we obtain $4 \in \mathcal{C}$. This gives $\zeta_6, \zeta_4 \in K$ and $n=12$ follows, a contradiction.

If $3 \notin \mathcal{C}$ and $4 \in \mathcal{C}$, then $i \in K$ and $\mathcal{C} = \{1,2,4\}$. Thus K is trivial. ■

Lemma 11. *Let $K=Q(v)$ be of signature $(0,2)$, where v is as in Lemma 10(ii). Then the minimal polynomial of v is of the form $F(X)=X^4+aX^3+bX^2+(-1-a-b)X+1$ and $\mathrm{Disc}(K) \in \{117, 125, 144, 189, 229, 272\}$. Moreover,*

(i) $\mathrm{Disc}(K)=117$ *for* $(a,b) \in \{(-5,8),(-4,8),(-3,2),(-3,5),(-2,2),(-1,-1),(-1,2),(0,2),(1,-1)\}$;
(ii) $\mathrm{Disc}(K)=125$ *for* $(a,b) \in \{(-3,4),(-2,4),(-1,1)\}$;
(iii) $\mathrm{Disc}(K)=144$ *for* $(a,b) \in \{(-4,5),(-2,5),(0,-1)\}$;
(iv) $\mathrm{Disc}(K)=189$ *for* $(a,b) \in \{(-5,9),(-2,0),(1,0)\}$;
(v) $\mathrm{Disc}(K)=229$ *for* $(a,b) \in \{(-4,6),(-3,3),(-3,6),(-1,0),(-1,3),(0,0)\}$;
(vi) $\mathrm{Disc}(K)=272$ *for* $(a,b) \in \{(-4,7),(-2,1),(0,1)\}$.

There are no more possibilities for (a,b).
In particular, if K is as in (i)-(vi), then there is a cycle of length 3 in Z_K.

Proof. Let $X^4+aX^3+bX^2+cX+1$ be the minimal polynomial of v (the last coefficient equals ± 1 since v is a unit, but it cannot be -1 since K is totally complex). The minimal polynomial for the unit $v-1$ is $(X+1)^4+a(X+1)^3+b(X+1)^2+c(X+1)+1$ with the constant term $1+a+b+c+1$, and $c=-1-a-b$ follows.

Because of the signature $(0,2)$, the polynomial $F(X)$ has no real roots. So in particular, $F(-1)=2b+3>0$, $16F(\frac{1}{2})=-4b-6a+9>0$ and $F(2)=6a+2b+15>0$. This gives $b \geqslant -1$ and $-2b-15<6a<-4b+9$. In view of $-2b-15<-4b+9$ we get $b \leqslant 11$. For each $-1 \leqslant b \leqslant 11$ we see that $\frac{-2b-15}{6} \leqslant a \leqslant \frac{-4b+9}{6}$. Thus we obtain quite a small number of possibilities for (a,b). For each resulting pair we use PARI to find whether $F(X)$ is irreducible and whether it has only non-real roots. PARI also computes the discriminants. The resulting calculations are listed in the lemma. ■

Lemma 12. *Let $K=Q(\eta)$ be of signature $(0,2)$, where η is as in Lemma 10(iv). Let $F(X)=X^4+aX^3+bX^2+cX+1$ be the minimal polynomial of η. Then $K=Q(\theta)$, where θ is a root of F, and (a,c,b) equals one of the following possibilities:*

(i) $(-1,-2,2)$, $\mathrm{Disc}(Q(\theta))=117$;
(ii) $(-3,-2,4)$, $\mathrm{Disc}(Q(\theta))=125$;
(iii) $(2,-2,2)$, $\mathrm{Disc}(Q(\theta))=144$;

(iv) $(1,-2,0)$, $\mathrm{Disc}(Q(\theta)) = 189$;
(v) $(1,-1,2)$, $\mathrm{Disc}(Q(\theta)) = 225$;
(vi) $(0,1,0)$, $\mathrm{Disc}(Q(\theta)) = 229$;
(vii) $(0,0,6)$, $\mathrm{Disc}(Q(\theta)) = 256$;
(viii) $(0,1,1)$, $\mathrm{Disc}(Q(\theta)) = 257$;
(ix) $(0,2,1)$, $\mathrm{Disc}(Q(\theta)) = 272$;
(x) $(2,-2,0)$, $\mathrm{Disc}(Q(\theta)) = 320$;
(xi) $(3,-3,1)$, $\mathrm{Disc}(Q(\theta)) = 333$;
(xii) $(1,-1,0)$, $\mathrm{Disc}(Q(\theta)) = 392$;
(xiii) $(0,0,3)$, $\mathrm{Disc}(Q(\theta)) = 400$;
(xiv) $(2,2,6)$, $\mathrm{Disc}(Q(\theta)) = 432$;
(xv) $(0,0,5)$, $\mathrm{Disc}(Q(\theta)) = 441$;
(xvi) $(0,4,4)$, $\mathrm{Disc}(Q(\theta)) = 512$;
(xvii) $(2,-2,5)$, $\mathrm{Disc}(Q(\theta)) = 576$.

Moreover, the fields in $(i)-(xvii)$ are chosen in such a way, that among the possible triples (a,c,b) we choose the triple for which the corresponding polynomial $F(X)$ has a root $v \in K$ with minimal value $|v| > 1$. This implies that for any chosen value of (a,c,b) any root of $F(X)$ lying in K, with absolute value bigger than 1, satisfies the conditions for d in Lemma 3.

Proof. As $1 < |\eta| \leqslant 1+\sqrt{2}$, because of the signature $(0,2)$ (in particular, two roots of $F(X)$ have the same absolute value $|\eta|$, whereas the other two have the absolute value $\frac{1}{|\eta|}$), using Vieta's formulae we obtain $|a| \leqslant 2(|\eta| + \frac{1}{|\eta|}) \leqslant 4\sqrt{2} < 6$. The similar estimate holds for $|c|$. For b we have $|b| \leqslant |\eta|^2 + \frac{1}{|\eta|^2} + 4 \leqslant 10$.

As the fields corresponding to (a,c,b) and $(-a,-c,b)$ are isomorphic and have the same absolute values of their roots, we can assume $a \geqslant 0$. For each resulting triple we use PARI to check the irreducibility of $F(X)$, and calculate the signature and the discriminant of the resulting field. Furthermore, we check that for each value (a,c,b) giving the irreducible polynomial with no real roots the resulting field is isomorphic to one from the provided list, and the root with absolute value bigger than 1 has the absolute value equal or greater than the absolute value of the corresponding root of a suitable polynomial from the list. ■

Lemma 13. *Let $K = Q(w)$ be of signature $(0,2)$, where w is as in Lemma 10(iii). Then the minimal polynomial of w is of the form $F(X) = X^4 + a(X^3 - X) + bX^2 + 1$ and $\mathrm{Disc}(K) \in \{117, 144, 225, 256, 320, 392, 441\}$. Moreover,*

(i) $\mathrm{Disc}(K) = 117$ *for* $(b,a) \in \{(-1,-1),(-1,1),(14,-4),(14,4)\}$;
(ii) $\mathrm{Disc}(K) = 144$ *for* $(b,a) \in \{(-1,0),(2,-2),(2,2),(14,0)\}$;
(iii) $\mathrm{Disc}(K) = 225$ *for* $(b,a) \in \{(2,-1),(2,1)\}$;
(iv) $\mathrm{Disc}(K) = 256$ *for* $(b,a) \in \{(0,0),(6,0)\}$;
(v) $\mathrm{Disc}(K) = 320$ *for* $(b,a) \in \{(0,-2),(0,2),(6,-4),(6,4)\}$;
(vi) $\mathrm{Disc}(K) = 392$ *for* $(b,a) \in \{(0,-1),(0,1),(6,-2),(6,2)\}$;
(vii) $\mathrm{Disc}(K) = 441$ *for* $(b,a) \in \{(2,-3),(2,3)\}$.

There are no more possibilities for (b,a).
In particular, if K is as in (i)-(vii), then there is a cycle of length 4 in Z_K.

Proof. Let $X^4+aX^3+bX^2+cX+1$ be the minimal polynomial of w. We easily see that the constant term of the minimal polynomial for $w-1$ is $2+a+b+c$, whereas the corresponding coefficient for $w+1$ is $2-a+b-c$. Since $w-1 \sim w+1$, we have $2+a+b+c = 2-a+b-c$, and $c=-a$ follows. So the minimal polynomial of w has the required form. Now we are going to specify the possible values of (b,a).

Since $F(1) > 0$, we have $b \geqslant -1$. Moreover, as $F(X) = X^2((X-\frac{1}{X})^2 + a(X-\frac{1}{X})+b+2)$ and $F(X)$ has no real roots, we get $a^2-4(b+2)<0$.

The condition $w-1 \sim w+1$ is equivalent to $w-1 \mid 2$ and $w+1 \mid 2$. Thus $\frac{2}{w-\epsilon}$ is an algebraic integer for $\epsilon = -1, 1$. The minimal polynomial for $\frac{2}{w-\epsilon}$ is $X^4+(\frac{2(4\epsilon+2b\epsilon+2a)}{2+b})X^3+(\frac{4(6+b+3a\epsilon)}{2+b})X^2+(\frac{8(a+4\epsilon)}{2+b})X+\frac{16}{2+b}$.

But $\frac{2}{w-\epsilon}$ is an algebraic integer, so all the coefficients of this polynomial are integers. We thus obtain for $\epsilon=-1,1$ that $2+b \mid 8\epsilon+4a+4b\epsilon;\ 2+b \mid 24+4b+12a\epsilon;\ 2+b \mid 8a+32\epsilon;\ 2+b \mid 16$, which is equivalent to $2+b \mid 4a$ and $2+b \mid 16$. So we get $b \in \{-1,0,2,6,14\}$.

For $b=14$ we get $a=-4,0,4$. For $b=6$ we get $a=-4,-2,0,2,4$. For $b=2$ we obtain $a=-3,-2,-1,0,1,2,3$, but for $a=0$ we obtain the reducible polynomial. For $b=0$ we obtain $a=-2,-1,0,1,2$. For $b=-1$ we get $a=-1,0,1$. The discriminants were computed by PARI. ∎

Proposition 1. *Every non-trivial field of signature* $(0,2)$ *is isomorphic to a field listed in Lemma 12.*

Proof. The discriminants of $Q(\zeta_8), Q(\zeta_{10}), Q(\zeta_{12})$ are $256, 125, 144$, respectively. Using PARI, we check that these cyclotomic fields and the fields listed in Lemmas 11 and 13 are isomorphic to suitable fields from Lemma 12. ∎

Remark. It may seem that Lemmas 11 and 13 are redundant, but they will be used later to determine all cycles of the form $0,1,v$ and $0,1,1+w,w$ in Z_K.

4. Proof of Theorem 1 (giving lengths of cycles in some fields)

In this section we will prove Theorem 1. In the following subsections we shall find the sets $\mathcal{CYCL}(Z_K)$ for all fields K listed in Lemma 12. We will use notation from that lemma, and the letter t will denote an element satisfying the conditions given in Lemma 1(x). For fixed K we shall denote $\mathcal{CYCL}(Z_K)$ by $\mathcal{C}$.

The triple (a,c,b) describes the minimal polynomial of θ, as given in Lemma 12. From two roots θ of $F(X)$ with $|\theta|>1$, we choose that with positive imaginary part, and denote it by d. Using PARI we verify whether $i, \zeta_6, \zeta_8, \zeta_{10}, \zeta_{12}, \sqrt{2}, \sqrt{5} \in K$ and, if so, we express them in terms of d. We list non-trivial solutions of (1), taking into account what was written in section 2.3 about equivalent solutions. Using lemmas 4,11 and 13, we determine the sets $\mathcal{V}(K)$ and $\mathcal{E}(K)$.

Computing d with sufficient accuracy, and using the roots of unity in K, we determine all non-trivial solutions of (1). We used PARI to find prime ideals in Z_K of some small norms.

Discriminant 257, $\mathcal{CYCL}(Z_K) = \{1,2,4\}$(Theorem 1(vii)).

Here $(a,c,b) = (0,1,1)$. PARI gives $2Z_K = \mathfrak{pq}$, with prime ideals $\mathfrak{p} \neq \mathfrak{q}$ and $N(\mathfrak{p}) = 2$. Thus $(Z_K)_{\mathfrak{p}}$ is isomorphic to Z_2. Hence by Lemma 5(v) we get $\mathcal{C} \subseteq \mathcal{CYCL}(Z_2) = \{1,2,4\}$. As $1 + d^4 - (-d) = -d^2$ is a unit and $1 + d^4 \sim 1 + d$, by Lemma 1(ix), $0, 1, 1 + d^4, -d$ is a cycle. Thus $\mathcal{C} = \{1,2,4\}$. As $i, \sqrt{2} \notin K$, we get that K is not trivial.

Discriminant 392, $\mathcal{CYCL}(Z_K) = \{1,2,4\}$(Theorem 1(ix)).

Here $(a,c,b) = (1,-1,0)$. As $N_{K/Q}(1-d) = 2$, in Z_K there is an ideal of norm 2. Then, by Lemma 5, $\mathcal{C} \subseteq \{1,2,4,8,16,\ldots\}$. Lemma 13 shows that $4 \in \mathcal{C}$. It suffices to get $8 \notin \mathcal{C}$.

By a calculation we obtain that the unique non-trivial solution of (1) is $(-d^4, -d^3, d)$, with $(4,8,2)$ as the attached triple. Thus $d_1(K) = \varnothing$, and by Lemma 6(ii), $8 \notin \mathcal{C}$. As $i, \sqrt{2} \notin K$, we are done.

Discriminant 320, $\mathcal{CYCL}(Z_K) = \{1,2,4\}$, K is trivial.

Here $(a,c,b) = (2,-2,0)$. As $N_{K/Q}(d-1) = 2$, in Z_K there is an ideal of norm 2. By Lemma 5 we then have $\mathcal{C} \subseteq \{1,2,4,8,\ldots\}$. One checks that $i \in K$. Since there is a cycle of length 4 in $Z_{Q(i)}$, to establish the triviality of K it suffices to show $8 \notin \mathcal{C}$.

It turns out that $(-d^3 i, -d^2 i, d), (d^2, -id, d)$ are the only solutions of (1), with $(10,8,2), (4,2,2)$ as the attached triples. We get $\mathcal{E}(K) = \{d, -d, \frac{1}{d}, -\frac{1}{d}, d^2 i, -d^2 i, \frac{i}{d^2}, \frac{-i}{d^2}, i, -i\}$ and $e(K) = \{2,4,8\}$. Therefore we get $g(K) = \{2,4,8\}$. A prime ideal $\mathfrak{p} = (d+2)$ has norm 5. Thus $5 \mid m(8)$, and Lemma 6(i) gives $8 \notin \mathcal{C}$.

Discriminant 400, $\mathcal{CYCL}(Z_K) = \{1,2,3,4\}$, K is trivial.

Here $(a,c,b) = (0,0,3)$. As $i = -d^3 - 2d, N_{K/Q}(1+i) = 4$, by Lemma 5, the lengths of cycles in Z_K are of the form $2^\alpha 3^\beta$. In view of $\sqrt{5} \in K$, to get $\mathcal{C} = \{1,2,3,4\}$ and the triviality of K, it suffices to prove that $9, 8, 6 \notin \mathcal{C}$. We have $\mathcal{E}(K) = \{\pm i, \pm 2 \pm \sqrt{5}, \frac{\pm 1 \pm \sqrt{5}}{2}\}$, and $e(K) = \{1,4,16\}$ follows. In Z_K, only $(u,v,w) = (d^3 i, di, di), (-d^3 i, -d^2, -d^2), (d^4, -d^3 i, di)$ are non-trivial solutions of (1), and $(16,1,1), (16,1,1), (25,16,1)$ are the attached triples. Hence we get $g(K) = \{1,4,16\}$.

There are two prime ideals $\mathfrak{p}_1 = (d-1)$ and $\mathfrak{p}_2 = (d+1)$ of norm 5. We see that $\mathfrak{p}_1 \mathfrak{p}_2 = (\sqrt{5})$. Thus $5 \mid m(8) \mid m(9)$, and Lemma 6(i) gives $8, 9 \notin \mathcal{C}$.

Suppose that $0, 1, x_2, x_3, x_4, x_5$ is a cycle, with $x_2 \notin Q(\sqrt{5})$ (see Lemma 2). As $di = -\frac{1+\sqrt{5}}{2}$, all non-trivial solutions of (1) lie in $Q(\sqrt{5})$. By $x_2 \notin Q(\sqrt{5})$ and Lemma 9, we then have that $x_2 = 1 - u, x_3 = 2 - u$ for some invertible u. Lemma 9 gives $u \equiv 2 \mod \sqrt{5}$. Write $u = i^a (di)^b$, for some integers a, b. In view of $di \equiv 2 \mod \sqrt{5}$ and $i \equiv (-1)^{j-1} 2 \mod \mathfrak{p}_j$, we get $2 \mid a$. This gives $u, x_2 \in Q(\sqrt{5})$, a contradiction.

Discriminant 432, $\mathcal{CYCL}(Z_K) = \{1,2,3,4,6\}$(Theorem 1(x)).

Here $(a,c,b) = (2,2,6)$. We see that $\zeta_6 = \frac{-1}{2}(d^3 + 2d^2 + 5d)$, and $\sqrt{2}, \sqrt{5}, i \notin K$. Since $N_{K/Q}(1 + d\zeta_6^5) = 3$, Lemma 5 gives that each $k \in \mathcal{C}$ is of the form $2^\alpha 3^\beta$. Using Lemma 1, one checks that $0, 1, 1 + d\zeta_6^5, -d\zeta_6^5$ is a cycle in Z_K of length 4. As $\zeta_6 \in K$, we get $\{1,2,3,4,6\} \subseteq \mathcal{C}$, and to have equality here we should show that $8, 9, 12 \notin \mathcal{C}$.

We see that $\mathcal{E}(K)$ is empty. The only solution of (1) is $(-d^2, -d\zeta_6^5, -d\zeta_6^5)$, with $(16,3,3)$ as the attached triple. This gives $g(K) = \{3\}$ (we have already seen that $g(K)$ is not empty).

The prime ideal $\mathfrak{q} = (d+2, 7)$ has norm 7. Thus $7 \mid m(8) \mid m(9)$, and Lemma 6(i) gives $8, 9 \notin \mathcal{C}$. Lemma 7 gives $12 \notin \mathcal{C}$.

Discriminant 272, $\mathcal{CYCL}(Z_K) = \{1,2,3,4\}$(Theorem 1(viii)).

Here $(a,c,b) = (0,2,1)$. We have $i = -d^3 + d^2 - d - 1$, and $\zeta_6, \sqrt{2}, \sqrt{5} \notin K$. Since $N_{K/Q}(1 - id^3) = 4$, each $k \in \mathcal{C}$ is of the form $2^\alpha 3^\beta$. By Lemma 11 and $i \in K$, we see that $1,2,3,4 \in \mathcal{C}$. To get the equality it suffices to prove that $8, 6, 9 \notin \mathcal{C}$.

By a direct calculation, $(-d^4, id^3, -d), (-d^3, -d, di), (id^3, -d^2 i, d^2)$ are the only solutions of (1), and $(17,4,1), (4,1,5), (4,1,5)$ are the attached triples. Thus $d_1(K) = \varnothing$, and Lemma 6(ii) shows that $8, 9 \notin \mathcal{C}$.

There are two prime ideals $\mathfrak{p}_1 = (d-1, 5)$ and $\mathfrak{p}_2 = (d-2, 5)$ of norm 5. We see that $\mathcal{V}(K) = \{-d, -di, -\frac{1}{d}, \frac{i}{d}, -id^2, \frac{i}{d^2}\} = \mathcal{A}(-d)$.

Suppose that $6 \in \mathcal{C}$. Then by Lemma 1(xi) and the last assertion, we get that in Z_K there is a cycle $0, 1, x_2, \ldots, x_5$ with $\frac{x_4}{x_2} = -d$. A direct checking using MAPLE gives that (2) from Lemma 9 does not hold for any non-trivial solution (α, β, γ) of (1). Hence Lemma 9 gives $x_3 = 2 - u$; $x_4 = -d(1-u)$. But then $u \equiv 2 \mod \mathfrak{p}_2$ and $x_4 - 1 = -d(1-u) - 1 \equiv 0 \mod \mathfrak{p}_2$ give $d - 1 \in \mathfrak{p}_2$, a contradiction.

Discriminant 441, $\mathcal{CYCL}(Z_K) = \{1,2,3,4,6\}$(Theorem 1(xi)).

Here $(a,c,b) = (0,0,5)$ and $i, \sqrt{2}, \sqrt{5} \notin K$. We see that $\zeta_6 = -\frac{1}{2}d^3 - 2d + \frac{1}{2}$. Since $N_{K/Q}(1 - \zeta_6 d) = 4$, each $k \in \mathcal{C}$ is of the form $k = 2^\alpha 3^\beta$. As $\mathcal{CYCL}(Z_{Q(\zeta_6)}) = \{1,2,3,6\}$, and $4 \in \mathcal{C}$ (Lemma 13), it suffices to prove that $9, 8, 12 \notin \mathcal{C}$.

Since $\mathcal{E}(K) = \{d\zeta_6, d\zeta_6^2, d\zeta_6^4, d\zeta_6^5, \frac{\zeta_6}{d}, \frac{\zeta_6^2}{d}, \frac{\zeta_6^4}{d}, \frac{\zeta_6^5}{d}\}$, we obtain $e(K) = \{4\}$.

By a direct calculation, we see that $(-d^2, d\zeta_6, d\zeta_6^2)$ is the only solution of (1), with $(9,4,4)$ as the attached triple. However, $1 - d\zeta_6$ is not associated to $1 - d\zeta_6^2$. Thus $g(K) = \{4\}$ and $d_1(K) = \varnothing$. Lemma 6(ii) shows that $8, 9 \notin \mathcal{C}$. We see that $(d-1)$ has norm 7. Lemma 7 then gives $12 \notin \mathcal{C}$.

Discriminant 333, $\mathcal{CYCL}(Z_K) = \{1,2,3,6\}$, K is trivial.

Here $(a,c,b) = (3,-3,1)$. We have $\zeta_6 = d^3 + 3d^2 + 2d - 1$. In $Z_{Q(\zeta_6)}$ there are cycles of lengths $1,2,3,6$. In view of $N_{K/Q}(d-1) = 3$, each $k \in \mathcal{C}$ is of the form $2^\alpha 3^\beta$. Thus, by Lemma 1, to get $\mathcal{C} = \{1,2,3,6\}$ we should show that $4, 9 \notin \mathcal{C}$.

We have $\mathcal{E}(K) = \varnothing$. The only non-trivial solution of (1) is $(d^2, d, d\zeta_6^5)$, with the attached triple $(9,3,3)$. However, $1 - d$ is not associated to $1 - d\zeta_6^5$. Thus $g(K) = \varnothing$, and $4 \notin \mathcal{C}$ follows. Lemma 6(ii) gives $9 \notin \mathcal{C}$.

Discriminant 512, $\mathcal{CYCL}(Z_K) = \{1,2,4\}$, K is trivial.

Here $(a,c,b) = (0,4,4)$. Since $N_{K/Q}(d+1) = 2$, we see that $\mathcal{C} \subseteq \{1,2,4,8,\ldots\}$. Since $i \in K$, to get the triviality of K it is sufficient to prove that $8 \notin \mathcal{C}$.

We get $\mathcal{E}(K) = \{\pm i\}$ and $e(K) = \{4\}$. The only non-trivial solution of (1) is $(-d^2 i, -d, -d)$, with $(16,2,2)$ as the attached triple. Thus $g(K) = \{2,4\}$. We see that $\mathfrak{p} = (d+2, 5)$ is the prime ideal of norm 5. Thus $5 \mid m(8)$, and Lemma 6(i) gives $8 \notin \mathcal{C}$.

Discriminant 576, $\mathcal{CYCL}(Z_K) = \{1,2,3,4,6\}$, K is trivial.

Here $(a,c,b) = (2,-2,5)$, and $\zeta_6 = \frac{1}{5}(-2d^3 - 5d^2 - 10d + 4)$, $\sqrt{2} = d\zeta_6^4 - 1$. As $N_{K/Q}(\sqrt{2}) = 4$, each $k \in \mathcal{C}$ is of the form $k = 2^\alpha 3^\beta$. In view of Theorem B, it suffices to prove that $8, 9, 12 \notin \mathcal{C}$.

We get $\mathcal{E}(K) = \{\pm 1 \pm \sqrt{2}\}$, and $e(K) = \{4\}$ follows. The only non-trivial solution of (1) is $(d^2\zeta_6^2, d\zeta_6, d\zeta_6)$, with $(16,4,4)$ as the attached triple. Thus $g(K) = \{4\}$. We see that $(d-1)$ has norm 7. Thus $7 \mid m(8) \mid m(9)$, and Lemma 6(i) gives $8, 9 \notin \mathcal{C}$. Using Lemma 7 we obtain $12 \notin \mathcal{C}$.

Discriminant 256, $\mathcal{CYCL}(Z_K) = \{1,2,4,8\}$(Theorem 1(vi)).

Here $(a,c,b) = (0,0,6)$ and $\zeta_8 = \frac{1}{4}(d^3 - d^2 + 7d - 3)$. Clearly $1, \zeta_8, \ldots, \zeta_8^7$ is a cycle of length 8 for the polynomial $f(X) = \zeta_8 X$. The ideal $(\zeta_8 + 1)$ has norm 2, and we get $\mathcal{C} \subseteq \{1,2,4,8,16,\ldots\}$. It suffices to prove that $16 \notin \mathcal{C}$.

We get $\mathcal{E}(K) = \{\pm i, \pm 1 \pm \sqrt{2}, \zeta_8, \zeta_8^3, \zeta_8^5, \zeta_8^7, d, -d, \frac{1}{d}, -\frac{1}{d}\}$ and $e(K) = \{2,4,8\}$. By a calculation, $(d\zeta_8^4, d\zeta_8^7, \zeta_8^3), (d\zeta_8^2, d\zeta_8^5, d\zeta_8^7), (d\zeta_8^7, \zeta_8^5, \zeta_8^6)$ and $(d^2\zeta_8^4, d\zeta_8^2, d\zeta_8^2)$ are the only non-trivial solutions of (1). They have $(8,2,2), (4,2,2), (2,2,4)$ and $(16,4,4)$, as the attached triples. This gives $g(K) = \{2,4,8\}$. We see that $\mathfrak{p} = (\zeta_8^2 + 2\zeta_8 + 2, 3)$ is the prime ideal of norm 9. Thus $9 \mid m(16)$, and Lemma 6(i) gives $16 \notin \mathcal{C}$.

Discriminant 225, $\mathcal{CYCL}(Z_K) = \{1,2,3,4,6\}$, K is trivial.

Here $(a,c,b) = (1,-1,2)$. We have $\zeta_6 = \frac{1}{2}(-d^3 - 2d^2 - 2d + 1)$ and $\sqrt{5} = 2d\zeta_6^4 - 1$. As $\{1,2,3,6\} \subseteq \mathcal{CYCL}(Z_{Q(\zeta_6)})$, $4 \in \mathcal{CYCL}(Z_{Q(\sqrt{5})})$ and $N_{K/Q}(1-d) = 4$, it suffices to prove that $9, 12, 8 \notin \mathcal{C}$.

We see that $(d^2\zeta_6, d^2\zeta_6^3, d\zeta_6), (d^3\zeta_6^3, d^2\zeta_6^2, d^2\zeta_6^2), (d^2\zeta_6^2, d\zeta_6^2, d), (d^2\zeta_6, d, \zeta_6), (d^4\zeta_6^4, d^3\zeta_6^3, d\zeta_6), (d^3, d\zeta_6, d\zeta_6)$ are the only non-trivial solutions of (1), with $(4,4,1), (16,1,1), (1,4,4), (4,4,1), (25,16,1), (16,1,1)$ as the attached triples. Thus $d_1(K) \subseteq \{1,4\}$. We see that $w = \pm d, \pm\frac{1}{d}, \pm d\zeta_6^2, \pm\frac{1}{d}\zeta_6$ are the only elements from $\mathcal{E}(K)$ of degree 4 over Q. For all these w we have $N_{K/Q}(1+w) = 4$. Lemma 4(ii) gives that $w = \pm 2 \pm \sqrt{5}, \frac{\pm 1 \pm \sqrt{5}}{2}$ are the only elements from $\mathcal{E}(K)$ of degree 2 over Q. Thus $g(K) = \{1,4,16\}$.

In Z_K there are two prime ideals of norm 4, namely $\mathfrak{p}_1 = (d-1)$ and $\mathfrak{p}_2 = (1 + d\zeta_6^2)$. We see that $(2) = \mathfrak{p}_1\mathfrak{p}_2$. Thus $16 \mid m(9)$, and Lemma 6(i) gives $9 \notin \mathcal{C}$.

It turns out that the assumption of Lemma 7(b) is satisfied. We see that $\mathfrak{q} = (d^2 + 2d + 2, 3)$ is the prime ideal of norm 9. Lemma 7 gives $12 \notin \mathcal{C}$.

Remark. From forms of cycles of length 4 obtained above, we see that the only cycles of the form $0, 1, x_2, x_3$ with $2 \mid x_2$, are $0, 1, 1+w, w$ with $w = \pm 2 \pm \sqrt{5}$. In particular, if $x_2 \in \mathfrak{p}_1, \mathfrak{p}_2$, then $x_2, x_3 \in Q(\sqrt{5})$.

It suffices to get $8 \notin \mathcal{C}$. Let $0, 1, x_2, \ldots, x_7$ be a cycle in Z_K. Lemma 5 implies that $x_4 \in \mathfrak{p}_1\mathfrak{p}_2 = (2)$. Lemma 1 shows that $0, 1, x_4, x_5$ and $0, 1, \frac{x_4}{x_3}, \frac{x_7}{x_3}$ are cycles satisfying $2 \mid x_4$, respectively, $2 \mid \frac{x_4}{x_3}$. The above Remark shows now that $x_4, \frac{x_4}{x_3}, \frac{x_7}{x_3} \in Q(\sqrt{5})$, and $x_7 \in Q(\sqrt{5})$ follows.

Let $y_0, y_1, \ldots, y_7$ be any cycle in Z_K with $y_0, y_1 \in Q(\sqrt{5})$. Then $0, 1, \frac{y_2 - y_0}{y_1 - y_0}, \ldots, \frac{y_7 - y_0}{y_1 - y_0}$ is a cycle (see Lemma 1(ii)), and we obtain that $\frac{y_7 - y_0}{y_1 - y_0} \in Q(\sqrt{5})$. This gives

$y_7 \in Q(\sqrt{5})$. As $y_7, y_0, y_1, \ldots, y_6$ is a cycle, we obtain in a similar manner that $y_6 \in Q(\sqrt{5})$, and so on. Finally, we would get a cycle of length 8 already in $Z_{Q(\sqrt{5})}$, which is rejected by Theorem B.

Discriminant 229, $\mathcal{CYCL}(Z_K) = \{1, 2, 3, 4\}$(Theorem 1(v)).

Here $(a, c, b) = (0, 1, 0)$ and $i, \sqrt{2}, \sqrt{5}, \zeta_6 \notin K$. Since $N_{K/Q}(d-1) = 3$, each $k \in \mathcal{C}$ is of the form $k = 2^\alpha 3^\beta$. Lemma 11 guarantees that $3 \in \mathcal{C}$, whereas, using Lemma 1(ix), we see that $0, 1, 1-d^7, d^5$ is a cycle of length 4. In order to receive $\mathcal{C} = \{1, 2, 3, 4\}$, we therefore should get $8, 9, 6 \notin \mathcal{C}$.

By a direct calculation, we see that $(d^7, -d^6, d^5), (d^5, -d^4, d^2), (d^8, d^5, -d)$ and $(d^7, d^3, -d)$ are the only non-trivial solutions of (1), with $(3, 5, 3), (3, 1, 3), (15, 3, 1)$ and $(3, 9, 1)$ as the attached triples. This gives $d_1(K) = \{3\}$. We get $e(K) = \varnothing$, and $g(K) = \{3\}$ follows. Lemma 11(v) gives $\mathcal{V}(K) = \mathcal{A}(-d)$.

The prime ideal $\mathfrak{q}_1 = (d+2, 5)$ has norm 5. Thus $5 \mid m(8) \mid m(9)$, and Lemma 6(i) gives $8, 9 \notin \mathcal{C}$. It suffices to prove the same for 6.

Let $0, 1, x_2, \ldots, x_5$ be a cycle in Z_K of length 6. Using Lemma 1(xi), we may assume that $\frac{x_4}{x_2} = -d$. If (x_2, x_3, x_4) leads to the trivial solution of (1), as explained before Lemma 9, then $x_2 = 1-u, x_3 = 2-u, x_4 = -d(1-u)$. This leads to $2-u \in \mathfrak{q}_1, -d(1-u)-1 \in \mathfrak{q}_1$ and $d-1 \in \mathfrak{q}_1$, a clear contradiction.

We see that the possibilities for (x_2, x_3, x_4) that lead to the non-trivial solution of (1) from Lemma 9 and satisfy (2) are $(1-d, 1-d+\frac{1}{d}, -d(1-d)), (1-d, 1-d+d^3, -d(1-d))$. Hence $x_2 = 1-d$ and $x_4 = -d(1-d)$. As $x_4 - x_5 = -d(1-d) - x_5$ is invertible, taking into account all non-trivial solutions of (1), we obtain that $x_5 \in \{\frac{1}{d^5}, -\frac{1}{d^4}, \frac{1}{d^3}, -\frac{1}{d}, -1, -d, d^2, d^3\}$. But for cycles of length 6 we have $x_5 - 1 \sim x_2 = 1-d$, and $N_{K/Q}(x_5 - 1) = 3$ follows. Hence $x_5 \in \{\frac{1}{d^5}, d^2\}$. But $x_5 - x_2 \in \mathfrak{q}_1$, and no possibility for x_5 remains.

Discriminant 125, $\mathcal{CYCL}(Z_K) = \{1, 2, 3, 4, 5, 6, 8, 10\}$(Theorem 1(ii)).

Here $(a, c, b) = (-3, -2, 4)$. We see that $\zeta_{10} = -d^3 + 3d^2 - 3d + 1$. We obtain that the prime ideal $\mathfrak{p} = (d+3, 5)$ has norm 5, and $(11) = \mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3\mathfrak{q}_4$, with different prime ideals $\mathfrak{q}_1, \mathfrak{q}_2, \mathfrak{q}_3, \mathfrak{q}_4$ of norm 11.

By Lemma 5 (considering $\mathfrak{p}$) we get that the length of any cycle in Z_K is of one of the following forms: $5^\alpha, 2 \cdot 5^\alpha, 3 \cdot 5^\alpha, 4 \cdot 5^\alpha, 6 \cdot 5^\alpha, 8 \cdot 5^\alpha, 12 \cdot 5^\alpha, 16 \cdot 5^\alpha$.

As $1, \zeta_{10}, \zeta_{10}^2, \ldots, \zeta_{10}^9$ is a cycle for the polynomial $f(X) = \zeta_{10} X$, using Lemma 1, we get $\{1, 2, 3, 4, 5, 10\} \subseteq \mathcal{C}$.

Let $a_1 = 0, a_2 = 1, a_3 = \zeta_{10}^3, a_4 = d\zeta_{10}^7, b_1 = \zeta_{10}^3(1 - d^2\zeta_{10}^7), b_2 = \zeta_{10}^6, b_3 = \zeta_{10}^7, b_4 = \frac{\zeta_{10}^6}{d}$. Such a_i, b_j satisfy the conditions from Lemma 1(viii), so $6, 8 \in \mathcal{C}$. Thus $\{1, 2, 3, 4, 5, 6, 8, 10\} \subseteq \mathcal{C}$, and to get the equality we should show that $25, 16, 15, 12, 20 \notin \mathcal{C}$.

There are 23 non-trivial solutions of (1), with $(1, 1, 1), (5, 1, 1), (5, 5, 1), (11, 1, 1), (11, 5, 1), (11, 11, 1), (16, 1, 1), (25, 16, 1)$ as the attached triples. Thus $d(K) = \{1, 5, 11, 16, 25\}$. Since $\mathcal{E}(K) = \{\pm 2 \pm \sqrt{5}, \frac{\pm 1 \pm \sqrt{5}}{2}\}$ and $e(K) = \{1, 16\}$, we get $g(K) \subseteq \{1, 5, 11, 16\}$.

We see that $11^4 \mid m(16) \mid m(25)$, and Lemma 6(i) gives $16, 25 \notin \mathcal{C}$. We apply Lemma 8(ii) for $P = 11, j = 4$ and for $(k, p) = (15, 3), (12, 3), (20, 5)$. We then obtain $15, 12, 20 \notin \mathcal{C}$, respectively.

Discriminant 117, $\mathcal{CYCL}(Z_K) = \{1,2,3,4,5,6\}$(Theorem 1(i)).

Here $(a,c,b) = (-1,-2,2), \zeta_6 = -d^3 - d - 1$, and $\mathfrak{q} = (1+d^4)$ is the prime ideal of norm 9.

We have $\mathcal{E}(K) = \{d^5\zeta_6^2, d^5\zeta_6^5, d\zeta_6, d\zeta_6^4, \zeta_6^2\frac{1}{d}, \zeta_6^5\frac{1}{d}, \zeta_6\frac{1}{d^5}, \zeta_6^4\frac{1}{d^5}\}$, and $e(K) = \{1,16\}$, follows.

There are 27 non-trivial solutions of (1), with $(1,1,1), (7,1,1), (7,7,1), (9,1,1), (9,7,1), (13,1,1), (13,9,1), (16,1,1), (16,13,1), (19,7,1)$ as the attached triples. Thus $d_1(K) \subseteq \{1,7\}$ and $g(K) \subseteq \{1,7,16\}$.

We see that in Z_K there are two ideals of norm 7, namely $\mathfrak{p}_1 = (d+1,7)$ and $\mathfrak{p}_2 = (d+3,7)$.

As the difference of any two different elements in $\{0,1,\zeta_6,d,d\zeta_6,d^3\zeta_6^2\}$ is invertible, using the Vandermonde determinant, we get that any tuple of different elements lying in this set is a cycle in Z_K. Thus $1,2,3,4,5,6 \in \mathcal{C}$. By Lemmas 1 and 5 to get $\mathcal{C} = \{1,2,3,4,5,6\}$ it suffices to prove that $7,8,9,15,10,12 \notin \mathcal{C}$.

Let $0,1,x_2,\ldots,x_6$ be a cycle of length 7 in Z_K. By Lemma 1, we see that the differences of any two different elements in the set $\{0,1,x_2,\ldots,x_6\}$ are invertible. These elements in any order give a cycle of length 7 in Z_K. If u is invertible then $0,u,ux_2,\ldots,ux_6$ is a cycle in Z_K. We may thus assume that the absolute values of $x_2,\ldots,x_6$ are at least 1.

Note that $\zeta_6,\zeta_6^5,d,d\zeta_6,d\zeta_6^4,d\zeta_6^5,d^2\zeta_6,d^2\zeta_6^2,d^2\zeta_6^3,d^3\zeta_6,d^3\zeta_6^2$ are the only elements of $\mathcal{V}(K)$ with absolute value at least 1. A direct check shows that we cannot choose five elements out of them with the property that any two chosen elements have the invertible difference. This shows that $7 \notin \mathcal{C}$.

We see that $49 \mid m(8) \mid m(9)$, and Lemma 6(i) gives $8,9 \notin \mathcal{C}$. We apply Lemma 8(ii) with $P = 7, j = 2$ and $(k,p) = (15,5)$, and obtain $15 \notin \mathcal{C}$. The asumption (b) of Lemma 7 is satisfied, and considering $\mathfrak{q}$ we get $12 \notin \mathcal{C}$. We are left with 10.

Let $0,1,x_2,\ldots,x_9$ be a cycle. Lemma 1 shows that $0,1,x_2,x_3$ and $0,1,x_2,x_9$ are cycles in Z_K, at least one of them is not of the form $0,1,1+w,w$. By considerations in sect. 2.3, we then obtain that $N_{K/Q}(x_2) \in d_1(K) \subseteq \{1,7\}$. By Lemma 5(i), we have that x_2 is not in $\mathfrak{p}_1$ nor in $\mathfrak{p}_2$, and $7 \nmid N_{K/Q}(x_2)$ follows. This implies that x_2 (and then, by Lemma 1, also x_4,x_6,x_8) is invertible. Hence by Lemma 5, x_5 lies in $\mathfrak{p}_1$ and in $\mathfrak{p}_2$. In particular $49 \mid N_{K/Q}(x_5)$.

Applying Lemma 1, we see that $(1-x_5, x_5-x_7, x_7)$ and $(1-x_5, x_5-x_9, x_9)$ are solutions of (1), and at least one of them is not trivial. This gives that $N_{K/Q}(x_5) = N_{K/Q}(1-(1-x_5))$ belongs to $d(K)$. However, no element of $d(K)$ is divisible by 49, and $10 \notin \mathcal{C}$ follows.

Discriminant 189, $\mathcal{CYCL}(Z_K) = \{1,2,3,4,6\}$(Theorem 1(iv)).

Here $(a,c,b) = (1,-2,0)$, $\zeta_6 = -d^3 - 2d^2 - d + 2$ and $\sqrt{2}, \sqrt{5}, i \notin K$. We have $(3) = \mathfrak{p}^4$ with the prime ideal $\mathfrak{p} = (d+1)$ of norm 3, and $\mathfrak{q} = (d+5,7)$ has norm 7. By Lemma 5, each $k \in \mathcal{C}$ is of the form $k = 2^\alpha 3^\beta$.

We see that $(d^2, d^2\zeta_6^2, d)$, $(d^2\zeta_6, d\zeta_6, d\zeta_6^5)$, $(d^3\zeta_6, d^2\zeta_6, d^2)$, $(d^3, d^2, d\zeta_6)$, $(d^2, d\zeta_6^5, \zeta_6)$, $(d^4\zeta_6^2, d^3\zeta_6, d)$, $(d^3\zeta_6^5, d, d\zeta_6)$ are the only non-trivial solutions of (1), with $(3,3,1), (1,3,3), (9,1,3), (7,3,3), (3,3,1), (21,9,1), (9,1,3)$ as the attached

triples. As $(3,3,1)$ appears among the associated triples, we get $4 \in \mathcal{C}$. We see that $e(K) = \varnothing$, and $d_1(K) = g(K) = \{3\}$ follows.

As $\zeta_6 \in K$, we see that $1,2,3,6 \in \mathcal{C}$. So to get $\mathcal{C} = \{1,2,3,4,6\}$, it suffices to prove that $8,9,12 \notin \mathcal{C}$.

We have $7 \mid m(8) \mid m(9)$, and Lemma 6(i) gives $8,9 \notin \mathcal{C}$. Lemma 7 gives $12 \notin \mathcal{C}$.

Discriminant 144, $\mathcal{CYCL}(Z_K) = \{1,2,3,4,6,8,12\}$(Theorem 1(iii)).

Here $(a,c,b) = (2,-2,2)$. We check that $\zeta_{12} = -\frac{1}{2}d^2 - d - \frac{1}{2}$. We have that $\mathfrak{p} = (d-1)$ is the prime ideal of norm 4, and $(13) = \mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3\mathfrak{q}_4$ with distinct prime ideals $\mathfrak{q}_1, \mathfrak{q}_2, \mathfrak{q}_3, \mathfrak{q}_4$ of norm 13. Thus each $k \in \mathcal{C}$ is of the form $k = 2^\alpha 3^\beta$. We have $\mathcal{V}(K) = \{d\zeta_{12}^5, d\zeta_{12}^7, d\zeta_{12}^8, d\zeta_{12}^{10}, \zeta_{12}, \zeta_{12}^2, \zeta_{12}^5, \zeta_{12}^7, \zeta_{12}^{10}, \zeta_{12}^{11}, \frac{\zeta_{12}^2}{d}, \frac{\zeta_{12}^4}{d}, \frac{\zeta_{12}^5}{d}, \frac{\zeta_{12}^7}{d}\}$.

Since $\zeta_{12} \in K$, we have $12 \in \mathcal{C}$, and $\{1,2,3,4,6,12\} \subseteq \mathcal{C}$ follows. One checks that $a_1 = 0, a_2 = d, a_3 = d\zeta_{12}, a_4 = \zeta_{12}^5, b_1 = (d+1)d\zeta_{12}^8, b_2 = d\zeta_{12}^3, b_3 = d\zeta_{12}^{10}, b_4 = d^2\zeta_{12}^8$ satisfy the assumptions of Lemma 1(viii), and therefore $8 \in \mathcal{C}$. Hence to get $\mathcal{C} = \{1,2,3,4,6,8,12\}$, it suffices to prove that $16,24,9 \notin \mathcal{C}$.

The full list of non-trivial solutions of (1) consists of 16 items. We do not enlist them, but we will focus on the attached triples. They are as follows: $(4,1,1), (4,4,4), (9,4,1), (13,4,1), (16,1,1), (16,9,1)$.

We have $\mathcal{E}(K) = \{\zeta_{12}, \zeta_{12}^5, \zeta_{12}^7, \zeta_{12}^{11}, \pm d, \pm di, \pm\frac{1}{d}, \pm\frac{i}{d}, \pm d^2, \pm\frac{1}{d^2}, \pm i\}$ (where clearly $i = \zeta_{12}^3$) and $e(K) = \{1,4,16\}$. Hence $g(K) = \{1,4,16\}$. As $13 \mid m(16)$, Lemma 6(i) gives $16 \notin \mathcal{C}$. Applying Lemma 8(ii) with $P = 13, j = 4$ and $(k,p) = (24,3)$, we obtain $24 \notin \mathcal{C}$. We are left with 9.

Let $0, 1, x_2, \ldots, x_8$ be a cycle of length 9 in Z_K for $f(X)$. Take any $j \in \{3,6\}$. Lemma 5 shows that $x_j \in \mathfrak{p}$. By Lemma 1, we have that $0,1,x_j,x_4$ and $0,1,x_j,x_7$ are cycles in Z_K. Let $j_1 \in \{4,7\}$ be such that $0,1,x_j,x_{j_1}$ is not of the form $0,1,1+w,w$. Since $x_j, 1-x_{j_1} \in \mathfrak{p}$ we have that $(1-x_j, x_j - x_{j_1}, x_{j_1})$ is the non-trivial solution of (1), with at least two elements divisible by 4 in the attached triple. Hence this attached triple is $(4,4,4)$. Only (d^2i, di, d) is a solution of (1) with $(4,4,4)$ as the attached triple. This solution has three equivalent ones, namely $(\frac{1}{d}, -i, -di), (-\frac{i}{d}, i, -d)$ and $(-\frac{i}{d^2}, -\frac{1}{d}, \frac{i}{d})$ (other equivalent solutions arise by changing the order of terms). So $1-x_3,\ 1-x_6 \in \{d^2i, \pm di, \pm d, \pm\frac{1}{d}, \pm i, \pm\frac{i}{d}, -\frac{i}{d^2}\}$ $:= \mathcal{A}_1$, i.e. in $\mathcal{A}_1$ we gather the units appearing in these four solutions.

Remark. Let L be a Galois extension of Q, and σ be any automorphism of L. Assume that $y_0, y_1, \ldots, y_{k-1}$ is a cycle in Z_L for $g(X)$. Then $\sigma(y_0), \sigma(y_1), \ldots, \sigma(y_{k-1})$ is also a cycle in Z_L (for $(\sigma g)(X)$).

In $\mathcal{A}_1$ some numbers are conjugated. Namely $d, di, \frac{i}{d}, -\frac{1}{d}$ are conjugated. Analogously, the numbers $-di, -\frac{i}{d}, \frac{1}{d}$ are conjugated to $-d$. The numbers $d^2i = 2+\sqrt{3}$ and $-i$ are conjugated to $\frac{-i}{d^2} = 2-\sqrt{3}$ and to i, respectively.

Suppose that $1-x_3 \in \{d, di, \frac{i}{d}, -\frac{1}{d}\}$. We may take $1-x_3 = d$. As $x_6 - x_3 \sim x_3$ we have $N_{K/Q}(x_6 - x_3) = 4$. Since $1 - x_6 \in \mathcal{A}_1$, by a simple check we then get $1 - x_6 \in \{di, -di, i, -i, -\frac{i}{d}, d^2i\} := \mathcal{A}_2$.

Now we look at x_2, x_5, x_8. By Lemma 1, they lie in $\mathcal{V}(K)$. Moreover, $x_2 - x_3, x_5 - x_3, x_8 - x_3$ are also units. This gives that x_2, x_5, x_8 are in $\{d\zeta_{12}^5, d\zeta_{12}^7, d\zeta_{12}^8, d\zeta_{12}^{10}, \zeta_{12}^5, \zeta_{12}^{10}\} := \mathcal{A}_3$.

In view of $x_5-x_2 \sim x_8-x_2 \sim x_8-x_5 \sim x_3$, we get $x_2 \equiv x_5 \equiv x_8 \mod \mathfrak{p}$. This leads to $\{x_2,x_5,x_8\} = \{d\zeta_{12}^7, d\zeta_{12}^{10}, \zeta_{12}^{10}\} := \mathcal{A}_4$ or $\{x_2,x_5,x_8\} = \{d\zeta_{12}^8, d\zeta_{12}^5, \zeta_{12}^5\} := \mathcal{A}_5$.

By Lemma 1 the numbers $x_2-x_6, x_5-x_6, x_8-x_6$ are units. So for each $v \in \mathcal{A}_4$ we have that $v-x_6$ is a unit, or for each $v \in \mathcal{A}_5$ we have that $v-x_6$ is a unit. However, it turns out that no x_6 fulfilling $1-x_6 \in \mathcal{A}_2$ satisfies at least one of these two conditions. Thus $1-x_3 \in \{d, di, \frac{i}{d}, -\frac{1}{d}\}$ is impossible.

Suppose that $1-x_3 \in \{-d, -di, -\frac{i}{d}, \frac{1}{d}\}$. We may assume $1-x_3 = -d$. In a similar way as above we get $1-x_6 \in \{di, -di, i, -i, \frac{i}{d}, d^2 i\} := \mathcal{A}_2'$. We also get that x_2, x_5, x_8 are in $\{d\zeta_{12}^{10}, \zeta_{12}^2, \zeta_{12}^5, \zeta_{12}^7, \frac{\zeta_{12}^2}{d}, \frac{\zeta_{12}^7}{d}\} := \mathcal{A}_3'$, and $\{x_2,x_5,x_8\} = \{d\zeta_{12}^{10}, \zeta_{12}^7, \frac{\zeta_{12}^7}{d}\} := \mathcal{A}_4'$ or $\{x_2,x_5,x_8\} = \{\zeta_{12}^5, \zeta_{12}^2, \frac{\zeta_{12}^2}{d}\} := \mathcal{A}_5'$ follows. In a similar way as above a contradiction follows.

Suppose that $1-x_3 \in \{d^2 i, \frac{-i}{d^2}\}$. We may assume that $1-x_3 = d^2 i$. In a similar way as above, we get that x_2, x_5, x_8 lie in $\{d\zeta_{12}^5, d\zeta_{12}^{10}, \zeta_{12}^5, \zeta_{12}^7\} := \mathcal{A}_3''$. We see that one cannot find three elements in $\mathcal{A}_3''$ congruent to each other $\mod \mathfrak{p}$, a contradiction. So, we get $1-x_3 \in \{i, -i\}$, and $x_3 \in \{1 \pm i\}$ follows.

Therefore for any cycle in Z_K of the form $0, y_1, \ldots, y_8$ we have $\frac{y_3}{y_1} \in \{1 \pm i\}$.

By Remark, we may assume that $x_3 = 1+i$. Take any $l \in \{4,7\}$. We see that $3l \equiv 3 \pmod 9$. Then $0, x_l, x_{2l}, \ldots$ is a cycle for $f^{\circ l}$ of length 9. We thus have $(1+i)/x_l = (x_{3l \pmod 9})/x_l \in \{1 \pm i\}$. This gives $x_4, x_7 \in \{1, i\}$. But $x_4, x_7 \neq x_1 = 1$ and $x_4 \neq x_7$, a contradiction. In this way we obtained $9 \notin \mathcal{C}$.

As, according to Proposition 1, it was the last field to be considered, we proved Theorem 1.

Acknowledgements. The author thanks the referee for recommending various improvements in exposition. The computations needed in the proof of our results, in particular the calculation of roots, discriminants and indices have been performed with the use of GP/PARI CALCULATOR, Version 1.38(i386 version), Copyright 1989,1993 by C. Batut, D. Bernardi, H. Cohen and M. Olivier.

References

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

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

[3] W. Narkiewicz, *Polynomial cycles in cubic fields of negative discriminant*, Funct. Approx. Comment. Math. **35** (2006), no 1, 261–269.

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

Address: Tadeusz Pezda: Department of Mathematics, University of Wrocław, plac Grunwaldzki 2/4, 50–384 Wrocław, Poland.

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

Received: 14 Janurary 2013; **revised:** 10 June 2013