Journal of Algebra 394 (2013) 92–119

Contents lists available at SciVerse ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

Constants of cyclotomic derivations

Jean Moulin Ollagnier [a], Andrzej Nowicki [b,*]

[a] Laboratoire LIX, École Polytechnique, F 91128 Palaiseau Cedex, France
[b] Nicolaus Copernicus University, Faculty of Mathematics and Computer Science, ul. Chopina 12/18, 87-100 Toruń, Poland

ARTICLE INFO

Article history:
Received 25 January 2013
Available online 3 August 2013
Communicated by Kazuhiko Kurano

MSC:
primary 12H05
secondary 13N15

Keywords:
Derivation
Cyclotomic polynomial
Darboux polynomial
Euler totient function
Euler derivation
Factorisable derivation
Jouanolou derivation
Lotka–Volterra derivation

ABSTRACT

Let $k[X] = k[x_0, \dots, x_{n-1}]$ and $k[Y] = k[y_0, \dots, y_{n-1}]$ be the polynomial rings in $n \geqslant 3$ variables over a field k of characteristic zero containing the n-th roots of unity. Let d be the cyclotomic derivation of $k[X]$, and let Δ be the factorisable derivation of $k[Y]$ associated with d, that is, $d(x_j) = x_{j+1}$ and $\Delta(y_j) = y_j(y_{j+1} - y_j)$ for all $j \in \mathbb{Z}_n$. We describe polynomial constants and rational constants of these derivations. We prove, among others, that the field of constants of d is a field of rational functions over k in $n - \varphi(n)$ variables, and that the ring of constants of d is a polynomial ring if and only if n is a power of a prime. Moreover, we show that the ring of constants of Δ is always equal to $k[v]$, where v is the product $y_0 \cdots y_{n-1}$, and we describe the field of constants of Δ in two cases: when n is power of a prime, and when $n = pq$.

Introduction

Throughout this paper $n \geqslant 3$ is an integer, k is a field of characteristic zero containing the n-th roots of unity. We denote by $\mathbb{Z}_n$ the ring $\mathbb{Z}/n\mathbb{Z}$ and consider the two polynomial rings $k[X] = k[x_0, \dots, x_{n-1}]$ and $k[Y] = k[y_0, \dots, y_{n-1}]$ over k in n variables; the indexes of the variables $x_0, \dots, x_{n-1}$ and $y_0, \dots, y_{n-1}$ are elements of $\mathbb{Z}_n$.

We denote by $k(X) = k(x_0, \dots, x_{n-1})$ and $k(Y) = k(y_0, \dots, y_{n-1})$ the fields of quotients of $k[X]$ and $k[Y]$, respectively.

We then call *cyclotomic derivations* the following two derivations d and Δ:

i) d is the derivation of $k[X]$ defined by $d(x_j) = x_{j+1}$, for $j \in \mathbb{Z}_n$,

ii) Δ is the derivation of $k[Y]$ defined by $\Delta(y_j) = y_j(y_{j+1} - y_j)$, for $j \in \mathbb{Z}_n$.

* Corresponding author.
E-mail addresses: Jean.Moulin-Ollagnier@polytechnique.edu (J. Moulin Ollagnier), anow@mat.uni.torun.pl (A. Nowicki).

0021-8693/$ – see front matter
http://dx.doi.org/10.1016/j.jalgebra.2013.07.003

We denote also by d and Δ the unique extension of d to $k(X)$ and the unique extension of Δ to $k(Y)$, respectively. We will show that there are some important relations between d and Δ. In this paper we study polynomial and rational constants of these derivations.

In general, if δ is a derivation of a commutative k-algebra A, then we denote by A^{δ} the k-algebra of constants of δ, that is, $A^{\delta} = \{a \in A;\ \delta(a) = 0\}$. For a given derivation δ of $k[X]$, we are interested in some descriptions of $k[X]^{\delta}$ and $k(X)^{\delta}$. However, we know that such descriptions are usually difficult to obtain. Rings and fields of constants appear in various classical problems; for details we refer to [5,6,26,24]. The mentioned problems are already difficult for factorisable derivations. We say that a derivation $\delta : k[X] \to k[X]$ is *factorisable* if

$$\delta(x_i) = x_i \sum_{j=0}^{n-1} a_{ij} x_j$$

for all $i \in \mathbb{Z}_n$, where each a_{ij} belongs to k. Such factorisable derivations and factorisable systems of ordinary differential equations were intensively studied from a long time; see for example [8,7,22,25]. Our derivation Δ is factorisable, and the derivation d is *monomial*, that is, all the polynomials $d(x_0), \dots, d(x_{n-1})$ are monomials. With any given monomial derivation δ of $k[X]$ we may associate, using a special procedure, the unique factorisable derivation D of $k[Y]$ (see [16,27,21], for details), and then, very often, the problem of descriptions of $k[X]^{\delta}$ or $k(X)^{\delta}$ reduces to the same problem for the factorisable derivation D.

Consider a derivation δ of $k[X]$ given by $\delta(x_j) = x_{j+1}^s$ for $j \in \mathbb{Z}_n$, where s is an integer. Such δ is called a Jouanolou derivation [10,22,16,33]. The factorisable derivation D, associated with this δ, is a derivation of $k[Y]$ defined by $D(y_j) = y_j(sy_{j+1} - y_j)$, for $j \in \mathbb{Z}_n$. We proved in [16] that if $s \geqslant 2$ and $n \geqslant 3$ is prime, then the field of constants of δ is trivial, that is, $k(X)^{\delta} = k$. In 2003 H. Żołądek [33] proved that for $s \geqslant 2$, it is also true for arbitrary $n \geqslant 3$; without the assumption that n is prime. The central role, in his and our proofs, is played by some extra properties of the associated derivation D. Indeed, for $s \geqslant 2$, the differential field $(k(X), d)$ is a finite algebraic extension of $(k(Y), \delta)$.

Our cyclotomic derivation d is the Jouanolou derivation with $s = 1$, and the cyclotomic derivation Δ is the factorisable derivation of $k[Y]$ associated with d. In this case $s = 1$, the differential field $(k(X), d)$ is no longer a finite algebraic extension of $(k(Y), \delta)$; the relations between d and Δ are thus more complicated.

We present some algebraic descriptions of the domains $k[X]^d$, $k[Y]^{\Delta}$, and the fields $k(X)^d$, $k(Y)^{\Delta}$. Note that these rings are nontrivial. The cyclic determinant

$$w = \begin{vmatrix} x_0 & x_1 & \cdots & x_{n-1} \\ x_{n-1} & x_0 & \cdots & x_{n-2} \\ \vdots & \vdots & & \vdots \\ x_1 & x_2 & \cdots & x_0 \end{vmatrix}$$

is a polynomial belonging to $k[X]^d$, and the product $y_0 y_1 \cdots y_{n-1}$ belongs to $k[Y]^{\Delta}$. In this paper we prove, among others, that $k(X)^d$ is a field of rational functions over k in $n - \varphi(n)$ variables, where φ is the Euler totient function (Theorem 2.9), and that $k[X]^d$ is a polynomial ring over k if and only if n is a power of a prime (Theorem 3.7). The field $k(X)^d$ is in fact the field of quotients of $k[X]^d$ (Proposition 2.5). We denote by $\xi(n)$ the sum $\sum_{p|n} \frac{n}{p}$, where p runs through all prime divisors of n, and we prove that the number of a minimal set of generators of $k[X]^d$ is equal to $\xi(n)$ if and only if n has at most two prime divisors (Corollary 3.13). In particular, if $n = p^i q^j$, where $p \neq q$ are primes and i, j are positive integers, then the minimal number of generators of $k[X]^d$ is equal to $\xi(n) = p^{i-1} q^{j-1}(p + q)$ (Corollary 3.11).

The ring of constants $k[Y]^{\Delta}$ is always equal to $k[v]$, where $v = y_0 y_1, \dots, y_{n-1}$ (Theorem 4.2) and, if n is prime, then $k(Y)^{\Delta} = k(v)$ (Theorem 5.6). If $n = p^s$, where p is prime and $s \geqslant 2$, then

$k(Y)^{\Delta} = k(v, f_1, \dots, f_{m-1})$ with $m = p^{s-1}$, where $f_1, \dots, f_{m-1} \in k(Y)$ are homogeneous rational functions such that $v, f_1, \dots, f_{m-1}$ are algebraically independent over k (Theorem 7.1). A similar theorem we prove for $n = pq$ (Theorem 7.5).

In our proofs we use classical properties of cyclotomic polynomials, and some results ([11,12,31,32] and others) play an important role on vanishing sums of roots of unity.

1. Notations and preparatory facts

Recall that $\mathbb{Z}_n$ is the ring $\mathbb{Z}/n\mathbb{Z}$ and that the indexes of the variables $x_0, \dots, x_{n-1}$ and $y_0, \dots, y_{n-1}$ of the polynomial rings $k[X]$ and $k[Y]$, that we are interested in, are elements of $\mathbb{Z}_n$. This means in particular that, if i, j are integers, then $x_i = x_j \iff i \equiv j \pmod{n}$. Throughout this paper ε is a primitive n-th root of unity, and we assume that $\varepsilon \in k$, where the field k has characteristic 0.

We fix the notations d and Δ for the derivations of the polynomial rings $k[X] = k[x_0, \dots, x_{n-1}]$ and $k[Y] = k[y_0, \dots, y_{n-1}]$, respectively, defined by

$$d(x_j) = x_{j+1}, \qquad \Delta(y_j) = y_j(y_{j+1} - y_j) \quad \text{for } j \in \mathbb{Z}_n.$$

We denote also by d and Δ the unique extension of d to $k(X) = k(x_0, \dots, x_{n-1})$ and the unique extension of Δ to $k(Y) = k(y_0, \dots, y_{n-1})$, respectively.

The letters ϱ and τ we book for two k-automorphisms of the field $k(X)$, defined by

$$\varrho(x_j) = x_{j+1}, \qquad \tau(x_j) = \varepsilon^j x_j \quad \text{for all } j \in \mathbb{Z}_n.$$

We denote by $u_0, u_1, \dots, u_{n-1}$ the linear forms in $k[X]$, defined by

$$u_j = \sum_{i=0}^{n-1} (\varepsilon^j)^i x_i, \quad \text{for } j \in \mathbb{Z}_n.$$

If r is an integer and $n \nmid r$, then the sum $\sum_{j=0}^{n-1} (\varepsilon^r)^j$ is equal to 0, and in the other case, when $n \mid r$, this sum is equal to n. As a consequence of this fact, we obtain that

$$x_i = \frac{1}{n} \sum_{j=0}^{n-1} (\varepsilon^{-i})^j u_j \quad \text{for all } i \in \mathbb{Z}_n.$$

Thus, $k[X] = k[u_0, \dots, u_{n-1}]$, $k(X) = k(u_0, \dots, u_{n-1})$, and the forms $u_0, \dots, u_{n-1}$ are algebraically independent over k. Moreover, we have the following equalities.

Lemma 1.1. *$\tau(u_j) = u_{j+1}$, $\varrho(u_j) = \varepsilon^{-j} u_j$ for all $j \in \mathbb{Z}_n$.*

Proof.

$$\tau(u_j) = \tau\left(\sum_{i=0}^{n-1} (\varepsilon^j)^i x_i\right) = \sum_{i=0}^{n-1} (\varepsilon^j)^i \varepsilon^i x_i = \sum_{i=1}^{n} (\varepsilon^{j+1})^i x_i = u_{j+1},$$

$$\varrho(u_j) = \varrho\left(\sum_{i=0}^{n-1} (\varepsilon^j)^i x_i\right) = \sum_{i=0}^{n-1} (\varepsilon^j)^i x_{i+1} = \sum_{i=1}^{n} (\varepsilon^j)^{i-1} x_i$$

$$= \varepsilon^{-j} \sum_{i=1}^{n} (\varepsilon^j)^i x_i = \varepsilon^{-j} \sum_{i=0}^{n-1} (\varepsilon^j)^i x_i = \varepsilon^{-j} u_j. \qquad \square$$

For every sequence $\alpha = (\alpha_0, \alpha_1, \dots, \alpha_{n-1})$ of integers, we denote by $H_\alpha(t)$ the polynomial in $\mathbb{Z}[t]$ defined by

$$H_\alpha(t) = \alpha_0 + \alpha_1 t^1 + \alpha_2 t^2 + \cdots + \alpha_{n-1} t^{n-1}.$$

Two subsets of $\mathbb{Z}^n$ which we denote by $\mathcal{G}_n$ and $\mathcal{M}_n$ play an important role in our paper. The first subset $\mathcal{G}_n$ is the set of all sequences $\alpha = (\alpha_0, \dots, \alpha_{n-1}) \in \mathbb{Z}^n$ such that $\alpha_0 + \alpha_1\varepsilon^1 + \alpha_2\varepsilon^2 + \cdots + \alpha_{n-1}\varepsilon^{n-1} = 0$. The second subset $\mathcal{M}_n$ is the set of all such sequences $\alpha = (\alpha_0, \dots, \alpha_{n-1})$ which belong to $\mathcal{G}_n$ and the integers $\alpha_0, \dots, \alpha_{n-1}$ are nonnegative, that is, they belong to the set of natural numbers $\mathbb{N} = \{0, 1, 2, \dots\}$. Let us remember:

$$\mathcal{G}_n = \bigl\{\alpha \in \mathbb{Z}^n;\ H_\alpha(\varepsilon) = 0\bigr\}, \qquad \mathcal{M}_n = \bigl\{\alpha \in \mathbb{N}^n;\ H_\alpha(\varepsilon) = 0\bigr\} = \mathcal{G}_n \cap \mathbb{N}^n.$$

If $\alpha, \beta \in \mathcal{G}_n$, then of course $\alpha \pm \beta \in \mathcal{G}_n$, and if $\alpha, \beta \in \mathcal{M}_n$, then $\alpha + \beta \in \mathcal{M}_n$. Thus $\mathcal{G}_n$ is an abelian group, and $\mathcal{M}_n$ is an abelian monoid with zero $0 = (0, \dots, 0)$.

The primitive n-th root ε is an algebraic element over $\mathbb{Q}$, and its monic minimal polynomial is equal to the n-th cyclotomic polynomial $\Phi_n(t)$. Recall (see for example: [23,13]) that $\Phi_n(t)$ is a monic irreducible polynomial with integer coefficients of degree $\varphi(n)$, where φ is the Euler totient function. This implies the following proposition.

Proposition 1.2. *Let $\alpha \in \mathbb{Z}^n$. Then $\alpha \in \mathcal{G}_n$ if and only if there exists a polynomial $F(t) \in \mathbb{Z}[t]$ such that $H_\alpha(t) = F(t)\Phi_n(t)$.*

Put $e_0 = (1, 0, 0, \dots, 0)$, $e_1 = (0, 1, 0, \dots, 0)$, $\dots$, $e_{n-1} = (0, 0, \dots, 0, 1)$, and let $e = \sum_{i=0}^{n-1} e_i = (1, 1, \dots, 1)$. Since $\sum_{i=0}^{n-1} \varepsilon^i = 0$, the element e belongs to $\mathcal{M}_n$.

Proposition 1.3. *If $\alpha \in \mathcal{G}_n$, then there exist $\beta, \gamma \in \mathcal{M}_n$ such that $\alpha = \beta - \gamma$.*

Proof. Let $\alpha = (\alpha_0, \dots, \alpha_{n-1}) \in \mathcal{G}_n$, and let $r = \min\{\alpha_0, \dots, \alpha_{n-1}\}$. If $r \geqslant 0$, then $\alpha \in \mathcal{M}_n$ and then $\alpha = \beta - \gamma$, where $\beta = \alpha$, $\gamma = 0$. Assume that $r = -s$, where $1 \leqslant s \in \mathbb{N}$. Put $\beta = \alpha + se$ and $\gamma = se$. Then $\beta, \gamma \in \mathcal{M}_n$, and $\alpha = \beta - \gamma$. $\square$

The monoid $\mathcal{M}_n$ has an order $\geqslant$. If $\alpha, \beta \in \mathcal{M}_n$, then we write $\alpha \geqslant \beta$, if $\alpha - \beta \in \mathbb{N}^n$, that is, $\alpha \geqslant \beta \iff$ there exists $\gamma \in \mathcal{M}_n$ such that $\alpha = \beta + \gamma$. In particular, $\alpha \geqslant 0$ for any $\alpha \in \mathcal{M}_n$. It is clear that the relation $\geqslant$ is reflexive, transitive and antisymmetric. Thus $\mathcal{M}_n$ is a poset with respect to $\geqslant$.

Proposition 1.4. *The poset $\mathcal{M}_n$ is artinian, that is, if $\alpha^{(1)} \geqslant \alpha^{(2)} \geqslant \alpha^{(3)} \geqslant \cdots$ is a sequence of elements from $\mathcal{M}_n$, then there exists an integer s such that $\alpha^{(j)} = \alpha^{(j+1)}$ for all $j \geqslant s$.*

Proof. Given an element $\alpha = (\alpha_0, \dots, \alpha_{n-1}) \in \mathcal{M}_n$, we put $|\alpha| = \alpha_0 + \cdots + \alpha_{n-1}$. Observe that if $\alpha, \beta \in \mathcal{M}_n$ and $\alpha > \beta$, then $|\alpha| > |\beta|$. Suppose that there exists an infinite sequence $\alpha^{(1)} > \alpha^{(2)} > \alpha^{(3)} > \cdots$ of elements from $\mathcal{M}_n$, and let $s = |\alpha^{(1)}|$. Then we have an infinite sequence $s > |\alpha^{(2)}| > |\alpha^{(2)}| > \cdots \geqslant 0$, of natural numbers; a contradiction. $\square$

Let $\alpha \in \mathcal{M}_n$. We say that α is a *minimal element* of $\mathcal{M}_n$, if $\alpha \neq 0$ and there is no $\beta \in \mathcal{M}_n$ such that $\beta \neq 0$ and $\beta < \alpha$. Equivalently, α is a minimal element of $\mathcal{M}_n$, if $\alpha \neq 0$ and α is not a sum of two nonzero elements of $\mathcal{M}_n$. It follows from Proposition 1.4 that for any $0 \neq \alpha \in \mathcal{M}_n$ there exists a minimal element β such that $\beta \leqslant \alpha$. Moreover, every nonzero element of $\mathcal{M}_n$ is a finite sum of minimal elements.

Proposition 1.5. *The set of all minimal elements of $\mathcal{M}_n$ is finite.*

Proof. We use classical noetherian arguments. Consider the polynomial ring $R = \mathbb{Z}[z_0, \dots, z_{n-1}]$. If $\alpha = (\alpha_0, \dots, \alpha_{n-1})$ is an element from $\mathcal{M}_n$, then we denote by z^α the monomial $z_0^{\alpha_0} z_1^{\alpha_1} \cdots z_{n_1}^{\alpha_{n-1}}$. Let $\mathcal{S}$ be the set of all minimal elements of $\mathcal{M}_n$, and consider the ideal A of R generated by all elements of the form z^α with $\alpha \in \mathcal{S}$. Since R is noetherian, A is finitely generated; there exist $\alpha^{(1)}, \dots, \alpha^{(r)} \in \mathcal{S}$ such that $A = (z^{\alpha^{(1)}}, \dots, z^{\alpha^{(r)}})$. Let α be an arbitrary element from $\mathcal{S}$. Then $z^\alpha \in A$, and then there exist $j \in \{1, \dots, r\}$ and $\gamma \in \mathbb{N}^n$ such that $z^\alpha = z^\gamma \cdot z^{\alpha^{(j)}} = z^{\gamma + \alpha^{(j)}}$. This implies that $\alpha = \gamma + \alpha^{(j)}$. Observe that $\gamma = \alpha - \alpha^{(j)} \in \mathcal{G}_n \cap \mathbb{N}^n$, and $\mathcal{G}_n \cap \mathbb{N}^n = \mathcal{M}_n$, so γ belongs to $\mathcal{M}_n$. But α is minimal, so $\gamma = 0$, and consequently $\alpha = \alpha^{(j)}$. This means that $\mathcal{S}$ is a finite set equal to $\{\alpha^{(1)}, \dots, \alpha^{(r)}\}$. $\square$

We denote by ζ, the rotation of $\mathbb{Z}^n$ given by

$$\zeta(\alpha) = (\alpha_{n-1}, \alpha_0, \alpha_1, \dots, \alpha_{n-2}),$$

for $\alpha = (\alpha_0, \alpha_1, \dots, \alpha_{n-1}) \in \mathbb{Z}^n$. We have for example: $\zeta(e_j) = e_{j+1}$ for all $j \in \mathbb{Z}_n$, and $\zeta(e) = e$. The mapping $\zeta : \mathbb{Z}^n \to \mathbb{Z}^n$ is obviously an automorphism of the $\mathbb{Z}$-module $\mathbb{Z}^n$.

Lemma 1.6. *Let $\alpha \in \mathbb{Z}^n$. If $\alpha \in \mathcal{G}_n$, then $\zeta(\alpha) \in \mathcal{G}_n$. If $\alpha \in \mathcal{M}_n$, then $\zeta(\alpha) \in \mathcal{M}_n$. Moreover, α is a minimal element of $\mathcal{M}_n$ if and only if $\zeta(\alpha)$ is a minimal element of $\mathcal{M}_n$.*

Proof. Assume that $\alpha = (\alpha_0, \dots, \alpha_{n-1}) \in \mathcal{G}_n$. Then $\alpha_0 + \alpha_1\varepsilon + \cdots + \alpha_{n-1}\varepsilon^{n-1} = 0$. Multiplying it by ε, we have $0 = \alpha_0\varepsilon + \alpha_1\varepsilon^2 + \cdots + \alpha_{n-1}\varepsilon^n$. But $\varepsilon^n = 1$, so $\alpha_{n-1} + \alpha_0\varepsilon + \alpha_1\varepsilon^2 + \cdots + \alpha_{n-2}\varepsilon^{n-2} = 0$, and so $\zeta(\alpha) \in \mathcal{G}_n$. This implies also, that if $\alpha \in \mathcal{M}_n$, then $\zeta(\alpha) \in \mathcal{M}_n$.

Assume now that α is a minimal element of $\mathcal{M}_n$ and suppose that $\zeta(\alpha) = \beta + \gamma$, for some $\beta, \gamma \in \mathcal{M}_n$. Then we have $\alpha = \zeta^n(\alpha) = \zeta^{n-1}(\zeta(\alpha)) = \zeta^{n-1}(\beta) + \zeta^{n-1}(\gamma) = \beta' + \gamma'$, where $\beta' = \zeta^{n-1}(\beta)$ and $\gamma' = \zeta^{n-1}(\gamma)$ belong to $\mathcal{M}_n$. Since α is minimal, $\beta' = 0$ or $\gamma' = 0$, and then $\beta = 0$ or $\gamma = 0$. Thus if α is a minimal element of $\mathcal{M}_n$, then $\zeta(\alpha)$ is also a minimal element of $\mathcal{M}_n$. Moreover, if $\zeta(\alpha)$ is minimal, then α is minimal, because $\alpha = \zeta^{n-1}(\zeta(\alpha))$. $\square$

2. The derivation *d* and its constants

Let us recall that $d : k[X] \to k[X]$ is a derivation such that $d(x_j) = x_{j+1}$, for $j \in \mathbb{Z}_n$.

Proposition 2.1. *For each $j \in \mathbb{Z}_n$, the equality $d(u_j) = \varepsilon^{-j} u_j$ holds.*

Proof. See the proof of Lemma 1.1. $\square$

This means that d is a diagonal derivation of the polynomial ring $k[U] = k[u_0, \dots, u_{n-1}]$ which is equal to the ring $k[X]$. It is known (see for example [24]) that the algebra of constants of every diagonal derivation of $k[U] = k[X]$ is finitely generated over k. Therefore, $k[X]^d$ is finitely generated over k. We would like to describe a minimal set of generators of the ring $k[X]^d$, and a minimal set of generators of the field $k(X)^d$.

If $\alpha = (\alpha_0, \dots, \alpha_{n-1}) \in \mathbb{Z}^n$, then we denote by u^α the rational monomial $u_0^{\alpha_0} \cdots u_{n-1}^{\alpha_{n-1}}$. Recall (see the previous section) that $H_\alpha(t)$ is the polynomial $\alpha_0 + \alpha_1 t^1 + \cdots + \alpha_{n-1} t^{n-1}$ belonging to $\mathbb{Z}[t]$. As a consequence of Proposition 2.1 we obtain

Proposition 2.2. $d(u^\alpha) = H_\alpha(\varepsilon^{-1}) u^\alpha$ *for all* $\alpha \in \mathbb{Z}^n$.

Note that ε^{-1} is also a primitive n-th root of unity. Hence, by Proposition 1.2, we have the equivalence $H_\alpha(\varepsilon^{-1}) = 0 \iff H_\alpha(\varepsilon) = 0$, and so, by the previous proposition, we see that if $\alpha \in \mathbb{Z}^n$, then $d(u^\alpha) = 0 \iff \alpha \in \mathcal{G}_n$, and if $\alpha \in \mathbb{N}^n$, then $d(u^\alpha) = 0 \iff \alpha \in \mathcal{M}_n$. Moreover, if $F = b_1 u^{\alpha^{(1)}} + \cdots + b_r u^{\alpha^{(r)}}$, where $b_1, \dots, b_r \in k$ and $\alpha^{(1)}, \dots, \alpha^{(r)}$ are pairwise distinct elements of $\mathbb{N}^n$, then $d(F) = 0$ if and only if $d(b_i u^{\alpha^{(i)}}) = 0$ for every $i = 1, \dots, r$. Hence, $k[X]^d$ is generated over k by all elements of the form u^α with $\alpha \in \mathcal{M}_n$. We know (see the previous section), that every nonzero element of $\mathcal{M}_n$ is a finite sum of minimal elements of $\mathcal{M}_n$. Thus we have the following proposition.

Proposition 2.3. *The ring of constants $k[X]^d$ is generated over k by all the elements of the form u^β, where β is a minimal element of the monoid $\mathcal{M}_n$.*

In the next section we will prove some additional facts on the minimal number of generators of the ring $k[X]^d$. Now, let us look at the field $k(X)^d$.

Proposition 2.4. *The field of constants $k(X)^d$ is generated over k by all elements of the form u^γ with $\gamma \in \mathcal{G}_n$.*

Proof. Let L be the subfield of $k(X)$ generated over k by all elements of the form u^γ with $\gamma \in \mathcal{G}_n$. It is clear that $L \subseteq k(X)^d$. We will prove the reverse inclusion. Assume that $0 \neq f \in k(X)^d$. Since $k(X) = k(U)$, we have $f = A/B$, where A, B are coprime polynomials in $k[U]$. Put

$$A = \sum_{\alpha \in S_1} a_\alpha u^\alpha, \qquad B = \sum_{\beta \in S_2} b_\beta u^\beta,$$

where all a_α, b_β are nonzero elements of k, and S_1, S_2 are some subsets of $\mathbb{N}^n$. Since $d(f) = 0$, we have the equality $Ad(B) = d(A)B$. But A, B are relatively prime, so $d(A) = \lambda A$, $d(B) = \lambda B$ for some $\lambda \in k[U]$. Comparing degrees, we see that $\lambda \in k$. Moreover, by Proposition 2.2, we deduce that $d(u^\alpha) = \lambda u^\alpha$ for all $\alpha \in S_1$, and also $d(u^\beta) = \lambda u^\beta$ for all $\beta \in S_2$. This implies that if $\delta_1, \delta_2 \in S_1 \cup S_2$, then $d(u^{\delta_1 - \delta_2}) = 0$. In fact, $d(u^{\delta_1-\delta_2}) = d\left(\frac{u^{\delta_1}}{u^{\delta_2}}\right) = \frac{1}{u^{2\delta_2}}(d(u^{\delta_1})u^{\delta_2} - u^{\delta_1}d(u^{\delta_2})) = \frac{1}{u^{2\delta_2}}(\lambda u^{\delta_1}u^{\delta_2} - \lambda u^{\delta_1}u^{\delta_2}) = 0$. This means, that if $\delta_1, \delta_2 \in S_1 \cup S_2$, then $\delta_1 - \delta_2 \in \mathcal{G}_n$. Fix an element δ from $S_1 \cup S_2$. Then all $\alpha - \delta$, $\beta - \delta$ belong to $\mathcal{G}_n$, and we have

$$f = \frac{A}{B} = \frac{\sum a_\alpha u^\alpha}{\sum b_\beta u^\beta} = \frac{u^{-\delta}\sum a_\alpha u^\alpha}{u^{-\delta}\sum b_\beta u^\beta} = \frac{\sum a_\alpha u^{\alpha-\delta}}{\sum b_\beta u^{\beta-\delta}},$$

and hence, $f \in L$. $\square$

Let us recall (see Proposition 1.3) that every element of the group $\mathcal{G}_n$ is a difference of two elements from the monoid $\mathcal{M}_n$. Using this fact and the previous propositions we obtain

Proposition 2.5. *The field $k(X)^d$ is the field of quotients of the ring $k[X]^d$.*

Now we will prove that $k(X)^d$ is a field of rational functions over k, and its transcendental degree over k is equal to $n - \varphi(n)$, where φ is the Euler totient function. For this aim look at the cyclotomic polynomial $\Phi_n(t)$. Assume that

$$\Phi_n(t) = c_0 + c_1 t + \cdots + c_{\varphi(n)} t^{\varphi(n)}.$$

All the coefficients $c_0, \ldots, c_{\varphi(n)}$ are integers, and $c_0 = c_{\varphi(n)} = 1$. Put $m = n - \varphi(n)$ and

$$\gamma_0 = (c_0, c_1, \ldots, c_{\varphi(n)}, \underbrace{0, \ldots, 0}_{m-1}).$$

Note that $\gamma_0 \in \mathbb{Z}^n$, and $H_{\gamma_0}(t) = \Phi_n(t)$. Consider the elements $\gamma_0, \gamma_1, \ldots, \gamma_{m-1}$ defined by

$$\gamma_j = \zeta^j(\gamma_0), \quad \text{for } j = 0, 1, \ldots, m-1.$$

Observe that $H_{\gamma_j}(t) = \Phi_n(t) \cdot t^j$ for all $j \in \{0, \dots, m-1\}$. Since $\Phi_n(\varepsilon) = 0$, we have $H_{\gamma_j}(\varepsilon) = 0$, and so, the elements $\gamma_0, \dots, \gamma_{m-1}$ belong to $\mathcal{G}_n$.

Lemma 2.6. *The elements $\gamma_0, \dots, \gamma_{m-1}$ generate the group $\mathcal{G}_n$.*

Proof. Let $\alpha \in \mathcal{G}_n$. It follows from Proposition 1.2, that $H_\alpha(t) = F(t)\Phi_n(t)$, for some $F(t) \in \mathbb{Z}[t]$. Then obviously $\deg F(t) < m$. Put $F(t) = b_0 + b_1 t + \dots + b_{m-1}t^{m-1}$, with $b_0, \dots, b_{m-1} \in \mathbb{Z}$. Then we have

$$\begin{aligned} H_\alpha(t) &= b_0\big(\Phi_n(t)t^0\big) + b_1\big(\Phi_n(t)t^1\big) + \dots + b_{m-1}\big(\Phi_n(t)t^{m-1}\big) \\ &= b_0 H_{\gamma_0}(t) + \dots + b_{m-1}H_{\gamma_{m-1}}(t), \end{aligned}$$

and this implies that $\alpha = b_0\gamma_0 + b_1\gamma_1 + \dots + b_{m-1}\gamma_{m-1}$. $\square$

Consider now the rational monomials $w_0, \dots, w_{m-1}$ defined by

$$w_j = u^{\gamma_j} = u_{0+j}^{c_0} u_{1+j}^{c_1} u_{2+j}^{c_2} \cdots u_{\varphi(n)+j}^{c_{\varphi(n)}}$$

for $j = 0, 1, \dots, m-1$, where $m = n - \varphi(n)$. Each w_j is a rational monomial with respect to $u_0, \dots, u_{n-1}$ of the same degree equal to $\Phi_n(1) = c_0 + c_1 + \dots + c_{\varphi(n)}$. It is known (see for example [13]) that $\Phi_n(1) = p$ if n is power of a prime number p, and $\Phi_n(1) = 1$ in all other cases. As each u_j is a homogeneous polynomial in $k[X]$ of degree 1, we have:

Proposition 2.7. *The elements $w_0, \dots, w_{m-1}$ are homogeneous rational functions with respect to variables $x_0, \dots, x_{n-1}$, of the same degree r. If n is a power of a prime number p, then $r = p$, and $r = 1$ in all other cases.*

As an immediate consequence of Lemma 2.6 and Proposition 2.4, we obtain the equality $k(X)^d = k(w_0, \dots, w_{m-1})$.

Lemma 2.8. *The elements $w_0, \dots, w_{m-1}$ are algebraically independent over k.*

Proof. Let A be the $n \times m$ Jacobi matrix $[a_{ij}]$, where $a_{ij} = \frac{\partial w_j}{\partial u_i}$ for $i = 0, 1, \dots, n-1$, $j = 0, 1, \dots, m-1$. It is enough to show that $\operatorname{rank}(A) = m$ (see for example [9]). Observe that $\frac{\partial w_0}{\partial u_0} = c_0 u_0^{c_0-1} u_1^{c_1} \cdots u_{\varphi(n)}^{c_{\varphi(n)}} \neq 0$ (because $c_0 = 1$), and $\frac{\partial w_j}{\partial u_0} = 0$ for $j \geqslant 1$. Moreover, $\frac{\partial w_1}{\partial u_1} \neq 0$ and $\frac{\partial w_j}{\partial u_1} = 0$ for $j \geqslant 2$, and in general, $\frac{\partial w_i}{\partial u_i} \neq 0$ and $\frac{\partial u_j}{\partial u_i} = 0$ for all $i, j = 0, \dots, m-1$ with $j > i$. This means, that the upper $m \times m$ matrix of A is a triangular matrix with a nonzero determinant. Therefore, $\operatorname{rank}(A) = m$. $\square$

Thus, we proved the following theorem.

Theorem 2.9. *The field of constants $k(X)^d$ is a field of rational functions over k and its transcendental degree over k is equal to $m = n - \varphi(n)$, where φ is the Euler totient function. More precisely,*

$$k(X)^d = k(w_0, \dots, w_{m-1}),$$

where the elements $w_0, \dots, w_{m-1}$ are as above.

Now we will describe all constants of d which are homogeneous rational functions of degree zero. Let us recall that a nonzero polynomial F is homogeneous of degree r, if all its monomials are of the same degree r. We assume that the zero polynomial is homogeneous of arbitrary degree. Homogeneous polynomials are also homogeneous rational functions, which are defined in the following way. Let $f = f(x_0, \dots, x_{n-1}) \in k(X)$. We say that f is *homogeneous* of degree $s \in \mathbb{Z}$, if in the field $k(t, x_0, \dots, x_{n-1})$ the equality $f(tx_0, tx_1, \dots, tx_{n-1}) = t^s \cdot f(x_0, \dots, x_{n-1})$ holds. The characteristic plays no role in the previous definition whereas it is easy to prove (see for example [24, Proposition 2.1.3]) the following equivalent formulations of homogeneous rational functions when the characteristic of k is 0.

Proposition 2.10. *Let k be a field of characteristic 0. Let F, G be nonzero coprime polynomials in $k[X]$ and let $f = F/G$. Let $s \in \mathbb{Z}$. The following conditions are equivalent.*

(1) *The rational function f is homogeneous of degree s.*

(2) *The polynomials F, G are homogeneous of degrees p and q, respectively, where $s = p - q$.*

(3) $x_0 \frac{\partial f}{\partial x_0} + \cdots + x_{n-1} \frac{\partial f}{\partial x_{n-1}} = sf$.

Equality (3) is called the *Euler formula*. In this paper we denote by E the *Euler derivation* of $k(X)$, that is, E is a derivation of $k(X)$ defined by $E(x_j) = x_j$ for all $j \in \mathbb{Z}_n$. As usual, we denote by $k(X)^E$ the field of constants of E. Observe that, by Proposition 2.10, a rational function $f \in k(X)$ belongs to $k(X)^E$ if and only if f is homogeneous of degree zero. In particular, the set of all homogeneous rational functions of degree zero is a subfield of $k(X)$. It is obvious that the quotients $\frac{x_1}{x_0}, \dots, \frac{x_{n-1}}{x_0}$ belong to $k(X)^E$, and they are algebraically independent over k. Moreover, $k(X)^E = k(\frac{x_1}{x_0}, \dots, \frac{x_{n-1}}{x_0})$. Therefore, $k(X)^E$ is a field of rational functions over k, and its transcendence degree over k is equal to $n-1$. Put $q_j = \frac{x_{j+1}}{x_j}$ for all $j \in \mathbb{Z}_n$. In particular, $q_{n-1} = \frac{x_0}{x_{n-1}}$. The elements $q_0, \dots, q_{n-1}$ belong to $k(X)^E$ and moreover, $\frac{x_j}{x_0} = q_0 q_1 \cdots q_{j-1}$ for $j = 1, \dots, n-1$. Thus we have the following equality.

Proposition 2.11. $k(X)^E = k(\frac{x_1}{x_0}, \frac{x_2}{x_1}, \dots, \frac{x_{n-1}}{x_{n-2}}, \frac{x_0}{x_{n-1}})$.

Now consider the field $k(X)^{d,E} = k(X)^d \cap k(X)^E$.

Lemma 2.12. *Let $d_1, d_2 : k(X) \to k(X)$ be two derivations. Assume that $K(X)^{d_1} = k(c, b_1, \dots, b_s)$, where $c, b_1, \dots, b_s$ are algebraically independent over k elements from $k(X)$ such that $d_2(b_1) = \cdots = d_2(b_s) = 0$ and $d_2(c) \neq 0$. Then $k(X)^{d_1} \cap k(X)^{d_2} = k(b_1, \dots, b_s)$.*

Proof. Put $L = k(b_1, \dots, b_s)$. Observe that $k(X)^{d_1} = L(c)$, and c is transcendental over L. Let $0 \neq f \in k(X)^{d_1} \cap k(X)^{d_2}$. Then $f = \frac{F(c)}{G(c)}$, where $F(t), G(t)$ are coprime polynomials in $L[t]$. We have: $d_2(F(c)) = F'(c)d_2(c)$, $d_2(G(c)) = G'(c)d_2(c)$, where $F'(t), G'(t)$ are derivatives of $F(t), G(t)$, respectively. Since $d_2(f) = 0$, we have

$$0 = d_2\bigl(F(c)\bigr)G(c) - d_2\bigl(G(c)\bigr)F(c) = \bigl(F'(c)G(c) - G'(c)F(c)\bigr)d_2(c),$$

and so, $(F'G - G'F)(c) = 0$, because $d_2(c) \neq 0$. Since c is transcendental over L, we obtain the equality $F'(t)G(t) = G'(t)F(t)$ in $L[t]$, which implies that $F(t)$ divides $F'(t)$ and $G(t)$ divides $G'(t)$ (because $F(t), G(t)$ are relatively prime), and comparing degrees we deduce that $F'(t) = G'(t) = 0$, that is, $F(t) \in L$ and $G(t) \in L$. Thus the elements $F(c)$, $G(c)$ belong to L and so, $f = \frac{F(c)}{G(c)}$ belongs to L. Therefore, $k(X)^{d_1} \cap k(X)^{d_2} \subseteq L$. The reverse inclusion is obvious. $\square$

Let us return to the rational functions $w_0, \dots, w_{m-1}$. We know (see Proposition 2.7) that they are homogeneous of the same degree. Put: $d_1 = d$, $d_2 = E$, $c = w_0$ and $b_j = \frac{w_j}{w_0}$ for $j = 1, \dots, m-1$, then, as a consequence of Lemma 2.12. We obtain the following proposition.

Proposition 2.13. $k(X)^{d,E} = k(\frac{w_1}{w_0}, \dots, \frac{w_{m-1}}{w_0})$.

Since $w_0, \dots, w_{m-1}$ are algebraically independent over k (see Lemma 2.8), the quotients $\frac{w_1}{w_0}, \dots, \frac{w_{m-1}}{w_0}$ are also algebraically independent over k. Thus, $k(X)^{d,E}$ is a field of rational functions and its transcendental degree over k is equal to $n-\varphi(n)-1$, where φ is the Euler totient function. Since n is prime if and only if $n-\varphi(n)-1=0$, we obtain:

Corollary 2.14. *$k(X)^{d,E}=k \iff n$ is a prime number.*

3. Numbers of minimal elements

Let $\mathcal{F}$ be the set of all the minimal elements of the monoid $\mathcal{M}_n$, and denote by $\nu(n)$ the cardinality of $\mathcal{F}$. We know, by Proposition 1.5, that $\nu(n)<\infty$. We also know (see Proposition 2.3) that the ring $k[X]^d$ is generated over k by all the elements of the form u^β, where $\beta\in\mathcal{F}$. But $k[X]$ is equal to the polynomial ring $k[U]=k[u_0,\dots,u_{n-1}]$, so $k[X]^d$ is generated over k by a finite set of monomials with respect to the variables $u_0,\dots,u_{n-1}$.

It is clear that if β,γ are distinct elements from $\mathcal{F}$, then $u^\beta\nmid u^\gamma$ and $u^\gamma\nmid u^\beta$. This implies that no monomial u^β, $\beta\in\mathcal{F}$ belongs to the algebra generated by other u^γ, $\gamma\in\mathcal{F}$, $u^\gamma\nmid u^\beta$. Thus, $\{u^\beta;\ \beta\in\mathcal{F}\}$ is a minimal set of generators of $k[X]^d$.

Moreover, $\{u^\beta;\ \beta\in\mathcal{F}\}$ is a set of generators of $k[X]^d$ with the minimal number of elements according to the following proposition.

Proposition 3.1. *Let $f_1,\dots,f_s$ be polynomials in $k[X]$. If $k[X]^d=k[f_1,\dots,f_s]$, then $s\geqslant\nu(n)$.*

Proof. Let M be the maximal ideal of $k[X]^d$ of all $f\in k[X]^d$ such that $f(0)=0$. All u^β with $\beta\in\mathcal{M}_n\setminus\{0\}$ belong to M; their set is a basis of the k-vector space M whereas the subset $\{u^\beta,\beta\in\mathcal{M}_n\setminus\{0\},\beta\notin\mathcal{F}\}$ of it is a basis of M^2. The image of $\{u^\beta,\beta\in\mathcal{F}\}$ in M/M^2 then constitutes a basis of the k-vector space M/M^2 whose finite dimension is thus $\nu(n)$.

Now, for any $f\in k[X]^d$, denote by $\tilde f$ the difference $\tilde f=f-f(0)$, which belongs to M.

If $\{f_1,\dots,f_s\}$ generates the algebra $k[X]^d$, the same is true for the set $\{\tilde f_1,\dots,\tilde f_s\}$ of elements of M. As a k-vector space, M is then generated by all products $\prod_{i=1}^{i=s}\tilde f_i^{\alpha_i}$, where the α_i are natural numbers with $\sum\alpha_i\geqslant 1$. All such products with $\sum\alpha_i\geqslant 2$ then belong to M^2 and the images of $\tilde f_1,\dots,\tilde f_s$ in M/M^2 generate the k-vector space M/M^2. So we have: $s\geqslant\nu(n)$. $\square$

In this section we prove, among others, that $k[X]^d$ is a polynomial ring over k if and only if n is a power of a prime number. Moreover, we present some additional properties of the number $\nu(n)$, which are consequences of known results on vanishing sums of roots of unity; see for example [12,29,31,32], where many interesting facts and references on this subject can be found.

We denote by $\xi(n)$ the sum $\sum_{p|n}\frac{n}{p}$, where p runs through all prime divisors of n. Note that if a,b are positive coprime integers, then $\xi(ab)=a\xi(b)+\xi(a)b$.

First we show that the computation of $\nu(n)$ can be reduced to the case when n is square-free. For this aim let us denote by n_0 the largest square-free factor of n, and by n' the integer n/n_0. Then $\varphi(n)=n'\varphi(n_0)$ and $\xi(n)=n'\xi(n_0)$. Moreover, it is not difficult to prove that $\Phi_n(t)=\Phi_{n_0}(t^{n'})$. Indeed, observe that $\Phi_{n_0}(t^{n'})$ is a monic polynomial of degree $\varphi(n_0)n'=\varphi(n)$. Since $\varepsilon^{n'}$ is a primitive n_0-th root of unity, we have $\Phi_{n_0}(\varepsilon^{n'})=0$. Hence, $\Phi_n(t)$ divides $\Phi_{n_0}(t^{n'})$, and thus equals to $\Phi_{n_0}(t^{n'})$.

Assume now that $n=mc$, where $m\geqslant 2$, $c\geqslant 2$ are integers. For a given sequence $\gamma=(\gamma_0,\dots,\gamma_{m-1})\in\mathbb{Z}^m$, consider the sequence

$$\overline{\gamma}=(\gamma_0,\underbrace{0,\dots,0}_{c-1},\gamma_1,\underbrace{0,\dots,0}_{c-1},\dots,\gamma_{m-1},\underbrace{0,\dots,0}_{c-1}).$$

This sequence is an element of $\mathbb{Z}^n$, and it is easy to prove the following lemma.

Lemma 3.2. *$\overline{\gamma}\in\mathcal{G}_n \iff \gamma\in\mathcal{G}_m$, and $\overline{\gamma}\in\mathcal{M}_n \iff \gamma\in\mathcal{M}_m$. Moreover, $\overline{\gamma}$ is a minimal element of $\mathcal{M}_n \iff \gamma$ is a minimal element of $\mathcal{M}_m$.*

Using the above notations, we have:

Proposition 3.3. $\nu(n) = n'\nu(n_0)$, *for all* $n \geqslant 3$.

Proof. If $n' = 1$ then this is clear. Assume that $n' \geqslant 2$. Let $\alpha = (\alpha_0, \ldots, \alpha_{n-1})$ be an element of $\mathcal{M}_n$. For every $j \in \{0, 1, \ldots, n'-1\}$, let us denote:

$$f_j(t) = \sum_{i=0}^{n_0-1} \alpha_{in'+j} t^{in'+j} = t^j \sum_{i=0}^{n_0-1} \alpha_{in'+j} t^{in'}, \qquad \beta_j = (\alpha_{0n'+j}, \alpha_{1n'+j}, \ldots, \alpha_{(n_0-1)n'+j}).$$

Note that $f_j(t) \in \mathbb{Z}[t]$ and $\beta_j \in \mathbb{N}^{n_0}$. Consider the elements $\overline{\beta_0}, \overline{\beta_1}, \ldots, \overline{\beta_{n'-1}}$, introduced before Lemma 3.2 for $m = n_0$ and $c = n'$. Observe that

$$\alpha = \overline{\beta_0} + \zeta(\overline{\beta_1}) + \zeta^2(\overline{\beta_2}) + \cdots + \zeta^{n'-1}(\overline{\beta_{n'-1}}) \tag{$*$}$$

where ζ is the rotation of $\mathbb{Z}^n$, as in Section 1. Denote also by $f(t)$ the polynomial $H_\alpha(t) = \alpha_0 + \alpha_1 t + \cdots + \alpha_{n-1}t^{n-1}$, that is, $f(t) = \sum_{j=0}^{n'-1} f_j(t)$. It follows from Proposition 1.2, that $f(t) = g(t)\Phi_n(t)$ for some $g(t) \in \mathbb{Z}[t]$.

For every $j \in \{0, 1, \ldots, n'-1\}$, denote by A_j the set of polynomials $F(t) \in \mathbb{Z}[t]$ such that the degrees of all nonzero monomials of $F(t)$ are congruent to j modulo n'. We assume that the zero polynomial also belongs to A_j. It is clear that each A_j is a $\mathbb{Z}$-module, $A_iA_j \subseteq A_{i+j}$ for $i, j \in \mathbb{Z}_{n'}$, and $\mathbb{Z}[t] = \bigoplus_{j \in \mathbb{Z}_{n'}} A_j$. Thus, we have a gradation on $\mathbb{Z}[t]$ with respect to $\mathbb{Z}_{n'}$. We will say that it is the *n'-gradation*, and the decompositions of polynomials with respect to this gradation we will call the *n'-decompositions*.

Let $g(t) = g_0(t) + g_1(t) + \cdots + g_{n'-1}(t)$ be the n'-decomposition of $g(t)$; each $g_j(t)$ belongs to A_j. Since $\Phi_n(t) = \Phi_{n_0}(t^{n'})$, we have $\Phi_n(t) \in A_0$. Hence,

$$f(t) = g_0(t)\Phi_n(t) + g_1(t)\Phi_n(t) + \cdots + g_{n'-1}(t)\Phi_n(t)$$

is the n'-decomposition of $f(t)$. But the previous equality $f(t) = \sum f_j(t)$ is also the n'-decomposition of $f(t)$, so we have $f_j(t) = g_j(t)\Phi_n(t)$ for all $j \in \mathbb{Z}_{n'}$.

Put $\eta = \varepsilon^{n'}$. Then η is a primitive n_0-th root of unity and, for every $j \in \mathbb{Z}_{n'}$, we have

$$\sum_{i=0}^{n_0-1} \alpha_{in'+j}\eta^i = \varepsilon^{-j} f_j(\varepsilon) = \varepsilon^{-j} g_j(\varepsilon)\Phi_n(\varepsilon) = \varepsilon^{-j} g_j(\varepsilon) \cdot 0 = 0.$$

The equality says that $H_{\overline{\beta}_j}(\varepsilon) = 0$, and so $\overline{\beta}_j \in \mathcal{M}_n$. Hence, β_j is an element of $\mathcal{M}_{n_0}$ by Lemma 3.2.

Assume now that the above α is a minimal element of $\mathcal{M}_n$. Then, by $(*)$, we have $\alpha = \zeta^j(\overline{\beta_j})$ for some $j \in \{0, \ldots, n'-1\}$. Then $\overline{\beta_j} = \zeta^{n-j}(\alpha)$ and so, $\overline{\beta_j}$ is (by Lemma 1.6) a minimal element of $\mathcal{M}_n$, and this implies, by Lemma 3.2, that β_j is a minimal element of $\mathcal{M}_{n_0}$. Thus, every minimal element α of $\mathcal{M}_n$ is of the form $\alpha = \zeta^j(\overline{\beta})$, where $j \in \{0, \ldots, n'-1\}$ and β is a minimal element of $\mathcal{M}_{n_0}$, and it is clear that this presentation is unique. This means, that $\nu(n) \leqslant n' \cdot \nu(n_0)$.

Assume now that β is a minimal element of $\mathcal{M}_{n_0}$. Then we have n' pairwise distinct sequences $\overline{\beta}, \zeta(\overline{\beta}), \zeta^2(\overline{\beta}), \ldots, \zeta^{n'-1}(\overline{\beta})$, which are (by Lemmas 1.6 and 3.2) minimal elements of $\mathcal{M}_n$. Hence, $\nu(n) \geqslant n' \cdot \nu(n_0)$. Therefore, $\nu(n) = n' \cdot \nu(n_0)$. $\square$

If p is prime, then $\nu(p) = 1$; the constant sequence $e = (1, 1, \ldots, 1)$ is the unique minimal element of $\mathcal{M}_p$. In this case $k[X]^d$ is the polynomial ring $k[w]$, where $w = u_0 \ldots u_{p-1}$ is the cyclic determinant of the variables $x_0, \ldots, x_{p-1}$ (see the Introduction). In particular, if $p = 3$, then $k[x_0, x_1, x_2]^d = k[x_0^3 + x_1^3 + x_2^3 - 3x_0x_1x_2]$. Using Proposition 3.3 and its proof we obtain:

Proposition 3.4. *Let $n = p^s$, where $s \geqslant 1$ and p is a prime number. Then $\nu(n) = \xi(n) = p^{s-1}$, and the ring of constants $k[X]^d$ is a polynomial ring over k in p^{s-1} variables.*

Assume now that p is a prime divisor of n. Denote by n_p the integer n/p, and consider the sequences

$$E_i^{(p)} = \sum_{j=0}^{p-1} e_{i+jn_p},$$

for $i = 0, 1, \dots, n_p - 1$. Recall that $e_0 = (1, 0, \dots, 0)$, $\dots$, $e_{n-1} = (0, 0, \dots, 0, 1)$ are the basic elements of $\mathbb{Z}^n$. Observe that each $E_i^{(p)}$ is equal to $\zeta^i(E_0^{(p)})$, where ζ is the rotation of $\mathbb{Z}^n$. Observe also that $E_0^{(p)} = \bar{e}$, where in this case $e = (1, 1, \dots, 1) \in \mathbb{Z}^p$ and $\bar{e}$ is the element of $\mathbb{Z}^n$ introduced before Lemma 3.2 for $m = p$ and $c = n_p$. But e is a minimal element of $\mathcal{M}_p$, so we see, by Lemmas 3.2 and 1.6, that each $E_i^{(p)}$ is a minimal element of $\mathcal{M}_n$. We will call such $E_i^{(p)}$ a *standard* minimal element of $\mathcal{M}_n$. It is clear that if $i, j \in \{0, 1, \dots, n_p - 1\}$ and $i \neq j$, then $E_i^{(p)} \neq E_j^{(p)}$. Observe also that, for every i, we have $|E_i^{(p)}| = p$. This implies, that if $p \neq q$ are prime divisors of n, then $E_i^{(p)} \neq E_j^{(q)}$ for all $i \in \{0, \dots, n_p - 1\}$, $j \in \{0, 1, \dots, n_q - 1\}$. Assume that $p_1, \dots, p_s$ are all the prime divisors of n. Then, by the above observations, the number of all standard minimal elements of $\mathcal{M}_n$ is equal to $n_{p_1} + \dots + n_{p_s} = \xi(n)$. Hence, we proved the following proposition.

Proposition 3.5. $\nu(n) \geqslant \xi(n)$, *for all $n \geqslant 3$.*

For a proof of the next result we need the following lemma.

Lemma 3.6. *If n is divisible by two distinct primes, then $\xi(n) + \varphi(n) > n$.*

Proof. Since $\xi(n) = n'\xi(n_0)$, $\varphi(n) = n'\varphi(n_0)$ and $n = n'n_0$ we may assume that n is square-free. Let $n = p_1 \cdots p_s$, where $s \geqslant 2$ and $p_1, \dots, p_s$ are distinct primes. If $s = 2$, then the equality is obvious. Assume that $s \geqslant 3$, and that the equality is true for $s - 1$. Put $p = p_s$, $m = p_1 \cdots p_{s-1}$. Then m is square-free, $n = mp$, $\gcd(m, p) = 1$, $\xi(m) + \varphi(m) > m$ by induction assumption and moreover, $\varphi(m) < m$. Hence, $\xi(n) + \varphi(n) = p\xi(m) + \xi(p)m + \varphi(p)\varphi(m) = p\xi(m) + m + (p-1)\varphi(m) > p\xi(m) + p\varphi(m) > pm = n$. $\square$

Theorem 3.7. *The ring of constants $k[X]^d$ is a polynomial ring over k if and only if n is a power of a prime number.*

Proof. Assume that n is divisible by two distinct primes, and suppose that $k[X]^d$ is a polynomial ring of the form $k[f_1, \dots, f_s]$, where $f_1, \dots, f_s \in k[X]$ are algebraically independent over k. Then, by Proposition 3.1, we have $s \geqslant \nu(n)$. The polynomials $f_1, \dots, f_s$ belong to the field $k(X)^d$, and we know, by Theorem 2.9, that the transcendental degree of this field over k is equal to $n - \varphi(n)$. Hence, $s \leqslant n - \varphi(n)$. But $\nu(n) \geqslant \xi(n)$ (Proposition 3.5) and $\xi(n) > n - \varphi(n)$ (Lemma 3.6), so we have a contradiction: $s \geqslant \nu(n) \geqslant \xi(n) > n - f(n)$. This means, that if n is divisible by two distinct primes, then $k[X]^d$ is not a polynomial ring over k. The "if" part follows from Proposition 3.4. $\square$

It is well known (see for example [2]) that all coefficients of the cyclotomic polynomial $\Phi_n(t)$ are nonnegative if and only if n is a power of a prime. Thus, we proved that $k[X]^d$ is a polynomial ring over k if and only if all coefficients of $\Phi_n(t)$ are nonnegative.

In our next considerations we will apply the following theorem of Rédei, de Bruijn and Schoenberg.

Theorem 3.8. *(See [28,4,30].) The standard minimal elements of $\mathcal{M}_n$ generate the group $\mathcal{G}_n$.*

Known proofs of the above theorem usually use techniques of group rings. Lam and Leung [12] gave a new proof using induction and group-theoretic techniques.

Now, let us assume that $n = pq$, where $p \neq q$ are primes. In this case, Lam and Leung [12] proved that $\nu(n) = p + q$. We will give a new elementary proof of this fact. Note that in this case $n_p = q$ and $n_q = p$. Put $P_i = E_i^{(q)}$ for $i = 0, 1, \dots, p-1$, and $Q_j = E_j^{(p)}$ for $j = 0, \dots, q-1$. We have $p + q$ elements $P_0, \dots, P_{p-1}, Q_0, \dots, Q_{q-1}$, which are the standard minimal elements of $\mathcal{M}_{pq}$.

Lemma 3.9. *For every $\beta \in \mathcal{M}_{pq}$ there exist nonnegative integers $a_0, \dots, a_{p-1}, b_0, \dots, b_{q-1}$ such that $\beta = a_0 P_0 + \cdots + a_{p-1} P_{p-1} + b_0 Q_0 + \cdots + b_{q-1} Q_{q-1}$.*

Proof. Let $\beta \in \mathcal{M}_{pq}$. Then $\beta \in \mathcal{G}_{pq}$ and, by Theorem 3.8, we have an equality $\beta = \sum a_i P_i + \sum b_j Q_j$, for some integers $a_0, \dots, a_{p-1}, b_0, \dots, b_{q-1}$. Since $\sum_{i=0}^{p-1} P_i = e = \sum_{j=0}^{q-1} Q_j$, we may assume that $b_{q-1} = 0$. Let us recall that $P_i = \sum_{j=0}^{q-1} e_{jp+i}$ for $i = 0, \dots, p-1$, and $Q_j = \sum_{i=0}^{p-1} e_{iq+j}$ for $j = 0, \dots, q-1$. Thus, we have

$$\beta = \sum_{i=0}^{p-1} \sum_{j=0}^{q-1} (a_i e_{jp+i} + b_j e_{iq+j}).$$

By the Chinese Remainder Theorem, the map

$$\{0, \dots, pq-1\} \ni l \mapsto \big(\lambda(l), \mu(l)\big) \in \{0, \dots, p-1\} \times \{0, \dots, q-1\}$$

is a bijection, where $\lambda(l)$ and $\mu(l)$ are remainders of l divided by p and q, respectively. Hence, we have

$$\beta = \sum_{i=0}^{p-1} \sum_{j=0}^{q-1} (a_i e_{jp+i} + b_j e_{iq+j}) = \sum_{l=0}^{pq-1} (a_{\lambda(l)} + b_{\mu(l)}) e_l.$$

Since β is an element of $\mathcal{M}_{pq} \subset \mathbb{N}^{pq}$, it follows that

$$a_i + b_j \geqslant 0 \quad \text{for all } i \in \{0, \dots, p-1\},\ j \in \{0, \dots, q-1\}. \tag{$*$}$$

Let $s \in \{0, \dots, q-1\}$ be such that $b_s = \min\{b_0, \dots b_{q-1}\}$. Since $\sum_{i=0}^{p-1} P_i = e = \sum_{j=0}^{q-1} Q_j$, we can express

$$\beta = \sum_{i=0}^{p-1} a_i P_i + \sum_{j=0}^{q-1} b_j Q_j = \sum_{i=0}^{p-1} (a_i + b_s) P_i + \sum_{j=0}^{q-1} (b_j - b_s) Q_j,$$

in which $a_i + b_s \geqslant 0$ for each i by $(*)$, and $b_j - b_s \geqslant 0$ for each j by the minimality of b_s. $\square$

Theorem 3.10. *(See [12].) Let $n = p^i q^j$, where $p \neq q$ are primes and i, j are positive integers. Then $\nu(n) = \xi(n) = p^{i-1} q^{j-1}(p+q)$. In other words, the monoid $\mathcal{M}_n$ has exactly $p^{i-1} q^{j-1}(p+q)$ minimal elements, and all its minimal elements are standard.*

Proof. Let $n = pq$, and $\mathcal{B} = \{P_0, \dots, P_{p-1}, Q_0, \dots, Q_{q-1}\}$. Then $\mathcal{B}$ is contained in $\mathcal{F}$. By Lemma 3.9, we have $\mathcal{B} = \mathcal{F}$. Hence, we get $\nu(pq) = \#\mathcal{F} = \#\mathcal{B} = p + q = \xi(pq)$. This implies, by the equality $\xi(n) = n' \xi(n_0)$ and Proposition 3.3, that $\nu(n) = \xi(n)$ for all n of the form $p^i q^j$. $\square$

As a consequence of Theorem 3.10 and Proposition 3.1 we obtain:

Corollary 3.11. *Let $n = p^i q^j$, where $p \neq q$ are primes and i, j are positive integers. Then the minimal number of generators of the ring of constants $k[X]^d$ is equal to $\xi(n) = p^{i-1}q^{j-1}(p+q)$.*

We already know that if n is divisible by at most two distinct primes, then every minimal element of $\mathcal{M}_n$ is standard. It is well known (see for example [12,32,29]) that in all other cases there always exist nonstandard minimal elements. For instance, Lam and Leung [12] proved that if n is divisible by three primes $p_1 < p_2 < p_3$, then the equality $a_1a_2 + a_3 = 0$, where $a_j = \sum_{i=1}^{p_1-1} \varepsilon^{inp_i}$ for $j = 1, 2, 3$, is of the form $H_\alpha(\varepsilon) = 0$, where α is a nonstandard minimal element of $\mathcal{M}_n$. There are also other examples. Assume that $n = p_1 \cdots p_s$, where $p_1, \ldots, p_s$ are distinct primes, and denote by U the set of all numbers from $\{1, 2, \ldots, n-1\}$ which are relatively prime to n. If $s \geqslant 3$ is odd, then

$$\gamma = e_0 + \sum_{u \in U} e_u$$

is a nonstandard minimal element of $\mathcal{M}_n$. This element γ belongs to $\mathcal{M}_n$, because the sum of all primitive n-th roots of unity is equal to $\mu(n)$, where μ is the Möbius function (see for example [15,19]). The minimality of γ follows from the known fact (see for example [3]) that if n is square-free, then all the primitive n-th roots of unity form a basis of $\mathbb{Q}(\varepsilon)$ over $\mathbb{Q}$. Observe also that $|\gamma| = \varphi(n) + 1 \neq p_i$ for all $i = 1, \ldots, s$, so γ is nonstandard.

If $s \geqslant 4$ is even, then put $p = p_s$, $n' = p_1 \cdots p_{s-1}$, and let U' be the set of all numbers from $\{1, 2, \ldots, n'-1\}$ which are relatively prime to n'. Then ε^p is a primitive n'-th root of unity and, using similar arguments, we see that

$$\gamma' = e_0 + \sum_{v \in U'} e_{vp}$$

is a nonstandard minimal element of $\mathcal{M}_n$. Now we use Lemma 3.2 and Proposition 3.3, and we obtain the following result of Lam and Leung.

Theorem 3.12. *(See [12].) If $n \geqslant 3$ is an integer, then $\nu(n) = \xi(n)$ if and only if n has at most two prime divisors.*

Now, as a consequence of the previous considerations, we obtain:

Corollary 3.13. *The number of a minimal set of generators of $k[X]^d$ is equal to $\xi(n)$ if and only if n has at most two prime divisors.*

Note that in our examples all nonzero coefficients of the minimal (standard or nonstandard) elements of $\mathcal{M}_n$ were equal to 1. Recently, John P. Steinberger [32] gave the first explicit constructions of nonstandard minimal elements of $\mathcal{M}_n$ (for some n) with coefficients greater than 1 (indeed containing arbitrary large coefficients). He gave at the same time an answer to an old question of H.W. Lenstra Jr. [14] concerning this subject.

4. Polynomial constants of Δ

Let us recall that Δ is the derivation of $k[Y]$ given by $\Delta(y_j) = y_j(y_{j+1} - y_j)$ for $j \in \mathbb{Z}_n$, where $k[Y] = k[y_0, \ldots, y_{n-1}]$. It is a homogeneous derivation, that is, all the polynomials $\Delta(y_0), \ldots, \Delta(y_{n-1})$ are homogeneous of the same degree. Put $v = y_0y_1 \cdots y_{n-1}$. Observe that $v \in k[Y]^\Delta$. In this section we will prove that $k[Y]^\Delta = k[v]$. For this aim we first study Darboux polynomials of Δ.

We say that a nonzero polynomial $F \in k[Y]$ is a *Darboux polynomial* of Δ, if F is homogeneous and there exists a polynomial $\Lambda \in k[Y]$ such that $\Delta(F) = \Lambda F$. Such a polynomial Λ is uniquely determined and we say that Λ is the *cofactor* of F. Some basic properties of Darboux polynomials of arbitrary homogeneous derivations one can find for example in [22,20] or [24]. Note that if $F, G \in k[Y]$ and

FG is a Darboux polynomial of Δ, then F, G are also Darboux polynomials of Δ [22,24]. It is obvious that in our case each cofactor Λ is of the form $\lambda_0 y_0 + \lambda_1 y_1 + \cdots + \lambda_{n-1} y_{n-1}$, where the coefficients $\lambda_0, \dots, \lambda_{n-1}$ belong to k. We say that a Darboux polynomial is *strict* if it is not divisible by any of the variables $y_0, \dots, y_{n-1}$. The following important proposition is a special case of Proposition 3 from our paper [17]. For the sake of completeness we repeat its proof.

Proposition 4.1. *Let $F \in k[Y] \setminus k$ be a strict Darboux polynomial of Δ and let $\Lambda = \lambda_0 y_0 + \cdots + \lambda_{n-1} y_{n-1}$ be its cofactor. Then all λ_i are integers and they belong to the interval $[-r, 0]$, where $r = \deg F$. Moreover, at least two of the λ_i's are nonzero.*

Proof. As F is strict, for any i, the polynomial $F_i = F_{|y_i=0}$ (that we get by evaluating F in $y_i = 0$) is a nonzero homogeneous polynomial with the same degree r in $n-1$ variables (all but y_i). Evaluating the equality $\Delta(F) = \Lambda F$ at $y_{n-1} = 0$ we obtain

$$\sum_{i=0}^{n-3} y_i(y_{i+1} - y_i)\frac{\partial F_{n-1}}{\partial y_i} - y_{n-2}^2 \frac{\partial F_{n-1}}{\partial y_{n-2}} = \left(\sum_{i=0}^{n-2} \lambda_i y_i\right) F_{n-1}. \tag{$*$}$$

Let r_0 be the degree of F_{n-1} with respect to y_0. Then obviously $0 \leqslant r_0 \leqslant r$. Consider now F_{n-1} as a polynomial in $k[y_1, \dots, y_{n-2}][y_0]$. Balancing monomials of degree $r_0 + 1$ in the equality $(*)$ gives $\lambda_0 = -r_0$. The same results hold for all coefficients of the cofactor Λ.

We have already proved that all λ_i are integers and $-r \leqslant \lambda_i \leqslant 0$. Moreover, we have proved that $|\lambda_i|$ is the degree of F_{i-1} with respect to y_i (for any $i \in \mathbb{Z}_n$). Thus $\lambda_i = 0$ means that the variable y_{i-1} appears in every monomial of F in which y_i appears. Then, if all λ_i vanish, the product of all variables divides the nonzero polynomial F, a contradiction with the fact that F is strict. In the same way, if all λ_i but one vanish, the variable corresponding to the nonzero coefficient divides F, once again a contradiction. $\square$

Theorem 4.2. *The ring of constants $k[Y]^\Delta$ is equal to $k[v]$, where $v = y_0 y_1 \dots, y_{n-1}$.*

Proof. The inclusion $k[v] \subseteq k[Y]^\Delta$ is obvious. We will prove the reverse inclusion. For every Darboux polynomial F of Δ, we denote by $\Lambda(F)$ the cofactor of F. Then we have $\Delta(F) = \Lambda(F) \cdot F$, and $\Lambda(F) = \lambda_0 y_0 + \cdots + \lambda_{n-1} y_{n-1}$, where the coefficients $\lambda_0, \dots, \lambda_{n-1}$ are uniquely determined. In this case we denote by $\Gamma(F)$ the sum $\lambda_0 + \lambda_1 + \cdots + \lambda_{n-1}$. In particular, the variables $y_0, \dots, y_{n-1}$ are Darboux polynomials of Δ, and $\Lambda(y_j) = y_{j+1} - y_j$, $\Gamma(y_j) = 0$, for any $j \in \mathbb{Z}_n$. It follows from Proposition 4.1 that if a Darboux polynomial F is strict and $F \notin k$, then $\Gamma(F)$ is an integer, and $\Gamma(F) \leqslant -2$. Note also that if F, G are Darboux polynomials of Δ, then FG is a Darboux polynomial of Δ, and then

$$\Lambda(FG) = \Lambda(F) + \Lambda(G) \quad \text{and} \quad \Gamma(FG) = \Gamma(F) + \Gamma(G).$$

Assume now that F is a nonzero polynomial belonging to $k[Y]^\Delta$. We will show that $F \in k[v]$. Since the derivation Δ is homogeneous we may assume that F is homogeneous. Thus F is a Darboux polynomial of Δ and its cofactor is equal to 0. Let us write this polynomial in the form

$$F = y_0^{\beta_0} y_1^{\beta_1} \cdots y_{n-1}^{\beta_{n-1}} \cdot G,$$

where $\beta_0, \dots, \beta_{n-1}$ are nonnegative integers, and G is a nonzero polynomial from $K[Y]$ which is not divisible by any of the variables $y_0, \dots, y_{n-1}$ i.e. a strict Darboux polynomial of Δ. Let us suppose that $G \notin k$. Then $\Gamma(G) \leqslant -2$ (by Proposition 4.1), and we have a contradiction:

$$0 = \Gamma(F) = \sum_{j=0}^{n-1} \beta_j \Gamma(y_j) + \Gamma(G) = \sum_{j=0}^{n-1} \beta_j \cdot 0 + \Gamma(G) = \Gamma(G) \leqslant -2.$$

Thus F is a monomial of the form $by^{\beta} = by_0^{\beta_0} y_1^{\beta_1} \cdots y_{n-1}^{\beta_{n-1}}$, with some nonzero $b \in k$. But $\Delta(F) = 0$, so $\beta_0(y_1 - y_0) + \beta_1(y_2 - y_1) + \cdots + \beta_{n-1}(y_0 - y_{n-1}) = 0$, and so $\beta_0 = \beta_1 = \cdots = \beta_{n-1} = c$, for some $c \in \mathbb{N}$.

Now we have $F = by^{\beta} = b(y_0 \cdots y_{n-1})^c = bv^c$, and hence $F \in k[v]$. $\square$

5. The mappings @ and τ

In this section we show that the derivations d and Δ have certain additional properties, and we present some specific relations between these derivations.

Let us fix the following two notations:

$$\underline{a} = \left(\frac{x_1}{x_0}, \frac{x_2}{x_1}, \ldots, \frac{x_{n-1}}{x_{n-2}}, \frac{x_0}{x_{n-1}}\right) \quad \text{and} \quad v = y_0 y_1 \cdots y_{n-1}.$$

We already know, by Proposition 2.11 and Theorem 4.2, that $k(X)^E = k(\underline{a})$ and $k[Y]^{\Delta} = k[v]$.

Lemma 5.1. *Let $F \in k[Y]$. If $F(\underline{a}) = 0$, then there exists a polynomial $G \in k[Y]$ such that $F = (v-1)G$.*

Proof. First note that if $b = (b_0, \ldots, b_{n-1})$ is an element of k^n such that the product $b_0 b_1 \cdots b_{n-1}$ equals 1, then b is of the form $b = \left(\frac{c_1}{c_0}, \frac{c_2}{c_1}, \ldots, \frac{c_{n-1}}{c_{n-2}}, \frac{c_0}{c_{n-1}}\right)$, for some nonzero elements $c_0, \ldots, c_{n-1}$ from k. In fact, put: $c_0 = 1$, $c_1 = b_0$, $c_2 = b_0 b_1, \ldots, c_{n-1} = b_0 b_1 \cdots b_{n-2}$.

Let $P = v - 1$, and let A be the ideal of $\bar{k}[Y] = \bar{k}[y_0, \ldots, y_{n-1}]$ generated by P, where $\bar{k}$ is the algebraic closure of k. Observe that, for any $b \in \bar{k}^n$, if $P(b) = 0$, then (by the assumption and the above note) $F(b) = 0$. This means, by the Nullstellensatz, that some power of F belongs to the ideal A. But A is a prime ideal, so $F \in A$ and so, there exists a polynomial $G \in \bar{k}[Y]$ such that $F = (v-1)G$. Since $F, v-1$ belong to $k[Y]$, it is obvious that G also belongs to $k[Y]$. $\square$

Lemma 5.2. *If F is a nonzero homogeneous polynomial in $k[Y]$, then $F(\underline{a}) \neq 0$.*

Proof. Suppose that $F(\underline{a}) = 0$. Then, by Lemma 5.1, $F = (v-1)G$, for some $G \in k[Y]$. As F is homogeneous, the polynomials $v - 1$ and G are also homogeneous; but it is a contradiction, because $v - 1$ is not homogeneous. $\square$

Let us denote by S the multiplicative subset $\{F \in k[Y];\ F(\underline{a}) \neq 0\}$ and consider the quotient ring

$$\mathcal{A} = S^{-1}k[Y].$$

Every element of this ring is of the form F/G, where $F, G \in k[Y]$ and $G(\underline{a}) \neq 0$. It is a local ring with the unique maximal ideal $I = \left\{\frac{F}{G} \in \mathcal{A};\ F(\underline{a}) = 0\right\}$. It follows from Lemma 5.1 that $I = (v-1)\mathcal{A}$. Observe that $\Delta(\mathcal{A}) \subseteq \mathcal{A}$ and $\Delta(I) \subseteq I$, so Δ is a derivation of $\mathcal{A}$ and I is a differential ideal of $\mathcal{A}$. By Lemma 5.2, every homogeneous element of $k(Y)$ belongs to $\mathcal{A}$.

If $f \in \mathcal{A}$, then $f(\underline{a})$ is well-defined, and it is a homogeneous rational function of degree zero, that is, $f(\underline{a}) \in k(X)^E$. Thus we have a k-algebra homomorphism from $\mathcal{A}$ to $k(X)^E$. This homomorphism we will denote by @. So we have:

$$@ : \mathcal{A} \to k(X)^E, \qquad @(f) = f(\underline{a}) \quad \text{for } f \in \mathcal{A}.$$

In particular, $@(v) = 1$, and $@(y_j) = \frac{x_{j+1}}{x_j}$ for $j \in \mathbb{Z}_n$. These equalities imply that @ is surjective. Note also that $\ker @ = I$, so the field $k(X)^E$ is isomorphic to the factor ring $\mathcal{A}/I$. Moreover, as a consequence of Lemma 5.2 we have:

Proposition 5.3. *If $f \in k(Y)$ is homogeneous and $@(f) = 0$, then $f = 0$.*

Note also the next important proposition.

Proposition 5.4. *$d \circ @ = @ \circ \Delta$, that is, $d(f(\underline{a})) = (\Delta(f))(\underline{a})$ for $f \in \mathcal{A}$.*

Proof. It is enough to prove that the above equality holds in the case when $f = y_j$ with $j \in \mathbb{Z}_n$. Let $f = y_j$, $j \in \mathbb{Z}_n$. Then:

$$d\big(f(\underline{a})\big) = d\left(\frac{x_{j+1}}{x_j}\right) = \frac{d(x_{j+1})x_j - d(x_j)x_{j+1}}{x_j^2} = \frac{x_{j+2}x_j - x_{j+1}^2}{x_j^2} = \frac{x_{j+1}}{x_j}\left(\frac{x_{j+2}}{x_{j+1}} - \frac{x_{j+1}}{x_j}\right)$$
$$= \big(y_j(y_{j+1} - y_j)\big)(\underline{a}) = \big(\Delta(y_j)\big)(\underline{a}) = \big(\Delta(f)\big)(\underline{a}).$$

This completes the proof. □

Corollary 5.5. *Let $f \in \mathcal{A}$. If $\Delta(f) = 0$, then $d(@(f)) = 0$.*

Proof. $d(@(f)) = @(\Delta(f)) = @(0) = 0$ (by Proposition 5.4). □

Now we are ready to prove the following theorem.

Theorem 5.6. *If n is a prime number, then $k(Y)^{\Delta} = k(v)$, where $v = y_0 y_1 \cdots y_{n-1}$.*

Proof. Put $P = v - 1$. Note that $\Delta(P) = 0$. Let $0 \neq f = \frac{F}{G} \in k(Y)$, where F, G are nonzero, coprime polynomials in $k[Y]$, and assume that $\Delta(f) = 0$. We will show, using an induction with respect to $\deg F + \deg G$, that $f \in k(v)$.

If $\deg F + \deg G = 0$, then $f \in k$, so $f \in k(v)$. Assume that $\deg F + \deg G = r > 0$.

If P divides F, then $F = F'P$, for some $F' \in k[Y]$, and then $\Delta\big(\frac{F'}{G}\big) = \frac{1}{P}\Delta\big(\frac{F}{G}\big) = 0$ with $\deg F' + \deg G < r$. Then, by induction, $\frac{F'}{G} \in k(v)$ and this implies that $\frac{F}{G} \in k$, because $\frac{F}{G} = P\frac{F'}{G}$ and $P \in k(v)$. We use the same argument in the case when P divides G.

Now we may assume that $P \nmid F$ and $P \nmid G$. In this case, by Lemma 5.1, the quotient $\frac{F}{G}$ belongs to $\mathcal{A}$, and $@\big(\frac{F}{G}\big) \neq 0$. Moreover, we may assume that $\deg F \geqslant \deg G$ (in the opposite case we consider G/F instead of F/G).

Since $\Delta(f) = 0$, we have (by Corollary 5.5) $@(f) \in k(X)^d \cap k(X)^E = k(X)^{d,E}$. But n is prime so, by Corollary 2.14, $k(X)^{d,E} = k$. Therefore, $@\big(\frac{F}{G}\big) = c$, for some nonzero $c \in k$. Thus we have

$$0 = @\left(\frac{F}{G}\right) - c = @\left(\frac{F}{G} - c\right) = @\left(\frac{F - cG}{G}\right) = \frac{@(F - cG)}{@(G)},$$

and hence, $@(F - cG) = 0$. If $F - cG = 0$, then $\frac{F}{G} = c \in k(v)$. Assume that $F - cG \neq 0$. Then, by Lemma 5.1, $F - cG = H \cdot P$, for some nonzero $H \in k[Y]$. As $\gcd(F, G) = 1$, we have $\gcd(H, G) = 1$. Observe that $\Delta\big(\frac{H}{G}\big) = 0$. In fact, $\Delta\big(\frac{H}{G}\big) = \frac{1}{P}\Delta\big(\frac{PH}{G}\big) = \frac{1}{P}\Delta\big(\frac{F-cG}{G}\big) = \frac{1}{P}\Delta\big(\frac{F}{G} - c\big) = \frac{1}{P}\Delta\big(\frac{F}{G}\big) = 0$. Since $\deg F \geqslant \deg F$ and $\deg P > 0$, we have $\deg F \geqslant \deg(F - cG) = \deg HP > \deg H$, and so (by induction) the quotient $\frac{H}{G}$ belongs to $k(v)$. But

$$f = \frac{F}{G} = \left(\frac{F}{G} - c\right) + c = \frac{F - cG}{G} + c = P\frac{H}{G} + c,$$

so $f \in k(v)$. We have proved that $k(Y)^{\Delta} \subseteq k(v)$. The reverse inclusion is obvious. □

Let us recall (see Theorem 4.2), that the ring of constants $k[Y]^{\Delta}$ is always equal to $k[v]$. Thus, if n is prime, then $k(Y)^{\Delta}$ is the field of quotients of $k[Y]^{\Delta}$. In a general case a similar statement is not true. For example, if $n=4$, then the rational function

$$y_1 y_3 \frac{2y_0y_2 - y_2y_3 - y_0y_1}{y_1y_2 + y_0y_3 - 2y_1y_3}$$

belongs to $k(Y)^{\Delta}$ and it is not in $k(v)$. We will check it later in Example 7.2.

Let us recall (see Section 1) that τ is an automorphism of $k(X)$ defined by

$$\tau(x_j) = \varepsilon^j x_j \quad \text{for all } j \in \mathbb{Z}_n.$$

We say that a rational function $f \in k(X)$ is *τ-homogeneous*, if f is homogeneous in the ordinary sense and $\tau(f) = \varepsilon^s f$ for some $s \in \mathbb{Z}_n$. In this case we say that s is the τ-degree of f and we write $\deg_\tau(f) = s$. Note that $\deg_\tau(f)$ is an element of $\mathbb{Z}_n$.

Let $\alpha = (\alpha_0, \dots, \alpha_{n-1}) \in \mathbb{Z}^n$. As usual, we denote by x^α the rational monomial $x_0^{\alpha_0} \cdots x_{n-1}^{\alpha_{n-1}}$, and by $|\alpha|$ the sum $\alpha_0 + \cdots + \alpha_{n-1}$. Moreover, we denote by $\sigma(\alpha)$ the element from $\mathbb{Z}_n$ defined by

$$\sigma(\alpha) = 0\alpha_0 + 1\alpha_1 + 2\alpha_2 + \cdots + (n-1)\alpha_{n-1} \pmod{n}.$$

Let us recall (see Section 1) that $\varrho : k(X) \to k(X)$ is a field automorphism, defined by $\varrho(x_j) = x_{j+1}$ for all $j \in \mathbb{Z}_n$. It is very easy to check that:

Lemma 5.7. *Every rational monomial x^α, where $\alpha \in \mathbb{Z}^n$, is τ-homogeneous and its τ-degree is equal to $\sigma(\alpha)$. Moreover, if $0 \neq f \in k(X)$ and f is τ-homogeneous, then $\varrho(f)$ is also τ-homogeneous, and $\deg_\tau \varrho(f) \equiv \deg_\tau f + \deg f \pmod{n}$.*

The derivation d has the following additional properties.

Lemma 5.8. *$\tau d \tau^{-1} = \varepsilon d$.*

Proof. It is enough to show that $\tau d(x_j) = \varepsilon d(\tau(x_j))$ for $j \in \mathbb{Z}_n$. Let us verify: $\tau d(x_j) = \tau(x_{j+1}) = \varepsilon^{j+1} x_{j+1} = \varepsilon \cdot \varepsilon^j d(x_j) = \varepsilon d(\varepsilon^j x_j) = \varepsilon d(\tau(x_j))$. $\square$

Lemma 5.9. *Let $f \in k(X)$. If f is τ-homogeneous, then $d(f)$ is τ-homogeneous and $\deg_\tau d(f) = 1 + \deg_\tau f$.*

Proof. Assume that f is τ-homogeneous and $s = \deg_\tau f$. Since the derivation d is homogeneous and f is homogeneous in the ordinary sense, $d(f)$ is also homogeneous in the ordinary sense. Moreover, by the previous proposition, we have: $\tau(d(f)) = \varepsilon d(\tau(f)) = \varepsilon d(\varepsilon^s f) = \varepsilon^{s+1} d(f)$, so $d(f)$ is τ-homogeneous and $\deg_\tau d(f) = s+1$. $\square$

Proposition 5.10. *Let $F \in k[X]$ be a Darboux polynomial of d. If F is τ-homogeneous, then $d(F) = 0$.*

Proof. Assume that $d(F) = bF$ with $b \in k[X]$, F is homogeneous in the ordinary sense, and $\tau(F) = \varepsilon^s F$ for some $s \in \mathbb{Z}_n$. Then $b \in k$, and we have $\varepsilon d(F) = \varepsilon^{-s} \varepsilon d(\varepsilon^s F) = \varepsilon^{-s} \varepsilon d(\tau(F)) = \varepsilon^{-s} \tau(d(F)) = \varepsilon^{-s} \tau(bF) = b\varepsilon^{-s} \tau(F) = b\varepsilon^{-s} \varepsilon^s F = bF = d(F)$. Hence, $(\varepsilon - 1) d(F) = 0$. But $\varepsilon \neq 1$, so $d(F) = 0$. $\square$

Proposition 5.11. *Let $f = \frac{P}{Q}$, where P, Q are nonzero coprime polynomials in $k[X]$. If f is τ-homogeneous, then P, Q are also τ-homogeneous, and $\deg_\tau f = \deg_\tau P - \deg_\tau Q$. Moreover, if f is τ-homogeneous and $d(f) = 0$, then $d(P) = d(Q) = 0$.*

Proof. Assume that f is τ homogeneous and $\deg_\tau f = s$. Then f is homogeneous in the ordinary sense and then, by Proposition 2.10, the polynomials P, Q are also homogeneous in the ordinary sense. Since $\tau\big(\frac{P}{Q}\big) = \varepsilon^s \frac{P}{Q}$, we have $\tau(P)Q = \varepsilon^s P\tau(Q)$ and this implies that $\tau(P) = aP$, $\tau(Q) = bQ$, for some $a, b \in k[X]$ (because P, Q are relatively prime). Comparing degrees, we deduce that $a, b \in k \smallsetminus \{0\}$. But τ^n is the identity map, so $P = \tau^n(P) = a^n P$ and $Q = \tau^n(Q) = b^n Q$ and so, a, b are n-th roots of unity. Since ε is a primitive n-root, we have $a = \varepsilon^{s_1}$, $b = \varepsilon^{s_2}$, for some $s_1, s_2 \in \mathbb{Z}_n$. Thus, the polynomials P, Q are τ-homogeneous, and it is clear that $s \equiv s_1 - s_2 \pmod n$.

Assume now that f is τ-homogeneous and $d(f) = 0$. Then P, Q are τ-homogeneous Darboux polynomials of d (with the same cofactor) and, by Proposition 5.10, we have $d(P) = d(Q) = 0$. $\square$

Note also the following proposition.

Proposition 5.12. *If $f \in k(Y)$ is homogeneous, then $@(f)$ is τ-homogeneous, and $\deg_\tau @(f) \equiv \deg f \pmod n$.*

Proof. First assume that $f = F$ is a nonzero homogeneous polynomial in $k[Y]$ of degree s and consider all the monomial of F. Every nonzero monomial is of the form by^α, where $0 \neq b \in k$, and $\alpha \in \mathbb{N}^n$ with $|\alpha| = s$. For each such y^α, we have $@(y^\alpha) = x^\beta$, where $\beta = (\beta_0, \dots, \beta_{n-1}) = (\alpha_{n-1} - \alpha_0, \alpha_0 - \alpha_1, \alpha_1 - \alpha_2, \dots, \alpha_{n-2} - \alpha_{n-1})$, and then

$$\sigma(\beta) = \sum_{j=0}^{n-1} j\beta_j = |\alpha| - n\alpha_{n-1} = s - n\alpha_{n-1},$$

so $\sigma(\beta) \equiv s \pmod n$. This means that $\tau(x^\beta) = \varepsilon^s x^\beta$. Thus, for every nonzero monomial P which appears in F, we have $\tau(@(P)) = \varepsilon^s @(P)$. This implies that $\tau(@(f)) = \varepsilon^s @(f)$. But $@(F)$ is also homogeneous in the ordinary sense (because $@(F) \in k(X)^E$), so $@(F)$ is τ-homogeneous, and $\deg_\tau @(F) = \deg F \pmod n$.

Now let $0 \neq f \in k(Y)$ be an arbitrary homogeneous rational function. Let $f = \frac{F}{G}$ with $F, G \in k[Y] \smallsetminus \{0\}$ and $\gcd(F, G) = 1$. Then F, G are homogeneous (by Proposition 2.10), and $@(f) = \frac{@(F)}{@(G)}$. Thus, by the above proof for polynomials, $@(f)$ is τ-homogeneous, and $\deg_\tau @(f) \equiv \deg f \pmod n$. $\square$

Proposition 5.13. *Let $f, g \in k(Y)$ be homogeneous rational functions. If $@(f) = @(g)$, then $f = v^c g$, for some $c \in \mathbb{Z}$.*

Proof. Assume that $@(f) = @(g)$. Then, by Proposition 5.12, $\deg f \equiv \deg_\tau @(f) = \deg_\tau @(g) \equiv \deg g \pmod n$, so there exists $c \in \mathbb{Z}$ such that $\deg f = nc + \deg g$. Then f and $v^c g$ are homogeneous of the same degree, so $f - v^c g$ is homogeneous. Observe that $@(f - v^c g) = @(f) - @(v)^c @(g) = @(f) - @(g) = 0$. Hence, by Proposition 5.3, we have $f = v^c g$. $\square$

Let us assume that g is a τ-homogeneous rational function belonging to the field $k(X)^{d,E}$. We will show that then there exists a homogeneous (in the ordinary sense) rational function $f \in k(Y)$ such that $\Delta(f) = 0$ and $@(f) = g$. This fact will play a key role in our description of the structure of the field $k(Y)^\Delta$. For a proof of this fact we need to prove some lemmas and propositions.

Let us recall from Section 1, that the elements $e_0, \dots, e_{n-1} \in \mathbb{Z}^n$ are defined by: $e_0 = (1, 0, 0, \dots, 0)$, $e_1 = (0, 1, 0, \dots, 0)$, $\dots$, $e_{n-1} = (0, 0, \dots, 0, 1)$. In particular, we have

$$@(y_j) = \frac{x_{j+1}}{x_j} = x^{e_{j+1} - e_j}, \quad \text{for } j \in \mathbb{Z}_n.$$

Lemma 5.14. *Let $\alpha \in \mathbb{Z}^n$. Assume that $|\alpha| = 0$ and $\sigma(\alpha) = 0 \pmod n$. Then there exists a sequence $\beta = (\beta_0, \dots, \beta_{n-1}) \in \mathbb{Z}^n$ such that $|\beta| = 0$ and $\alpha = \sum_{j=0}^{n-1} \beta_j(e_{j+1} - e_j)$.*

Proof. Since $\sigma(\alpha) \equiv 0 \pmod{n}$, there exists an integer r such that $n\alpha_0 + \sigma(\alpha) = -rn$. Put: $\beta_0 = r$ and $\beta_j = r - \sum_{i=1}^{j} \alpha_i$, for $j = 1, \dots, n-1$. $\square$

Lemma 5.15. *If $\alpha \in \mathbb{Z}^n$ with $|\alpha| = 0$, then there exists $\beta \in \mathbb{Z}^n$ such that $@(y^\beta) = x^\alpha$.*

Proof. Put: $\beta_j = \sum_{i=j+1}^{n-2} \alpha_i$ for $j = 0, 1, \dots, n-3$, and $\beta_{n-2} = 0$, $\beta_{n-1} = -\alpha_{n-1}$. $\square$

Now we assume that P is a fixed nonzero τ-homogeneous polynomial in $k[X]$. Let us write this polynomial in the form

$$P = c_1 x^{\gamma_1} + \dots + c_r x^{\gamma_r},$$

where $c_1, \dots, c_r$ are nonzero elements of k, and $\gamma_1, \dots, \gamma_r \in \mathbb{N}^n$. For every $q \in \{1, \dots, r\}$, we have $|\gamma_q| = \deg F$ and $\sigma(\gamma_q) \equiv \deg_\tau F \pmod{n}$, and hence, $|\gamma_q - \gamma_1| = 0$ and $\sigma(\gamma_q - \gamma_1) \equiv 0 \pmod{n}$. This implies, by Lemma 5.14, that for any $q \in \{1, \dots, r\}$, there exists a sequence $\beta^{(q)} = (\beta_0^{(q)}, \dots, \beta_{n-1}^{(q)}) \in \mathbb{Z}^n$ such that $|\beta^{(q)}| = 0$ and

$$\gamma_q - \gamma_1 = \sum_{j=0}^{n-1} \beta_j^{(q)} (e_{j+1} - e_j).$$

For each $j \in \{0, 1, \dots, n-1\}$, we define:

$$\alpha_j = \min\{\beta_j^{(1)}, \beta_j^{(2)}, \dots, \beta_j^{(r)}\},$$

and we denote by λ the sequence $(\lambda_0, \dots, \lambda_{n-1}) \in \mathbb{Z}^n$ defined by

$$\lambda = \gamma_1 + \sum_{j=0}^{n-1} \alpha_j (e_{j+1} - e_j).$$

Observe that $|\lambda| = |\gamma_1| = \deg P$, and $\gamma_q = \lambda + \sum_{j=0}^{n-1} (\beta_j^{(q)} - \alpha_j)(e_{j+1} - e_j)$ for any $q \in \{1, \dots, r\}$, and moreover, each $\beta_j^{(q)} - \alpha_j$ is a nonnegative integer. Put $a_{qj} = \beta_j^{(q)} - \alpha_j$, for $j \in \mathbb{Z}_n$, $q \in \{1, \dots, r\}$, and $a_q = (a_{q0}, a_{q1}, \dots, a_{q(n-1)})$ for all $q = 1, \dots, r$. Then each a_q belongs to $\mathbb{N}^n$, and we have the equalities

$$\gamma_q = \lambda + \sum_{j=0}^{n-1} a_{qj} (e_{j+1} - e_j), \quad \text{for any } q \in \{1, \dots, r\}.$$

Let us remark that $\lambda \in \mathbb{N}^n$. Indeed, for any $j \in \mathbb{Z}_n$, we have $\lambda_j = \gamma_{1j} + \alpha_{j-1} - \alpha_j$, where $\alpha_{j-1} = \beta_{j-1}^{(q)}$ for some q and $\alpha_j \leqslant \beta_j^{(q)}$. Thus $\lambda_j = \gamma_{1j} + \beta_{j-1}^{(q)} - \alpha_j \geqslant \gamma_{1j} + \beta_{j-1}^{(q)} - \beta_j^{(q)} = \gamma_{qj} \geqslant 0$. Moreover, $|a_q| = |\beta^{(q)} - \alpha| = |\beta^{(q)}| - |\alpha| = -|\alpha|$, because $|\beta^{(q)}| = 0$. This means that $|\alpha| \leqslant 0$, and all the numbers $|a_1|, \dots, |a_r|$ are the same; they are equal to $-|\alpha|$. Consider the polynomial in $k[Y]$ defined by

$$\overline{P} = c_1 y^{a_1} + \dots + c_r y^{a_r}.$$

It is a nonzero homogeneous (in the ordinary sense) polynomial of degree $-|\alpha|$. It is easy to check that $@(\overline{P}) = x^{-\lambda} P$. Thus, we proved the following proposition.

Proposition 5.16. *If $P \in k[X]$ is a nonzero τ-homogeneous polynomial, then there exist a sequence $\lambda \in \mathbb{Z}^n$ and a homogeneous polynomial $\overline{P} \in k[Y]$ such that $@(\overline{P}) = x^{-\lambda} P$ and $|\lambda| = \deg P$.*

Remark 5.17. In the above construction, the polynomial $\overline{P}$ is not divisible by any of the variables $y_0, \dots, y_n$. Let us additionally assume that $d(P) = 0$. Then it is not difficult to show that $\Delta(\overline{P}) = -(\lambda_0 y_0 + \cdots + \lambda_{n-1} y_{n-1})\overline{P}$, that is, $\overline{P}$ is a strict Darboux polynomial of Δ and its cofactor is equal to $-\sum \lambda_i y_i$. This implies, by Proposition 4.1, that if additionally $d(P) = 0$, among all nonnegative numbers $\lambda_0, \dots, \lambda_{n-1}$, at least two are different from zero.

Now we are ready to prove the following, mentioned above, proposition.

Proposition 5.18. *Let g be a τ-homogeneous rational function belonging to the field $k(X)^{d,E}$. Then there exists a homogeneous rational function $f \in k(Y)$ such that $\Delta(f) = 0$ and $@(f) = g$.*

Proof. For $g = 0$ it is obvious. Assume that $g \neq 0$, and let $g = \frac{P}{Q}$, where $P, Q \in k[X] \setminus \{0\}$ with $\gcd(P, Q) = 1$. It follows from Propositions 2.10 and 5.11, that the polynomials P, Q are homogeneous (in the ordinary sense) of the same degree, and they are also τ-homogeneous. By Proposition 5.16, there exist sequences $\lambda, \mu \in \mathbb{Z}^n$ and a homogeneous polynomials $\overline{P}, \overline{Q} \in k[Y]$ such that $@(\overline{P}) = x^{-\lambda} P$, $@(\overline{Q}) = x^{-\mu} Q$, and $|\lambda| = |\mu| = \deg P = \deg Q$. Then we have

$$g = \frac{P}{Q} = \frac{x^{\lambda}(x^{-\lambda} P)}{x^{\mu}(x^{-\mu} Q)} = \frac{x^{\lambda} @(\overline{P})}{x^{\mu} @(\overline{Q})} = x^{\lambda-\mu} @(\overline{P}/\overline{Q}).$$

Since $|\lambda - \mu| = 0$, there exists (by Lemma 5.15) $\beta \in \mathbb{Z}^n$ such that $@(y^{\beta}) = x^{\lambda-\mu}$. Put $f = y^{\beta} \cdot \overline{P}/\overline{Q}$. Then $f \in k(Y)$ is a homogeneous rational function, and $@(f) = g$. Now we will show that $\Delta(f) = 0$. To this aim let us recall that g belongs to the field $k(X)^{d,E}$, so $d(g) = 0$. This implies that $@(\Delta(f)) = 0$, because (by Proposition 5.4) $@(\Delta(f)) = d(@(f)) = d(g) = 0$. But the rational function $\Delta(f)$ is homogeneous, so by Proposition 5.3, $\Delta(f) = 0$. $\square$

6. Rational constants of Δ

We proved (see Proposition 2.13) that $k(X)^{d,E} = k(g_1, \dots, g_{m-1})$, where $m = n - \varphi(n)$, and $g_1, \dots, g_{m-1} \in k(X)$ are some algebraically independent homogeneous rational functions of degree 0. We proved in fact, that each g_j (for $j = 1, \dots, m-1$) is equal to the quotient $\frac{w_j}{w_0}$. These quotients are usually not τ-homogeneous. We will show in the next section that, in some cases, we are ready to find such algebraically independent generators of $k(X)^{d,E}$ which are additionally τ-homogeneous. In this section we prove that if we have τ-homogeneous generators of $k(X)^{d,E}$, then we may construct some algebraically independent generators of the field $k(Y)^{\Delta}$.

Let us assume that $k(X)^{d,E} = k(g_1, \dots, g_{m-1})$, where $g_1, \dots, g_{m-1} \in k(X)$ are algebraically independent τ-homogeneous rational functions. We know, by Proposition 5.18, that for each g_j there exists a homogeneous rational function $f_j \in k(Y)$ such that $\Delta(f_j) = 0$ and $@(f_j) = g_j$. Thus we have homogeneous rational functions $f_1, \dots, f_{m-1}$, belonging to the field $k(Y)^{\Delta}$. We know also that $v \in k(Y)^{\Delta}$, where $v = y_0 y_1 \cdots y_{n-1}$. In this section we will prove the following theorem.

Theorem 6.1. *Let $g_1, \dots, g_{m-1}$ and $v, f_1, \dots, f_{m-1}$ be as above. Then the elements $v, f_1, \dots, f_{m-1}$ are algebraically independent over k, and $k(Y)^{\Delta} = k(v, f_1, \dots, f_{m-1})$.*

We will prove it in several steps.

Step 1. *The elements $f_1, \dots, f_{m-1}$ are algebraically independent over k.*

Proof. Suppose that $W(f_1,\dots,f_{m-1})=0$ for some $W\in k[t_1,\dots,t_{m-1}]$. Then

$$0=@\big(W(f_1,\dots,f_{m_1})\big)=W\big(@(f_1),\dots,@(f_{m-1})\big)=W(g_1,\dots,g_{m-1}).$$

But $g_1,\dots,g_{m-1}$ are algebraically independent, so $W=0$. $\square$

In the next steps we write f instead of $\{f_1,\dots,f_{m-1}\}$, and g instead of $\{g_1,\dots,g_{m-1}\}$. In particular, $k(f)$ means $k(f_1,\dots,f_{m-1})$.

Step 2. $v\notin k(f)$.

Proof. Suppose that $v\in k(f)$. Let $v=P(f)/Q(f)$ for some $P,Q\in k[t_1,\dots,t_{m-1}]$. Then $Q(f)v-P(f)=0$ and we have $0=@(Q(f)v-P(f))=Q(g)@(v)-P(g)$. But $@(v)=1$, so $P(g)=Q(g)$, and so $P=Q$, because $g_1,\dots,g_{m-1}$ are algebraically independent. Thus $v=P(f)/Q(f)=P(f)/P(f)=1$; a contradiction. $\square$

Step 3. *The elements $v,f_1,\dots,f_{m-1}$ are algebraically independent over k.*

Proof. We already know (by Step 1) that $f_1,\dots,f_{m-1}$ are algebraically independent. Suppose that v is algebraic over $k(f)$. Let $F(t)=b_rt^r+\cdots+b_1t+b_0\in k(f)[t]$ (with $b_r\neq 0$) be the minimal polynomial of v over $k(f)$. Multiplying by the common denominator, we may assume that the coefficients $b_0,\dots,b_r$ belong to the ring $k[f]$. There exist polynomials $B_0,B_1,\dots,B_r\in k[t_1,\dots,t_{m-1}]$ such that $b_j=B_j(f)$ for all $j=0,\dots,r$. Thus, $B_r(f)v^r+\cdots+B_1(f)v+B_0(f)=0$. Using @, we obtain the equality

$$B_r(g)1^r+\cdots+B_1(g)1+B_0(g)=0,$$

which implies that $B_r+\cdots+B_1+B_0=0$, because $g_1,\dots,g_{m-1}$ are algebraically independent over k. This means, in particular, that $F(1)=0$. But $F(t)$ is an irreducible polynomial of degree $r\geqslant 1$, so $r=1$. Hence, $B_1(f)v+B_0(f)=0$, $B_1(f)\neq 0$, and hence $v=-B_0(f)/B_1(f)\in k(f)$; a contradiction with Step 2. $\square$

It is clear that $k(v,f)\subseteq k(Y)^{\Delta}$. For a proof of Theorem 6.1 we must show that the reverse inclusion also holds. Note that the derivation Δ is homogeneous, so it is well known that its field of constants is generated by some homogeneous rational functions. Hence for a proof of this theorem it suffices to prove that every homogeneous element of $k(Y)^{\Delta}$ is an element of $k(v,f)=k(v,f_1,\dots,f_{m-1})$.

Let us assume that H is a nonzero homogeneous rational function belonging to $k(Y)^{\Delta}$, and put $h=@(H)$.

Step 4. *$h\in k(g)$ and h is τ-homogeneous.*

Proof. Since $h=@(H)$, we have $h\in k(X)^E$. Moreover, $d(h)=d(@(H))=@(\Delta(H))=@(0)=0$, so $h\in k(X)^d\cap k(X)^E=k(X)^{d,E}=k(g)$. The τ-homogeneity of h follows from Proposition 5.12. $\square$

Now we introduce some new notations. The τ-degrees of $g_1,\dots,g_{m-1}$ we denote by $s_1,\dots,s_{m-1}$, respectively, and by s we denote the τ-degree of h. Thus we have $\tau(g_j)=\varepsilon^{s_j}g_j$ for $j=1,\dots,m-1$, and $\tau(h)=\varepsilon^s h$. We already know that $h\in k(g)$, so we have

$$h=\frac{A(g)}{B(g)}$$

for some relatively prime nonzero polynomials $A,B\in k[t_1,\dots,t_{m-1}]$.

Step 5. *The elements $A(g)$, $B(g)$ are τ-homogeneous.*

Proof. Since $\tau(h) = \varepsilon^s h$, we have $\tau(A(g)) \cdot B(g) = \varepsilon^s A(g) \cdot \tau(B(g))$, that is,

$$A\big(\varepsilon^{s_1} g_1, \ldots, \varepsilon^{s_{m-1}} g_{m-1}\big) \cdot B(g_1, \ldots, g_{m-1}) = \varepsilon^s A(g_1, \ldots, g_{m-1}) \cdot B\big(\varepsilon^{s_1} g_1, \ldots, \varepsilon^{s_{m-1}} g_{m-1}\big).$$

But the elements $g_1, \ldots, g_{m-1}$ are algebraically independent over k, so in the polynomial ring $k[t_1, \ldots, t_{m-1}]$ we have the equality

$$A\big(\varepsilon^{s_1} t_1, \ldots, \varepsilon^{s_{m-1}} t_{m-1}\big) \cdot B = \varepsilon^s A \cdot B\big(\varepsilon^{s_1} t_1, \ldots, \varepsilon^{s_{m-1}} t_{m-1}\big),$$

which implies that $A(\varepsilon^{s_1} t_1, \ldots, \varepsilon^{s_{m-1}} t_{m-1}) = pA$ and $B(\varepsilon^{s_1} t_1, \ldots, \varepsilon^{s_{m-1}} t_{m-1}) = qB$, for some $p, q \in k[t_1, \ldots, t_{m-1}]$ (because we assumed that $\gcd(A, B) = 1$). Comparing degrees we deduce that $p, q \in k$. Therefore, $\tau(A(g)) = A(\tau(g_1, \ldots, \tau(g_{m-1}))) = A(\varepsilon^{s_1} g_1, \ldots, \varepsilon^{s_{m-1}} g_{m-1}) = pA(g_1, \ldots, g_{m-1}) = pA(g)$, so, $\tau(A(g)) = pA(g)$, and similarly $\tau(B(g)) = qB(g)$. But τ^n is the identity map, so $p^n = q^n = 1$ and so, p, q are n-th roots of unity. Put $p = \varepsilon^a$ and $q = \varepsilon^b$, where $a, b \in \mathbb{Z}_n$. Then we have $\tau(A(g)) = \varepsilon^a A(g)$ and $\tau(B(g)) = \varepsilon^b B(g)$. Moreover, $A(g)$, $B(g)$ are homogeneous in the ordinary sense, because they belong to $k(X)^E$, so they are homogeneous rational functions of degree zero. This means that $A(g)$, $B(g)$ are τ-homogeneous. $\square$

Let us fix: $a = \deg_\tau A(g)$ and $b = \deg_\tau B(g)$.

If $\alpha = (\alpha_1, \ldots, \alpha_{m-1}) \in \mathbb{N}^{m-1}$ then, as usual, we denote by t^α and g^α the elements $t_1^{\alpha_1} \cdots t_{m-1}^{\alpha_{m-1}}$ and $g_1^{\alpha_1} \cdots g_{m-1}^{\alpha_{m-1}}$, respectively, and moreover, we denote:

$$\begin{aligned} w(\alpha) &= \alpha_1 s_1 + \cdots + \alpha_{m-1} s_{m-1}, \\ u(\alpha) &= \alpha_1 \deg f_1 + \cdots + \alpha_{m-1} \deg f_{m-1}. \end{aligned}$$

Recall that $s_j = \deg_\tau(g_j)$ and $@(f_j) = g_j$, for all $j = 1, \ldots, m-1$. It follows from Proposition 5.12 that for each j we have the congruence $s_j \equiv \deg f_j \pmod n$. Therefore,

$$u(\alpha) \equiv w(\alpha) \pmod n \quad \text{for all } \alpha \in \mathbb{N}^{n-1}.$$

Let us write the polynomials A, B in the forms

$$A = \sum_{\alpha \in S_A} A_\alpha t^\alpha, \qquad B = \sum_{\beta \in S_B} B_\beta t^\beta,$$

where A_α, B_β are nonzero elements of k, and S_A, S_B are finite subsets of $\mathbb{N}^{m-1}$.

Step 6. $w(\alpha) \equiv a \pmod n$ *for all* $\alpha \in S_A$, *and* $w(\beta) \equiv b \pmod n$ *for all* $\beta \in S_B$.

Proof. Since $\tau(A(g)) = \varepsilon^a A(g)$, we have

$$\begin{aligned} \varepsilon^a \sum A_\alpha g^\alpha = \varepsilon^a A(g) = \tau\big(A(g)\big) &= \sum A_\alpha \tau\big(t^\alpha\big) \\ &= \sum A_\alpha \big(\varepsilon^{s_1} g_1\big)^{\alpha_1} \cdots \big(\varepsilon^{s_{m-1}} g_{m-1}\big)^{\alpha_{m-1}} \\ &= \sum A_\alpha \varepsilon^{w(\alpha)} g^\alpha. \end{aligned}$$

Hence, $\sum A_\alpha(\varepsilon^a - \varepsilon^{w(\alpha)})g^\alpha = 0$. But $g_1, \dots, g_{m-1}$ are algebraically independent and each A_α is nonzero, so $\varepsilon^{w(\alpha)} = \varepsilon^a$ and consequently $w(\alpha) \equiv a \pmod{n}$, for all $\alpha \in S_A$. We do the same for the elements $w(\beta)$. □

Since $u(\alpha) \equiv w(\alpha) \pmod{n}$ for all $\alpha \in \mathbb{N}^{m-1}$, it follows from the above step that, for each $\alpha \in S_A$, there exists $p(\alpha) \in \mathbb{Z}$ such that $u(\alpha) = a + p(\alpha)n$. Put

$$p = \max\bigl(\{0\} \cup \bigl\{p(\alpha);\ \alpha \in S_A\bigr\}\bigr),$$

and put $a(\alpha) = p - p(\alpha)$ for $\alpha \in S_A$. Then all $a(\alpha)$ are nonnegative integers and all the numbers $u(\alpha) + a(\alpha)n$, for each $\alpha \in S_A$, are the same; they are equal to $a + pn$.

A similar procedure we do with elements of S_B. For each $\beta \in S_B$ there exists an integer $b(\beta)$ such that $u(\beta) + b(\beta)n = b + qn$, for all $\beta \in S_B$, where q is a nonnegative integer. Consider now the following quotient

$$\Theta = \frac{\sum_{\alpha \in S_A} A_\alpha f^\alpha v^{a(\alpha)}}{\sum_{\beta \in S_B} B_\beta f^\beta v^{b(\beta)}}.$$

This quotient belongs of course to $k(v, f_1, \dots, f_{n-1})$. In its numerator each component $A_\alpha f^\alpha v^{a(\alpha)}$, for all $\alpha \in S_A$, is a homogeneous rational function of the same degree $a + pn$, so the numerator is homogeneous. By the same way we see that the denominator is also homogeneous. Hence, Θ is a homogeneous rational function. Observe that $@(\Theta) = h$. We have also $@(H) = h$. Thus, H and Θ are two homogeneous rational functions such that $@(H) = @(\Theta)$. By Proposition 5.13, there exists an integer c such that $H = v^c \cdot \Theta$. Therefore, $H \in k(v, f_1, \dots, f_{n-1})$. This completes our proof of Theorem 6.1. □

7. Two special cases

In this section we present a description of the field $k(Y)^\Delta$ in the case when n is a power of a prime number, and in the case when n is a product of two primes.

Let $n = p^s$, where p is prime and $s \geqslant 1$. We already know, by Theorem 5.6, that if $s = 1$, then $k(Y)^\Delta = k(v)$. Now we assume that $s \geqslant 2$.

Theorem 7.1. *Assume that $n = p^s$ for some prime number p and an integer $s \geqslant 2$. Then, there exist homogeneous elements $f_1, \dots, f_{m-1}$ of $k(Y)^\Delta$ such that $v, f_1, \dots, f_{m-1}$ are algebraically independent over k and*

$$k(Y)^\Delta = k(v, f_1, \dots, f_{m-1}),$$

where $m = p^{s-1}$ and $v = y_0 \cdots y_{n-1}$.

Proof. In this case $m = n - \varphi(n) = p^s - \varphi(p^s) = p^{s-1}$ and hence, $n = pm$. Since $\Phi_{p^s}(t) = 1 + t^m + t^{2m} + \dots + t^{(p-1)m}$, we have: $w_0 = u_0 u_m u_{2m} \cdots u_{(p-1)m}$, and $w_j = u_{0m+j} u_{1m+j} u_{2m+j} \cdots u_{(p-1)m+j}$, for all $j = 0, 1, \dots, m-1$. Recall (see Lemma 1.1) that $\tau(u_j) = u_{j+1}$ for $j \in \mathbb{Z}_n$, so each w_j is equal to $\tau^j(w_0)$.

Observe that $\tau^m(w_0) = w_0$. This implies that the τ-degree of every nonzero monomial (with respect to variables $x_0, \dots, x_{n-1}$) of w_0 is divisible by p. This means that in the τ-decomposition of w_0 there are only components with τ-degrees $0, p, 2p, \dots, (m-1)p$. Let $w_0 = v_0 + v_1 + \dots + v_{m-1}$, where each $v_j \in k[X]$ is τ-homogeneous and $\tau(v_j) = \varepsilon^{pj} v_j$. Of course $d(v_j) = 0$ for all j (because $\tau d = \varepsilon d \tau$), and $\deg(v_j) = p$ for all j (by Proposition 2.7). Now observe that if $p \geqslant 3$ then $\varrho(w_0) = w_0$, and if $p = 2$ then $\varrho(w_0) = -w_0$. Hence $\varrho(w_0) = u w_0$ for some $u = \pm 1$ in any case and we have

$$v_0 + v_1 + \dots + v_{m-1} = w_0 = u\varrho(w_0) = u\bigl(\varrho(v_0) + \varrho(v_1) + \dots + \varrho(v_{m-1})\bigr).$$

Since the τ-decomposition of w_0 is unique, we deduce (by Lemma 5.7), that

$$v_1 = u\varrho(v_0), \quad v_2 = u\varrho(v_1), \quad \ldots, \quad v_{m-1} = u\varrho(v_{m-2}), \quad v_0 = u\varrho(v_{m-1}),$$

and we have $v_j = u^j\varrho^j(v_0)$ for all $j = 0, 1, \ldots, m-1$. Therefore, the τ-decomposition of w_0 is of the form $w_0 = v_0 + u^1\varrho(v_0) + u^2\varrho^2(v_0) + \cdots + u^{m-1}\varrho^{m-1}(v_0)$. This implies that

$$w_1 = \tau(w_0) = v_0 + u^1\varepsilon^p\varrho(v_0) + u^2\varepsilon^{2p}\varrho^2(v_0) + \cdots + u^{m-1}\varepsilon^{(m-1)p}\varrho^{m-1}(v_0).$$

We do the same for $w_2 = \tau(w_1) = \tau^2(w_0)$, and for all w_j. Thus, for all $j = 0, 1, \ldots, m-1$, we have $w_j = v_0 + c_{j1}\varrho(v_0) + c_{j2}\varrho^2(v_0) + \cdots + c_{j,m-1}\varrho^{m-1}(v_0)$, where each $c_{ji} = u^i\varepsilon^{pij}$ belongs to the ring $\mathbb{Z}[\varepsilon]$. Consider now the rational functions $g_1, \ldots, g_{m-1} \in k(X)$ defined for $j = 1, \ldots, m-1$ by

$$g_j = \frac{\varrho^j(v_0)}{v_0}.$$

These functions are τ-homogeneous. They are homogeneous of degree zero, and they are constants of d. Moreover, if $j \in \{1, \ldots, m-1\}$, then we have:

$$\frac{w_j}{w_0} = \frac{v_0 + \sum_{i=1}^{m-1} c_{ji}\varrho^i(v_0)}{v_0 + \sum_{i=1}^{m-1} c_{0i}\varrho^i(v_0)} = \frac{1 + v_0^{-1}\sum_{i=1}^{m-1} c_{ji}\varrho^i(v_0)}{1 + v_0^{-1}\sum_{i=1}^{m-1} c_{0i}\varrho^i(v_0)} = \frac{1 + \sum_{i=1}^{m-1} c_{ji}g_i}{1 + \sum_{i=1}^{m-1} c_{0i}g_i}.$$

All quotients $w_1/w_0, \ldots, w_{m-1}/w_0$ then belong to the field $k(g_1, \ldots, g_{m-1})$, and hence, by Proposition 2.13, the elements $g_1, \ldots, g_{m-1}$ are algebraically independent over k and we have the equality $k(X)^{E,d} = k(g_1, \ldots, g_{m-1})$. Note that $g_1, \ldots, g_{m-1}$ are τ-homogeneous. It follows from Proposition 5.18, that for each g_j there exists a homogeneous rational function $f_j \in k(Y)$ such that $\Delta(f_j) = 0$ and $@(f_j) = g_j$. We know, by Theorem 6.1, that the elements $v, f_1, \ldots, f_{m-1}$, are algebraically independent over k, and $k(Y)^\Delta = k(v, f_1, \ldots, f_{m-1})$. This completes our proof of Theorem 7.1. $\square$

If $n = 4$, then (in the notations of the above proof) $v_0 = x_0^2 + x_2^2 - 2x_1x_3$ and

$$g_1 = \frac{\varrho(v_0)}{v_0} = \frac{x_1^2 + x_3^2 - 2x_0x_2}{x_0^2 + x_2^2 - 2x_1x_3} = @(f_1),$$

where $f_1 = y_1y_3\frac{2y_0y_2 - y_2y_3 - y_0y_1}{y_1y_2 + y_0y_3 - 2y_1y_3}$.

Hence, we have:

Example 7.2. If $n = 4$, then $k(Y)^\Delta = k(v, f)$, where

$$f = y_1y_3\frac{2y_0y_2 - y_2y_3 - y_0y_1}{y_1y_2 + y_0y_3 - 2y_1y_3} \quad \text{and} \quad v = y_0y_1y_2y_3.$$

Consider the case $n = 6$.

Example 7.3. If $n = 6$, then $k(Y)^\Delta = k(v, f_1, f_2, f_3)$, where $v = y_0 \cdots y_5$, and f_1, f_2, f_3 are some homogeneous rational functions in $k(Y)$ such that v, f_1, f_2, f_3 are algebraically independent over k.

Proof. We have: $\varphi(n) = \varphi(6) = 2$, $m = n - \varphi(n) = 4$, $\Phi_6(t) = t^2 - t + 1$, and $w_0 = \frac{u_0u_2}{u_1}$, $w_1 = \frac{u_1u_3}{u_2} = \tau(w_0)$, $w_2 = \frac{u_2u_4}{u_3} = \tau^2(w_0)$, $w_3 = \frac{u_3u_5}{u_4} = \tau^3(w_0)$. Let us denote: $F_0 = u_0u_2u_4 = w_0w_1w_2$, $F_1 = u_1u_3u_5 = w_1w_2w_3 = \tau(F_0)$, $G_0 = u_0u_3 = w_0w_1$, $G1 = u_1u_4 = w_1w_2 = \tau(G_0)$,

$G_2 = u_2u_5 = w_2w_3 = \tau^2(G_0)$. By Theorem 2.9, the polynomials F_0, F_1, G_0, G_1, G_2 are constants of d. Note that $w_0 = \frac{F_0}{G_1}$, $w_1 = \frac{F_1}{G_2}$, $w_2 = \frac{F_0}{G_0}$, $w_3 = \frac{F_1}{G_1}$, so we have: $\frac{w_1}{w_0} = \frac{F_1G_1}{F_0G_2}$, $\frac{w_2}{w_0} = \frac{F_0G_1}{F_0G_0} = \frac{G_1}{G_0}$, $\frac{w_3}{w_0} = \frac{F_1G_1}{F_0G_1} = \frac{F_1}{F_0}$.

Observe that $\tau^2(F_0) = F_0$. This implies that the τ-degree of every nonzero monomial (with respect to variables $x_0, \dots, x_{n-1}$) of F_0 is divisible by 3. This means that in the τ-decomposition of F_0 there are only components with τ-degrees 0 and 3. Let $F_0 = v_0 + v_3$, where $v_0 \in k[X]$ is τ-homogeneous with $\deg_\tau(v_0) = 0$ (that is, $\tau(v_0) = v_0$), and $v_3 \in k[X]$ is τ-homogeneous with $\deg_\tau(v_3) = 3$ (that is, $\tau(v_3) = \varepsilon^3 v_3 = -v_3$). Of course $d(v_0) = d(v_3) = 0$ (by Lemma 5.8). Observe that $\varrho(F_0) = \varrho(u_0u_2u_4) = \varepsilon^{-(0+2+4)}u_0u_2u_4 = u_0u_2u_4 = F_0$. Hence,

$$v_0 + v_3 = F_0 = \varrho(F_0) = \varrho(v_0) + \varrho(v_3).$$

Since the τ-decomposition of F_0 is unique, we deduce (by Lemma 5.7), that $v_3 = \varrho(v_0)$ and $v_0 = \varrho(v_3)$, and so, the τ-decomposition of F_0 is of the form $F_0 = v_0 + \varrho(v_0)$. Moreover, $F_1 = \tau(F_0) = \tau(v_0 + v_3) = \tau(v_0) + \tau(v_3) = v_0 - \varrho(v_0)$.

We do a similar procedure with the polynomial G_0. We first observe that $\tau^3(G_0) = G_0$, and $\varrho(G_0) = -G_0$, and then we obtain the following three τ-decompositions: $G_0 = r_0 - \varrho(r_0) + \varrho^2(r_0)$, $G_1 = r_0 - \varepsilon^2\varrho(r_0) + \varepsilon^4\varrho^2(r_0)$, $G_2 = r_0 - \varepsilon^4\varrho(r_0) + \varepsilon^2\varrho^2(r_0)$, where r_0 is homogeneous polynomial of degree 2 which is τ-homogeneous of τ-degree zero. Consider now the rational functions $g_1, g_2, g_3 \in k(X)$ defined by

$$g_1 = \frac{\varrho(v_0)}{v_0}, \qquad g_2 = \frac{\varrho(r_0)}{r_0}, \qquad g_3 = \frac{\varrho^2(r_0)}{r_0}.$$

These functions are τ-homogeneous. They are homogeneous of degree zero (in the ordinary sense) and they are constants of d. Moreover, the quotients w_1/w_0, w_2/w_0 and w_3/w_0 belong to $k(g_1, g_2, g_3)$. In fact:

$$\begin{aligned}\frac{w_1}{w_0} = \frac{F_1G_1}{F_0G_2} &= \frac{(v_0 - \varrho(v_0))(r_0 - \varepsilon^2\varrho(r_0) + \varepsilon^4\varrho^2(r_0))}{(v_0 + \varrho(v_0))(r_0 - \varepsilon^4\varrho(r_0) + \varepsilon^2\varrho^2(r_0))} \\ &= \frac{v_0^{-1}r_0^{-1}(v_0 - \varrho(v_0))(r_0 - \varepsilon^2\varrho(r_0) + \varepsilon^4\varrho^2(r_0))}{v_0^{-1}r_0^{-1}(v_0 + \varrho(v_0))(r_0 - \varepsilon^4\varrho(r_0) + \varepsilon^2\varrho^2(r_0))} \\ &= \frac{(1 - g_1)(1 - \varepsilon^2 g_2 + \varepsilon^4 g_3)}{(1 + g_1)(1 - \varepsilon^4 g_2 + \varepsilon^2 g_3)},\end{aligned}$$

and so, $w_1/w_0 \in k(g_1, g_2, g_3)$. By a similar way we show that w_2/w_0 and w_3/w_0 also belong to $k(g_1, g_2, g_3)$. Hence, by Proposition 2.13, the elements g_1, g_2, g_3 are algebraically independent over k and $k(X)^{E,d} = k(g_1, g_2, g_3)$. It follows from Proposition 5.18, that for each g_j there exists a homogeneous rational function $f_j \in k(Y)$ such that $\Delta(f_j) = 0$ and $@(f_j) = g_j$. We know, by Theorem 6.1, that the elements v, f_1, f_2, f_3, are algebraically independent over k, and $k(Y)^\Delta = k(v, f_1, f_2, f_3)$. $\square$

Now we assume that $p > q$ are primes, and $n = pq$. In the above proof we used the explicit form of the cyclotomic polynomial $\Phi_6(t)$. Let $\Phi_{pq} = \sum c_j t^j$. In 1883, Migotti [18] showed that all c_j belong to $\{-1, 0, 1\}$. In 1964 Beiter [1] gave a criterion on j for c_j to be 0, 1 or -1.

In 1996, Lam and Leung [11] gave a similar but more elementary result. Their criterion is based on the elementary fact that there is a unique way to write $\varphi(pq) = (p-1)(q-1) = rp + sq$ with nonnegative integers r and s. Indeed, from the Bézout relation $up - vq = 1$ with $1 \leqslant u \leqslant q-1$ and $1 \leqslant v \leqslant p-1$, r and s have to be $r = u-1$ and $s = p-1-v$; then $0 \leqslant r \leqslant q-2$, $0 \leqslant s \leqslant p-2$. Using the numbers r, s, Lam and Leung proved:

Lemma 7.4. *(See [11].) Let* $\Phi_{pq}(t)=\sum_{l=0}^{\varphi(pq)} c_l t^l$*. Then*

$$\begin{aligned} c_l = 1 \quad &\Longleftrightarrow \quad l = ip + jq, \quad i \in \{0,1,\dots,r\},\ j \in \{0,1,\dots,s\}; \\ c_l = -1 \quad &\Longleftrightarrow \quad l = ip + jq + 1, \quad i \in \{0,1,\dots,(q-2)-r\},\ j \in \{0,1,\dots,(p-2)-s\}. \end{aligned}$$

Now we may prove the following theorem.

Theorem 7.5. *If $n = pq$ for some prime numbers $p > q$, then there exist homogeneous elements $f_1,\dots,f_{m-1}$ of $k(Y)^\Delta$ such that $v, f_1,\dots,f_{m-1}$ are algebraically independent over k and*

$$k(Y)^\Delta = k(v, f_1,\dots,f_{m-1}),$$

where $m = p+q-1$ and $v = y_0\cdots y_{n-1}$.

Proof. We use the same idea as in the proofs of Theorem 7.1 and Example 7.3. We have: $\varphi(n) = (p-1)(q-1)$ and $m = n-\varphi(n) = p+q-1$. For each $i \in \mathbb{Z}$, let us denote:

$$F_i = \prod_{j=0}^{p-1} u_{jq+i}, \qquad G_i = \prod_{j=0}^{q-1} u_{jp+i}.$$

In particular, $F_0 = u_0u_qu_{2q}\cdots u_{(p-1)q}$ $G_0 = u_0u_pu_{2p}\cdots u_{(q-1)p}$. Observe that if $i = bq + c$, where $b, c \in \mathbb{Z}$ and $0 \leqslant c < q$, then $F_i = F_c$. Similarly, if $i = bp + c$, where $b, c \in \mathbb{Z}$ and $0 \leqslant c < p$, then $G_i = G_c$. Let A be the set of all indexes $l \in \{0,1,\dots,\varphi(pq)\}$ with $c_l = 1$, and let B be the set of all indexes $l \in \{0,1,\dots,\varphi(pq)\}$ with $c_l = -1$. We have $B \neq \emptyset$ because n is not a power of prime (see the fact mentioned after Theorem 3.7). It is clear that $A \cap B = \emptyset$, $A \neq \emptyset$, and $w_0 = \frac{N}{D}$ where $N = \prod_{l\in A} u_l$, $D = \prod_{l\in B} u_l$. It follows from Lemma 7.4, that

$$N = \prod_{i=0}^{r}\prod_{j=0}^{s} u_{ip+jq}, \qquad D = \prod_{i=0}^{(q-2)-r}\ \prod_{j=0}^{(p-2)-s} u_{ip+jq+1}.$$

It is easy to check that $\prod_{i=0}^{r} F_{ip} = N\cdot S$ and $\prod_{j=0}^{p-2-s} G_{jq+1} = D\cdot T$, where

$$S = \prod_{i=0}^{r}\ \prod_{j=s+1}^{p-1} u_{ip+jq} \quad \text{and} \quad T = \prod_{j=0}^{p-2-s}\ \prod_{i=q-2-r+1}^{q-1} u_{ip+jq+1}.$$

Now we will show that $S = T$. First observe that S and T have the same number of factors, which is equal to $(r+1)(p-s-1)$. Next observe that

$$S = \prod_{i=0}^{r}\ \prod_{j=0}^{p-s-2} u_{ip+(s+1+j)q} \quad \text{and} \quad T = \prod_{j=0}^{p-2-s}\ \prod_{i=0}^{r} u_{(q-r-1+i)p+jq+1}.$$

Thus, it is enough to show that, for $i \in \{0,\dots,r\}$ and $j \in \{0,1,\dots,p-s-2\}$, we have $(s+1+j)q+ip \equiv (q-r-1+i)p+jq+1 \pmod{pq}$. But it is obvious, because $(p-1)(q-1) = rp+sq$. Therefore, $S = T$ and we have

$$w_0 = \frac{\prod_{i=0}^{r} F_{ip}}{\prod_{j=0}^{p-2-s} G_{jq+1}}. \tag{$*$}$$

Now we do exactly the same as in the proof of Example 7.3. We have the homogeneous polynomials $F_0, \dots, F_{q-1}$ and $G_0, \dots, G_{p-1}$, which are constants of d, and $F_i = \tau^i(F_0)$, $G_i = \tau^i(G_0)$, $\deg F_i = p$, $\deg G_i = q$, for each i. Observe that $\tau^q(F_0) = F_0$. This implies that the τ-degree of every nonzero monomial (with respect to variables $x_0, \dots, x_{n-1}$) of F_0 is divisible by p. This means that in the τ-decomposition of F_0 there are only components with τ-degrees $0, p, 2p, \dots, (q-1)p$. Let $F_0 = \sum_{i=0}^{q-1} v_i$, where each v_i is a τ-homogeneous polynomial from $k[X]$, and $\tau(v_i) = \varepsilon^{pi} v_i$. Of course $d(v_i) = 0$ for all i (because $\tau d = \varepsilon d \tau$ by Lemma 5.8), and $\deg(v_i) = p$. But $\varrho(u_j) = \varepsilon^{-j} u_j$ (see Lemma 1.1), so $\varrho(F_0) = \pm F_0$. Since $p > q \geqslant 2$, we have $p \geqslant 3$, and so $\varrho(F_0) = F_0$. Now we have

$$v_0 + v_1 + \cdots + v_{q-1} = F_0 = \varrho(F_0) = \varrho(v_0) + \varrho(v_1) + \cdots + \varrho(v_{q-1}).$$

Since the τ-decomposition of F_0 is unique, we deduce (by Lemma 5.7), that

$$v_1 = \varrho(v_0), \quad v_2 = \varrho(v_1), \quad \dots, \quad v_{q-1} = \varrho(v_{q-2}), \quad v_0 = \varrho(v_{q-1}),$$

and we have $v_j = \varrho^j(v_0)$ for all $j = 0, 1, \dots, q-1$. Therefore, the τ-decomposition of F_0 is of the form $F_0 = v_0 + \sum_{i=1}^{q-1} \varrho^i(v_0)$. This implies that $F_1 = \tau(F_0) = v_0 + \sum \varepsilon^{ip} \varrho(v_0)$. We do the same for $F_2 = \tau(F_1) = \tau^2(F_0)$, and for all F_j. Thus, for all $j = 0, 1, \dots, q-1$, we have

$$F_j = v_0 + \sum_{i=1}^{q-1} c_{ji} \varrho^i(v_0),$$

where each c_{ji} belongs to the ring $\mathbb{Z}[\varepsilon]$. We do a similar procedure with the polynomial G_0. First observe that $\tau^p(G_0) = G_0$ and $\varrho(G_0) = \pm G_0$, to obtain τ-decompositions of the forms

$$G_j = r_0 + \sum_{i=1}^{p-1} b_{ji} \varrho^i(r_0),$$

where each b_{ji} belongs to $\mathbb{Z}[\varepsilon]$ and r_0 is a homogeneous polynomial of degree q which is τ-homogeneous of τ-degree zero and then consider the elements $g_1, \dots, g_{m-1} \in k(X)$ defined by

$$g_i = \frac{\varrho^i(v_0)}{v_0}, \qquad g_{q-1+j} = \frac{\varrho^j(r_0)}{r_0},$$

for $i = 1, \dots, q-1$, and $j = 1, \dots, p-1$. These elements are τ-homogeneous. They are homogeneous of degree zero (in the ordinary sense) and they are constants of d. We know, by the above construction, that the elements $\frac{1}{v_0}\tau^i(F_j)$ and $\frac{1}{r_0}\tau^i(G_j)$ belong to the field $k(g_1, \dots, g_{m-1})$. But, by $(*)$, for each $a = 0, \dots, m-1$, we have

$$w_a \frac{r_0^{p-1-s}}{v_0^{r+1}} = \tau^a(w_0) \frac{r_0^{p-1-s}}{v_0^{r+1}} = \frac{\prod_{i=0}^{r} \frac{\tau^a(F_{ip})}{v_0}}{\prod_{j=0}^{p-2-s} \frac{\tau^a(G_{jq+1})}{r_0}},$$

and hence, each element $w_a r_0^{p-1-s} v_0^{-(r+1)}$ belongs to $k(g_1, \dots, g_{m-1})$. This implies, that for every $j - 1, \dots, m-1$, the quotient

$$\frac{w_j}{w_0} = \frac{r_0^{p-1-s} v_0^{-(r+1)} w_j}{r_0^{p-1-s} v_0^{-(r+1)} w_0}$$

belongs to $k(g_1, \dots, g_{m-1})$. Hence, by Proposition 2.13, the elements $g_1, \dots, g_m$ are algebraically independent over k and $k(X)^{E,d} = k(g_1, \dots, g_{m-1})$. It follows from Proposition 5.18, that for each g_j there exists a homogeneous rational function $f_j \in k(Y)$ such that $\Delta(f_j) = 0$ and $@(f_j) = g_j$. We know, by Theorem 6.1, that the elements $v, f_1, \dots, f_{m-1}$, are algebraically independent over k, and $k(Y)^\Delta = k(v, f_1, \dots, f_{m-1})$. This completes our proof of Theorem 7.5. $\square$

We already know a structure of the field $k(Y)^\Delta$ but only in the following two cases, when n is a power of a prime number (Theorem 7.1), and when n is the product of two prime numbers (Theorem 7.5). We do not know what happens in all other cases. Is this field always a purely transcendental extension of k? What is in the cases $n = 12$ or $n = 30$ or $n = 105$?

Acknowledgment

We would like to express our deep gratitude to the anonymous referee for her/his very careful reading of the manuscript and the resulting pertinent remarks and clever advices.

References

[1] M. Beiter, The midterm coefficient of the cyclotomic polynomial $F_{pq}(x)$, Amer. Math. Monthly 71 (1964) 769–770.
[2] M. Beiter, I.J. Schoenberg, Coefficients of the cyclotomic polynomial, Amer. Math. Monthly 73 (1966) 541–542.
[3] J.H. Conway, A.J. Jones, Trigonometric diophantine equations (On vanishing sums of roots of unity), Acta Arith. 30 (1976) 229–240.
[4] N.G. de Bruijn, On the factorization of cyclic groups, Indag. Math. 15 (1953) 370–377.
[5] A. van den Essen, Polynomial Automorphisms and the Jacobian Conjecture, Progr. Math., vol. 190, 2000.
[6] G. Freudenburg, Algebraic Theory of Locally Nilpotent Derivations, Encyclopedia Math. Sci., vol. 136, Springer, 2006.
[7] B. Grammaticos, J. Moulin Ollagnier, A. Ramani, J.-M. Strelcyn, S. Wojciechowski, Integrals of quadratic ordinary differential equations in $\mathbb{R}^3$: the Lotka–Volterra system, Phys. A 163 (1990) 683–722.
[8] J. Hofbauer, K. Sigmund, The Theory of Evolution and Dynamical Systems. Mathematical Aspects of Selection, London Math. Soc. Stud. Text, vol. 7, Cambridge University Press, Cambridge, 1988.
[9] N. Jacobson, Lectures in Abstract Algebra. Vol. III: Theory of Fields and Galois Theory, D. Van Nostrand Co., Inc., Princeton, NJ, Toronto, ON, London, New York, 1964.
[10] J.-P. Jouanolou, Équations de Pfaff algébriques, Lecture Notes in Math., vol. 708, Springer-Verlag, Berlin, 1979.
[11] T.Y. Lam, K.H. Leung, On the cyclotomic polynomial $\Phi_{pq}(x)$, Amer. Math. Monthly 103 (7) (1996) 562–564.
[12] T.Y. Lam, K.H. Leung, On vanishing sums of roots of unity, J. Algebra 224 (2000) 91–109.
[13] S. Lang, Algebra, second edition, Addison–Wesley Publishing Company, 1984.
[14] H.W. Lenstra Jr., Vanishing sums of roots of unity, in: Proc. Bicentennial Congress Wiskunding Genootschap, Part II, Vrije Univ. Amsterdam, 1978, in: Math. Centre Tracts, vol. 101, Math. Centrum, Amsterdam, 1979, pp. 249–268.
[15] R. Lidl, H. Niederreiter, Finite Fields, Encyclopedia Math. Appl., vol. 20, Addison–Wesley, 1983.
[16] A. Maciejewski, J. Moulin Ollagnier, A. Nowicki, J.-M. Strelcyn, Around Jouanolou non-integrability theorem, Indag. Math. (N.S.) 11 (2000) 239–254.
[17] A. Maciejewski, J. Moulin Ollagnier, A. Nowicki, Generic polynomial vector fields are not integrable, Indag. Math. (N.S.) 15 (1) (2004) 55–72.
[18] A. Migotti, Zur Theorie der Kreisteilungsgleichung, S.-B. der Math.-Naturwiss. Classe der Kaiser. Akad. der Wiss., Wien 87 (1983) 7–14.
[19] K. Motose, On values of cyclotomic polynomials, VI, Bull. Fac. Sci. Technol. Hirosaki Univ. 6 (2004) 1–5.
[20] J. Moulin Ollagnier, A. Nowicki, Derivations of polynomial algebras without Darboux polynomials, J. Pure Appl. Algebra 212 (2008) 1626–1631.
[21] J. Moulin Ollagnier, A. Nowicki, Monomial derivations, Comm. Algebra 39 (2011) 3138–3150.
[22] J. Moulin Ollagnier, A. Nowicki, J.-M. Strelcyn, On the non-existence of constants of derivations: The proof of a theorem of Jouanolou and its development, Bull. Sci. Math. 119 (1995) 195–233.
[23] T. Nagell, Introduction to Number Theory, Chelsea Publishing Company, New York, 1964.
[24] A. Nowicki, Polynomial Derivations and Their Rings of Constants, N. Copernicus University Press, Toruń, 1994.
[25] A. Nowicki, A factorisable derivation of polynomial rings in n variables, Univ. Iagel. Acta Math. (2010) 89–101.
[26] A. Nowicki, M. Nagata, Rings of constants for k-derivations in $k[x_1, \dots, x_n]$, J. Math. Kyoto Univ. 28 (1988) 111–118.
[27] A. Nowicki, J. Zieliński, Rational constants of monomial derivations, J. Algebra 302 (2006) 387–418.
[28] L. Rédei, Ein Beitrag zum Problem der Faktorisation von endlichen Abelschen Gruppen, Acta Math. Hungar. 1 (1950) 197–207.
[29] A. Satyanarayan Reddy, The lowest 0, 1-polynomial divisible by cyclotomic polynomial, arXiv:1106.1271v2, 2011.
[30] I.J. Schoenberg, A note on the cyclotomic polynomial, Mathematika 11 (1964) 131–136.
[31] J.P. Steinberger, The lowest-degree polynomial with nonnegative coefficients divisible by the n-th cyclotomic polynomial, Electron. J. Combin. 19 (4) (2012) 1–18.
[32] J.P. Steinberger, Minimal vanishing sums of roots of unity with large coefficients, Proc. Lond. Math. Soc. (3) (2012).
[33] H. Żołądek, Multi-dimensional Jouanolou system, J. Reine Angew. Math. 556 (2003) 47–78.