Analytic and Algebraic Geometry 2
Łódź University Press 2017, 97–121
DOI: http://dx.doi.org/10.18778/8088-922-4.15

RATIONAL CONSTANTS OF CYCLOTOMIC DERIVATIONS

JEAN MOULIN OLLAGNIER AND ANDRZEJ NOWICKI

1. Introduction

Let $K(X) = K(x_0, \ldots, x_{n-1})$ be the field of rational functions in $n \geqslant 3$ variables over a field K of characteristic zero. Let d be the cyclotomic derivation of $K(X)$, that is, d is the K-derivation of $K(X)$ defined by

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

We denote by $K(X)^d$ the field of constants of d, that is, $K(X)^d = \{f \in K(X);\ d(f) = 0\}$.

We are interested in algebraic descriptions of the field $K(X)^d$. However, we know that such descriptions are usually difficult to obtain. Fields of constants appear in various classical problems; for details we refer to [2], [3], [12], [9] and [11].

We already know (see [10]) that if K contains the n-th roots of unity, then $K(X)^d$ is a field of rational functions over K and its transcendence degree over K is equal to $m = n - \varphi(n)$, where φ is the Euler totient function. In our proof of this fact the assumption concerning n-th roots plays an important role. We do not know if the same is true without this assumption. What happens, for example, when $K = \mathbb{Q}$?

In this article we give a partial answer to this question, for arbitrary field K of characteristic zero.

We introduce a class of special positive integers, and we prove (see Theorem 9.1) that if n belongs to this class, then the mentioned result is also true for arbitrary field K of characteristic zero, without the assumption concerning roots of unity.

2010 *Mathematics Subject Classification.* Primary 12H05; Secondary 13N15.

Key words and phrases. Derivation, cyclotomic polynomial, Darboux polynomial, Euler totient function, Euler derivation, factorisable derivation, Jouanolou derivation, Lotka-Volterra derivation.

Moreover, we construct a set of free generators of $K(X)^d$, which are polynomials with integer coefficients. Thus, if the number n is special, then

$$K(X)^d = K\left(F_0, \dots, F_{m-1}\right),$$

for some, algebraically independent, polynomials $F_0, \dots, F_{m-1}$ belonging to the polynomial ring $\mathbb{Z}[X] = \mathbb{Z}\left[x_0, \dots, x_{n-1}\right]$, and where $m = n - \varphi(n)$. Note that in the segment $[3, 100]$ there are only 3 non-special numbers: 36, 72 and 100. We do not know if the same is true for non-special numbers, for example when $n = 36$.

In our proofs we use classical properties of cyclotomic polynomials, and an important role play some results ([4], [5], [16], [17] and others) on vanishing sums of roots of unity.

2. Notations and preparatory facts

Throughout this paper $n \geqslant 3$ is an integer, ε is a primitive n-th root of unity, and $\mathbb{Z}_n$ is the ring $\mathbb{Z}/n\mathbb{Z}$. Moreover, K is a field of characteristic zero, $K[X] = K[x_0, \dots, x_{n-1}]$ is the polynomial ring over K in variables $x_0, \dots, x_{n-1}$, and $K(X) = K(x_0, \dots, x_{n-1})$ is the field of quotients of $K[X]$. The indexes of the variables $x_0, \dots, x_{n-1}$ are elements of the ring $\mathbb{Z}_n$. The cyclotomic derivation d is the K-derivation of $K(X)$ defined by $d(x_j) = x_{j+1}$ for $j \in \mathbb{Z}_n$.

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

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

An important role in our paper will play two subsets of $\mathbb{Z}^n$ denoted by $\mathcal{G}_n$ and $\mathcal{M}_n$. The first subset is the set of all sequences $\alpha = (\alpha_0, \dots, \alpha_{n-1})$ such that $\alpha_0, \dots, \alpha_{n-1}$ are integers and

$$\alpha_0 + \alpha_1 \varepsilon^1 + \alpha_2 \varepsilon^2 + \cdots + \alpha_{n-1} \varepsilon^{n-1} = 0.$$

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 $\mathbb{N} = \{0, 1, 2, \dots\}$. To be precise,

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

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 $0 = (0, \dots, 0)$.

Let us recall that 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 also (see for example [6] or [7]) 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 2.1. *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 $\mathcal{M}_n$.

The monoid $\mathcal{M}_n$ has an order $\geqslant$. If $\alpha,\beta \in \mathcal{G}_n$, the 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 $\geqslant$.

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 $\mathcal{M}_n$.

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 $\alpha = (\alpha_0, \alpha_1, \dots, \alpha_{n-1}) \in \mathbb{Z}^n$. The mapping ζ is a $\mathbb{Z}$-module automorphism of $\mathbb{Z}^n$. Note that $\zeta^{-1}(\alpha) = (\alpha_1, \dots, \alpha_{n-1}, \alpha_0)$, for all $\alpha = (\alpha_0, \alpha_1, \dots, \alpha_{n-1}) \in \mathbb{Z}^n$. If $a, b \in \mathbb{Z}$ and $a \equiv b \pmod{n}$, then $\zeta^a = \zeta^b$. Moreover, $\zeta(e_j) = e_{j+1}$ for all $j \in \mathbb{Z}_n$, and $\zeta(e) = e$.

Let us recall from [10] some basic properties of $\mathcal{M}_n$ and $\mathcal{G}_n$.

Proposition 2.2 ([10]).

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

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

(3) *The set of all minimal elements of $\mathcal{M}_n$ is finite.*

(4) *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.*

(5) *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 $\mathcal{M}_n$.*

Look at the cyclotomic polynomial $\Phi_n(t)$. Assume that $\Phi_n(t) = c_0 + c_1 t + \dots + c_{\varphi(n)} t^{\varphi(n)}$. All the coefficients $c_0, \dots, c_{\varphi(n)}$ are integers, and $c_0 = c_{\varphi(n)} = 1$. Put $m = n - \varphi(n)$ and

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

Note that $\gamma_0 \in \mathbb{Z}^n$, and $H_{\gamma_0}(t) = \Phi_n(t)$. Consider the elements $\gamma_0, \gamma_1, \dots, \gamma_{m-1}$ defined by $\gamma_j = \zeta^j(\gamma_0)$, for $j = 0, 1, \dots, m-1$. 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 $\mathcal{G}_n$. Moreover, we proved in [10], that they form a basis over $\mathbb{Z}$, which is the following theorem.

Theorem 2.3 ([10]). *$\mathcal{G}_n$ is a free $\mathbb{Z}$-module, and the elements $\gamma_0, \dots, \gamma_{m-1}$, where $m = n - \varphi(n)$, form its basis over $\mathbb{Z}$.*

3. Standard minimal elements

Assume that p is a prime divisor of n, and consider the sequences

$$m(p,r) = \sum_{i=0}^{p-1} e_{r+i\frac{n}{p}},$$

for $r = 0, 1, \dots, \frac{n}{p} - 1$. Observe that each $m(p,r)$ is equal to $\zeta^r\left(m(p,0)\right)$. Each $m(p,r)$ is a minimal element of $\mathcal{M}_n$ (see [10] for details). We say that $m(p,r)$ is a *standard* minimal element of $\mathcal{M}_n$. In [10] we used the notation $E_r^{(p)}$ instead of $m(p,r)$. It is clear that if $r_1, r_2 \in \{0, 1, \dots, \frac{n}{p} - 1\}$ and $r_1 \neq r_2$, then $m(p,r_1) \neq m(p,r_2)$.

If $\alpha = (\alpha_0, \dots, \alpha_{n-1}) \in \mathbb{Z}^n$, then we denote by $|\alpha|$ the sum $\alpha_0 + \cdots + \alpha_{n-1}$. Observe that, for every r, we have $|m(p,r)| = p$. This implies, that if $p \neq q$ are prime divisors of n, then $m(p,r_1) \neq m(q,r_2)$ for all $r_1 \in \{0, \dots, \frac{n}{p} - 1\}$, $r_2 \in \{0, 1, \dots, \frac{n}{q} - 1\}$. Note the following two obvious propositions.

Proposition 3.1. $\sum_{r=0}^{\frac{n}{p}-1} m(p,r) = (1, 1, \dots, 1) = e.$

Proposition 3.2. *If p is a prime divisor of n, then the standard elements $m(p,0)$, $m(p,1)$, …, $m(p, \frac{n}{p} - 1)$ are linearly independent over $\mathbb{Z}$.*

The following two propositions are less obvious and deserve a proof.

Proposition 3.3. *Let $n = pqN$, where $p \neq q$ are primes and N is a positive integer. Then*

$$\sum_{k=0}^{p-1} m(q,kN) = \sum_{k=0}^{q-1} m(p,kN).$$

which, for any shift r, is easily extended to

$$\sum_{k=0}^{p-1} m(q,kN+r) = \sum_{k=0}^{q-1} m(p,kN+r).$$

Proof. If m is a positive integer, then we denote by $[m]$ the set $\{0, 1, \dots, m-1\}$. First observe that $\Big\{k + ip;\ k \in [p],\ i \in [q]\Big\} = \Big\{k + iq;\ k \in [q],\ i \in [p]\Big\} = [pq]$. Hence,

$$\begin{aligned}
\sum_{k=0}^{p-1} m(q,kN) &= \sum_{k=0}^{p-1}\sum_{i=0}^{q-1} e_{kN+i\frac{n}{q}} = \sum_{k=0}^{p-1}\sum_{i=0}^{q-1} e_{N(k+ip)} = \sum_{k=0}^{pq-1} e_{Nk};\\
\sum_{k=0}^{q-1} m(p,kN) &= \sum_{k=0}^{q-1}\sum_{i=0}^{p-1} e_{kN+i\frac{n}{p}} = \sum_{k=0}^{q-1}\sum_{i=0}^{p-1} e_{N(k+iq)} = \sum_{k=0}^{pq-1} e_{Nk}.
\end{aligned}$$

Thus, $\sum_{k=0}^{p-1} m(q,kN) = \sum_{k=0}^{pq-1} e_{kN} = \sum_{k=0}^{q-1} m(p,kN)$. □

Proposition 3.4. *Let p be a prime divisor of n. Let $0 \leqslant r < \frac{n}{p}$, and $a \in \mathbb{Z}$. Then*

$$\zeta^a\Big(m(p,r)\Big) = m(p,b), \quad \textit{where} \quad b = (a+r)\left(\text{mod } \frac{n}{p}\right)$$

Proof. Put $w = \frac{n}{p}$, and $[p] = \{0, 1, \dots, p-1\}$. Let $a + r = cw + b$, where $c, b \in \mathbb{Z}$ with $0 \leqslant b < w$. Observe that $\Big\{b + (c+i)w \ (\text{mod } n);\ i \in [p]\Big\} = \Big\{b + iw;\ i \in [p]\Big\}$. Hence,

$$\begin{aligned} \zeta^a\Big(m(p,r)\Big) &= \zeta^a\left(\sum_{i=0}^{p-1} e_{r+iw}\right) = \sum_{i=0}^{p-1} \zeta^a\left(e_{r+iw}\right) = \sum_{i=0}^{p-1} e_{a+r+iw} \\ &= \sum_{i=0}^{p-1} e_{b+cw+iw} = \sum_{i=0}^{p-1} e_{b+(c+i)w} = \sum_{i=0}^{p-1} e_{b+iw} = m(p,b), \end{aligned}$$

and $b = (a+r) \ (\text{mod } w)$. □

We will apply the following theorem of Rédei, de Bruijn and Schoenberg.

Theorem 3.5 ([13], [1], [15])**.** *The standard minimal elements of $\mathcal{M}_n$ generate the group $\mathcal{G}_n$.*

Known proofs of the above theorem used usually techniques of group rings. Lam and Leung [5] gave a new proof using induction and group-theoretic techniques.

We know (see for example [10]) that if n is divisible by at most two distinct primes, then every minimal element of $\mathcal{M}_n$ is standard. It is known (see for example [5], [17], [14]) that in all other cases always exist nonstandard minimal elements.

4. The sets I_j

Let $n \geqslant 3$ be an integer, and let $n = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$, where $p_1, \dots, p_s$ are distinct primes and $\alpha_1, \dots, \alpha_s$ are positive integers. Put $n_j = \frac{n}{p_j}$ for $j = 1, \dots, s$. Let $I_1, \dots, I_s$ be sets of integers defined as follows:

$$\begin{aligned} I_1 &= \Big\{r \in \mathbb{Z};\ 0 \leqslant r < n_1\Big\}, \\ I_2 &= \Big\{r \in \mathbb{Z};\ 0 \leqslant r < n_2,\ \gcd(r, p_1) = 1\Big\}, \\ I_3 &= \Big\{r \in \mathbb{Z};\ 0 \leqslant r < n_3,\ \gcd(r, p_1p_2) = 1\Big\}, \\ &\ \ \vdots \\ I_s &= \Big\{r \in \mathbb{Z};\ 0 \leqslant r < n_s,\ \gcd(r, p_1p_2\cdots p_{s-1}) = 1\Big\}. \end{aligned}$$

That is, $I_1 = \{r \in \mathbb{Z};\ 0 \leqslant r < n_1\}$ and $I_j = \{r \in \mathbb{Z};\ 0 \leqslant r < n_j,\ \gcd(r, p_1 \cdots p_{j-1}) = 1\}$ for $j = 2, \dots, s$. This definition depends of the fixed succession of primes. We will say that the above $I_1, \dots, I_s$ are the *n-sets of type* $[p_1, \dots, p_s]$.

Let for example $n = 12 = 2^2 3$. Then $I_1 = \{0, 1, 2, 3, 4, 5\}$, $I_2 = \{1, 3\}$ are the 12-sets of type $[2, 3]$, and $I_1 = \{0, 1, 2, 3\}$, $I_2 = \{1, 2, 4, 5\}$ are the 12-sets of type $[3, 2]$.

Example 4.1. *The* 30*-sets of a a given type:*

type	I_1	I_2	I_3
$[2,3,5]$	$\{0,1,2,\dots,14\}$	$\{1,3,5,7,9\}$	$\{1,5\}$
$[2,5,3]$	$\{0,1,2,\dots,14\}$	$\{1,3,5\}$	$\{1,3,7,9\}$
$[3,2,5]$	$\{0,1,2,\dots,9\}$	$\{1,2,4,5,7,8,10,11,13,14\}$	$\{1,5\}$
$[3,5,2]$	$\{0,1,2,\dots,9\}$	$\{1,2,4,5\}$	$\{1,2,4,7,8,11,13,14\}$
$[5,2,3]$	$\{0,1,2,3,4,5\}$	$\{1,2,3,4,6,7,8,9,11,12,13,14\}$	$\{1,3,7,9\}$
$[5,3,2]$	$\{0,1,2,3,4,5\}$	$\{1,2,3,4,6,7,8,9\}$	$\{1,2,4,7,8,11,13,14\}$

Now we calculate the cardinality of the sets $I_1, \dots, I_s$. We denote by $|X|$ the number of all elements of a finite set X. First observe that if a, b are relatively prime positive integers, then in the set $\{1, 2, \dots, ab\}$ there are exactly $\varphi(a)b$ numbers relatively prime to a. In fact, let $u \in \{1, 2, \dots, ab\}$. Then $u = ka + r$, where $0 \leqslant k \leqslant b$ and $0 \leqslant r < a$, and $\gcd(u, a) = 1 \iff \gcd(r, a) = 1$. Thus, every such u, which is relatively prime to a, is of the form $ka + r$ with $1 \leqslant r < a$, $\gcd(r, a) = 1$ and where k is an arbitrary number belonging to $\{0, 1, \dots, b-1\}$. Hence, we have exactly b such numbers k, and so, the number of integers in $\{1, \dots, ab\}$, relatively prime to a, is equal to $\varphi(a)b$. As a consequence of this fact we obtain

Lemma 4.2. *Let $a \geqslant 2$, $b \geqslant 2$ be relatively prime integers. Then there are exactly $\varphi(a)b$ such integers belonging to $\{0, 1, \dots, ab-1\}$ which are relatively prime to a.*

Let us recall that $\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\cdots\left(1 - \frac{1}{p_s}\right)$. Now we are ready to prove the following proposition.

Proposition 4.3. $|I_1| = n_1$, *and* $|I_j| = n_j\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_{j-1}}\right)$, *for all $j = 2, 3, \dots, s$.*

Proof. The case $|I_1| = n_1$ is obvious. Let $j \geqslant 2$, and put $a = p_1^{\alpha_1}\cdots p_{j-1}^{\alpha_{j-1}}$, $b = p_j^{\alpha_j - 1} p_{j+1}^{\alpha_{j+1}}\cdots p_s^{\alpha_s}$. Then $\gcd(a, b) = 1$, $n_j - 1 = ab - 1$, and if $r \in \{0, 1, \dots, n_j - 1\}$, then $r \in I_j \iff \gcd(r, a) = 1$. Hence, by Lemma 4.2, we have

$$\begin{aligned} |I_j| &= \varphi(a)b = p_1^{\alpha_1}\cdots p_{j-1}^{\alpha_{j-1}}\left(1 - \frac{1}{p_1}\right)\cdots\left(1 - \frac{1}{p_{j-1}}\right)b \\ &= p_1^{\alpha_1}\cdots p_{j-1}^{\alpha_{j-1}}\left(1 - \frac{1}{p_1}\right)\cdots\left(1 - \frac{1}{p_{j-1}}\right)p_j^{\alpha_j - 1}p_{j+1}^{\alpha_{j+1}}\cdots p_s^{\alpha_s} \\ &= \frac{n}{p_j}\left(1 - \frac{1}{p_1}\right)\cdots\left(1 - \frac{1}{p_{j-1}}\right) = n_j\left(1 - \frac{1}{p_1}\right)\cdots\left(1 - \frac{1}{p_{j-1}}\right). \end{aligned}$$

This completes the proof. □

Lemma 4.4. *Consider some nonzero numbers $z_1, \dots, z_s$. Define w_1 by $w_1 = \frac{1}{z_1}$ and w_j by $w_j = \frac{1}{z_j}\left(1 - \frac{1}{z_1}\right)\left(1 - \frac{1}{z_2}\right)\cdots\left(1 - \frac{1}{z_{j-1}}\right)$ for $j = 2, \dots, s$. Then*

$$w_1 + w_2 + \cdots + w_s = 1 - \left(1 - \frac{1}{z_1}\right)\left(1 - \frac{1}{z_2}\right)\cdots\left(1 - \frac{1}{z_s}\right).$$

Proof. The case $s = 1$ is obvious. Assume now that it is true for an integer $s \geqslant 1$, and consider nonzero numbers $z_1, \dots, z_{s+1}$. Then we have

$$\begin{aligned} &1 - \left(1 - \tfrac{1}{z_1}\right) \cdots \left(1 - \tfrac{1}{z_{s+1}}\right) \\ &= \left(1 - \left(1 - \tfrac{1}{z_1}\right) \cdots \left(1 - \tfrac{1}{z_s}\right)\right) + \tfrac{1}{z_{s+1}} \left(1 - \tfrac{1}{z_1}\right) \cdots \left(1 - \tfrac{1}{z_s}\right) \\ &= w_1 + \cdots + w_s + w_{s+1}. \end{aligned}$$

□

Proposition 4.5. $|I_1| + |I_2| + \cdots + |I_s| = n - \varphi(n)$.

Proof. We know, by Proposition 4.3, that $|I_j| = nw_j$, for $j = 1, \dots, s$, where $w_1 = \frac{1}{p_1}$ and $w_j = \frac{1}{p_j}\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_{j-1}}\right)$ for $j = 2, \dots, s$. Thus, by Lemma 4.4,

$$\begin{aligned} &|I_1| + |I_2| + \cdots + |I_s| = n\left(w_1 + \cdots + w_s\right) \\ &= n\left(1 - \left(1 - \tfrac{1}{p_1}\right)\left(1 - \tfrac{1}{p_2}\right) \cdots \left(1 - \tfrac{1}{p_s}\right)\right) \\ &= n - n\left(1 - \tfrac{1}{p_1}\right)\left(1 - \tfrac{1}{p_2}\right) \cdots \left(1 - \tfrac{1}{p_s}\right) = n - \varphi(n). \end{aligned}$$

This completes the proof. □

Let us recall the following well-known lemma where ε is a primitive n-th root of unity.

Lemma 4.6. *Let c be an integer and let $U = \sum_{r=0}^{n-1} (\varepsilon^c)^r$. If $n \nmid c$ then U is equal to 0, and in the other case, when $n \mid c$, this sum is equal to n.*

Using this lemma we may prove the following proposition.

Proposition 4.7. *If $c \in \mathbb{Z}$ then, for any $j \in \{1, \dots, s\}$, the sum $W_j = \sum_{r \in I_j} (\varepsilon^{p_j c})^r$ is an integer.*

Proof. First consider the case $j = 1$. Let $\eta = \varepsilon^{p_1}$. Then η is a primitive n_1-th root of unity, and $W_1 = \sum_{r=0}^{n_1 - 1} (\eta^c)^r$. It follows from Lemma 4.6 that W_1 is an integer.

Now assume that $j \geqslant 2$. Put $X = \{0, 1, \dots, n_j - 1\}$, and $D_i = \{r \in X;\ p_i \mid r\}$ for $i = 1, \dots, j-1$. Then $I_j = X \smallsetminus (D_1 \cup \cdots \cup D_{j-1})$, and then $W_j = U - V$, where

$$U = \sum_{r \in X} \left(\varepsilon^{p_j c}\right)^r, \quad V = \sum_{r \in D_1 \cup \cdots \cup D_{j-1}} \left(\varepsilon^{p_j c}\right)^r.$$

Observe that $U = \sum_{r=0}^{n_j - 1} (\eta^c)^r$, where $\eta = \varepsilon^{p_j}$ is a primitive n_j-root of unity. Thus, by Lemma 4.6, U is an integer. Now we will show that V is also an integer. For this aim first observe that

$$V = \sum_{k=1}^{j-1} (-1)^{k+1} \sum_{i_1 < \cdots < i_k} \sum_{r \in D_{i_1 \ldots i_k}} \left(\varepsilon^{p_j c}\right)^r ,$$

where the sum $\sum\limits_{i_1 < \cdots < i_k}$ runs through all integer sequences $(i_1, \ldots, i_k)$ such that $1 \leqslant i_1 < \cdots < i_k \leqslant j-1$, and where $D_{i_1 \ldots i_k} = D_{i_1} \cap \cdots \cap D_{i_k}$.

Let $1 \leqslant i_1 < \cdots < i_k \leqslant j-1$ be a fixed integer sequence. Then we have

$$\sum_{r \in D_{i_1 \ldots i_k}} \left(\varepsilon^{p_j c}\right)^r = \sum_{r=0}^{u-1} \left(\eta^c\right)^r ,$$

where $\eta = \varepsilon^{p_j \cdot p_{i_1} \cdots p_{i_k}}$, and $u = \frac{n_j}{p_{i_1} \cdots p_{i_k}} = \frac{n}{p_j \cdot p_{i_1} \cdots p_{i_k}}$. Since η is a primitive u-th root of unity, it follows from Lemma 4.6 that the last sum is an integer. Hence, every sum of the form $\sum\limits_{r \in D_{i_1 \ldots i_k}} \left(\varepsilon^{p_j c}\right)^r$ is an integer, and consequently, V is an integer. We already know that U is an integer. Therefore, $W_j = U - V$ is an integer. □

5. Special numbers

As in the previous section, let $n = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$, where $p_1, \ldots, p_s$ are distinct primes and $\alpha_1, \ldots, \alpha_s$ are positive integers. Put $n_j = \frac{n}{p_j}$ for $j = 1, \ldots, s$. Assume that $[p_1, \ldots, p_n]$ is a fixed type, and $I_1, \ldots, I_s$ are the n-sets of type $[p_1, \ldots, p_s]$. If $j \in \{1, \ldots, s\}$ and $0 \leqslant r < n_j$, then we have the standard minimal element $m(p_j, r) = \sum_{i=0}^{p_j - 1} e_{r + i n_j}$. Let us recall that each $m(p_j, r)$ belongs to the monoid $\mathcal{M}_n$, and it is a minimal element of $\mathcal{M}_n$. Moreover, $n_j = \frac{n}{p_j}$ for $j = 1, \ldots, s$.

The main role in this section will play the sets $\mathcal{A}_1, \ldots, \mathcal{A}_s$, which are subsets of the monoid $\mathcal{M}_n$. We define these subsets as follows

$$\mathcal{A}_j = \Big\{ m(p_j, r);\ r \in I_j \Big\},$$

for all $j = 1, \ldots, s$. We denote by $\mathcal{A}$ the union $\mathcal{A} = \mathcal{A}_1 \cup \cdots \cup \mathcal{A}_s$. Note that the above sets $\mathcal{A}$ and $\mathcal{A}_1, \ldots, \mathcal{A}_s$ are determined by the fixed succession $P = [p_1, \ldots, q_n]$ of the primes $p_1, \ldots, p_s$. In our case we will say that $\mathcal{A}$ is the *n-standard set of type P*.

Observe that the sets $\mathcal{A}_1, \ldots, \mathcal{A}_s$ are pairwise disjoint, and as a consequence of Proposition 4.5 we have the equality $|\mathcal{A}| = n - \varphi(n)$.

Let us recall (see Theorem 2.3) that the group $\mathcal{G}_n$ is a free $\mathbb{Z}$-module, and its rank is equal to $n - \varphi(n)$, so this rank is equal to $|\mathcal{A}|$. We are interested in finding conditions for $\mathcal{A}$ to be a basis of $\mathcal{G}_n$. First we need $\mathcal{A}$ to be linearly independent over $\mathbb{Z}$.

Special numbers will then be convenient to prove Theorem 9.1. We will say that the number n is *special of type* P if the n-standard set $\mathcal{A}$ of type P is linearly independent over $\mathbb{Z}$. Moreover, we will say that the number n is *special* if there exists a type P for which n is special of type P. We will say that the number n is *absolutely special* if it is special with respect to any type P.

Example 5.1. Let $n = 12 = 2^2 3$ and consider the type $[2, 3]$. In this case we have: $s = 2$, $p_1 = 2$, $p_2 = 3$, $n_1 = 6$, $n_2 = 4$, $I_1 = \{0, 1, 2, 3, 4, 5\}$ and $I_2 = \{1, 3\}$. The 12-standard set $\mathcal{A}$ of type $[2, 3]$ is the set of the following 8 sequences:

$$\begin{array}{rcl}
m(2,0) & = & (1,0,0,0,0,0,1,0,0,0,0,0),\\
m(2,1) & = & (0,1,0,0,0,0,0,1,0,0,0,0),\\
m(2,2) & = & (0,0,1,0,0,0,0,0,1,0,0,0),\\
m(2,3) & = & (0,0,0,1,0,0,0,0,0,1,0,0),\\
m(2,4) & = & (0,0,0,0,1,0,0,0,0,0,1,0),\\
m(2,5) & = & (0,0,0,0,0,1,0,0,0,0,0,1),\\
m(3,1) & = & (0,1,0,0,0,1,0,0,0,1,0,0),\\
m(3,3) & = & (0,0,0,1,0,0,0,1,0,0,0,1).
\end{array}$$

Observe that $m(2, 1) + m(2, 3) + m(2, 5) = m(3, 1) + m(3, 3)$. Hence, the set $\mathcal{A}$ is not linearly independent over $\mathbb{Z}$. This means, that 12 is not a special number of type $[2, 3]$.

Now consider $n = 12$ and the type $[3, 2]$. In this case $p_1 = 3$, $p_2 = 2$, $n_1 = 4$, $n_2 = 6$, $I_1 = \{0, 1, 2, 3\}$ and $I_2 = \{1, 2, 2, 5\}$. The 12-standard set $\mathcal{A}$ of type $[3, 2]$ is in this case the set of the following 8 sequences:

$$\begin{array}{rcl}
m(3,0) & = & (1,0,0,0,1,0,0,0,1,0,0,0),\\
m(3,1) & = & (0,1,0,0,0,1,0,0,0,1,0,0),\\
m(3,2) & = & (0,0,1,0,0,0,1,0,0,0,1,0),\\
m(3,3) & = & (0,0,0,1,0,0,0,1,0,0,0,1),\\
m(2,1) & = & (0,1,0,0,0,0,0,1,0,0,0,0),\\
m(2,2) & = & (0,0,1,0,0,0,0,0,1,0,0,0),\\
m(2,4) & = & (0,0,0,0,1,0,0,0,0,0,1,0),\\
m(2,5) & = & (0,0,0,0,0,1,0,0,0,0,0,1).
\end{array}$$

It is easy to check that in this case the set $\mathcal{A}$ is linearly independent over $\mathbb{Z}$. Thus, 12 is a special number of type $[3, 2]$, and 12 is not a special number of type $[2, 3]$.

$\square$

We will prove that the number n is absolutely special if and only if either n is square-free or n is a power of a prime number. Moreover, we will prove that the number n is special if and only if $n = p_1 p_2 \cdots p_{s-1} p_s^{\alpha_s}$, where $p_1, \ldots, p_s$ are distinct primes and $\alpha_s \geqslant 1$.

Proposition 5.2. *Every power of a prime is an absolutely special number.*

Proof. Let $n = p^m$, where p is a prime and $m \geqslant 1$. Then $s = 1$, $n_1 = p^{m-1}$, $I_1 = \{0, 1, \ldots, p^{m-1} - 1\}$ and there is only one type $P = [p]$. Thus, $\mathcal{A} = \mathcal{A}_1$ and, by Proposition 3.2, the set $\mathcal{A}$ is linearly independent over $\mathbb{Z}$. □

Lemma 5.3. *Let p be a prime number, and let $N \geqslant 2$ be an integer such that $p \nmid N$. Then, for every integer r, there exists a unique $c_r \in \{0, 1, \ldots, p-1\}$ such that the number $r + c_r N$ is divisible by p. Moreover, all numbers of the form $r + c_r N$ with $0 \leqslant r < N$ are pairwise different.*

Proof. Let $r \in \mathbb{Z}$. Consider the integers $r, r + N, r + 2N, \ldots, r + (p-1)N$, and observe that these numbers are pairwise noncongruent modulo p. Thus, there exists a unique $c_r \in \{0, 1, \ldots, p-1\}$ such that $r + c_r N = 0 \pmod p$. Assume that $r_1 + c_{r_1} N = r_2 + c_{r_2} N$ for some $r_1, r_2 \in \{0, 1, \ldots, N-1\}$. Then $N \mid r_1 - r_2$ and so, $r_1 = r_2$. □

Despite the fact that we need the full Theorem 5.10 ($\mathcal{A}$ generates $\mathcal{G}_n$), we first state and prove the following Proposition ($\mathcal{A}$ is linearly independent over $\mathbb{Z}$) for a better understanding. This Proposition is not equivalent, as $\mathcal{A}$ could generate a subgroup of $\mathcal{G}_n$ of finite index.

Proposition 5.4. *Let $n = p_1 \cdots p_{s-1} \cdot p_s^\alpha$, where $s \geqslant 2$, $\alpha \geqslant 1$, and $p_1, \ldots, p_s$ are distinct primes. Then n is a special number of every type of the form $\big[p_{\sigma(1)}, \ldots, p_{\sigma(s-1)}, p_s\big]$,where σ is a permutation of $\{1, \ldots, s-1\}$.*

Proof. Let P be a fixed type with p_s at the end. Without loss of generality, we may assume that $P = [p_1, \ldots, p_{s-1}, p_s]$. Let $I_1, \ldots, I_s$ be n-sets of type P, and assume that

$$(a) \qquad \sum_{j=1}^{s} \left(\sum_{r \in I_j} \gamma_r^{(j)} m(p_j, r) \right) = (0, 0, \ldots, 0),$$

where each $\gamma_r^{(j)}$ is an integer. We will show that $\gamma_r^{(j)} = 0$ for all j, r.

Note, that every standard element $u = m(p_j, r)$ is a sequence $(u_0, u_1, \ldots, u_{n-1})$, where all $u_0, \ldots, u_{n-1}$ are integers belonging to $\{0, 1\}$. We will denote by $S(u)$ the support of u, that is, $S(u) = \Big\{k \in \{0, 1, \ldots, n-1\};\ u_k = 1\Big\}$.

Consider the case $j = 1$. Put $p = p_1$ and $N = n_1 = \frac{n}{p} = p_2 p_3 \ldots p_{s-1} \cdot p_s^\alpha$. Observe that $p \nmid N$, and all the numbers $n_2, \ldots, n_s$ are divisible by p. Let $u = m(p_j, r)$ with $r \in I_j$, where $j \geqslant 2$. Then $p \nmid r$, and

$$S(u) = \{r,\ r + n_j,\ r + 2n_j,\ \ldots,\ r + (p_j - 1)n_j\},$$

and hence, all the elements of $S(u)$ are not divisible by p.

Look at the support of $m(p_1, r)$ with $r \in I_1$. We have $S\Big(m(p_1, r)\Big) = \Big\{r,\ r + N,\ r + 2N,\ \ldots,\ r + (p-1)N\Big\}$. It follows from Lemma 5.3 that in this support there exists exactly one element divisible by p. Let us denote this element by $r + c_r N$.

We know also from the same lemma, that all the elements $r + c_r N$ with $r \in I_1$ are pairwise different. These arguments imply, that in the equality (a) all the integers $\gamma_r^{(1)}$, with $r \in I_1$, are equal to zero.

Now let $2 \leqslant j_0 < s$, and assume that we already proved the equalities $\gamma_r^{(j)} = 0$ for all $j < j_0$ and $r \in I_j$. Then the equality (a) is of the form

$$(b) \qquad \sum_{j=j_0}^{s} \left(\sum_{r \in I_j} \gamma_r^{(j)} m(p_j, r) \right) = (0, 0, \dots, 0),$$

We will show that $\gamma_r^{(j_0)} = 0$ for all $r \in I_{j_0}$.

Put $p = p_{j_0}$ and $N = n_{j_0} = \frac{n}{p}$. Observe that $p \nmid N$, and all the numbers n_j with $j > j_0$ are divisible by p. Let $u = m(p_j, r)$ with $r \in I_j$, where $j > j_0$. Then $p \nmid r$, and

$$S(u) = \{r,\ r + n_j,\ r + 2n_j,\ \dots,\ r + (p_j - 1)n_j\},$$

and hence, all the elements of $S(u)$ are not divisible by p.

Look at the support of $m(p_{j_0}, r)$ with $r \in I_{j_0}$. We have $S\Big(m(p_{j_0}, r)\Big) = \Big\{r,\ r + N,\ r+2N,\ \dots,\ r+(p-1)N\Big\}$. It follows from Lemma 5.3 that in this support there exists exactly one element divisible by p. Let us denote this element by $r + c_r N$. We know also from the same lemma, that all the elements $r + c_r N$ with $r \in I_{j_0}$ are pairwise different. These arguments imply, that in the equality (b) all the integers $\gamma_r^{(j_0)}$, with $r \in I_{j_0}$, are equal to zero.

Hence, by the induction hypothesis, the equality (b) reduces to the equality

$$\sum_{r \in I_s} \gamma_r^{(s)} m(p_s, r) = (0, 0, \dots, 0),$$

where each $\gamma_r(s)$ is an integer. Now we use Proposition 3.2 and we have $\gamma_r(s) = 0$ for all $r \in I_s$. Thus, we proved that in the equality (a) all the integers of the form γ_r^j, where $j \in \{1, \dots, s\}$ and $r \in I_j$, are equal to zero. This means that the n-standard set $\mathcal{A}$ of type P is linearly independent over $\mathbb{Z}$. Therefore, n is a special number of type P. □

Using the above proposition for $\alpha = 1$ we obtain

Proposition 5.5. *Every square-free integer $n \geqslant 2$ is absolutely special.*

Lemma 5.6. *Let $n = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$, where $s \geqslant 2$, $p_1, \dots, p_s$ are distinct prime numbers and $\alpha_1, \dots, \alpha_s$ are positive integers. Let $P = [p_1, \dots, p_s]$. If $\alpha_1 \geqslant 2$, then n is not a special number of type P.*

Proof. Put $p = p_1$, $q = p_2$, $u = \frac{n}{p^2}$, $v = \frac{n}{pq}$, $a = \sum_{k=0}^{u-1} m(p, pk + 1)$, $b = \sum_{k=0}^{v-1} m(q, pk + 1)$. Observe that a is a sum of elements from $\mathcal{A}_1$, and b is a sum of elements from

$\mathcal{A}_2$. Moreover, $n_1 = \frac{n}{p} = pu$, $n_2 = \frac{n}{q} = pv$,

$$a = \sum_{k=0}^{u-1}\sum_{i=0}^{p-1} e_{pk+1+in_1} = \sum_{k=0}^{u-1}\sum_{i=0}^{p-1} e_{pk+1+ipu} = \sum_{k=0}^{u-1}\sum_{i=0}^{p-1} e_{p(k+iu)+1} = \sum_{j=0}^{n_1-1} e_{pj+1},$$

$$b = \sum_{k=0}^{v-1}\sum_{i=0}^{q-1} e_{pk+1+in_2} = \sum_{k=0}^{v-1}\sum_{i=0}^{q-1} e_{pk+1+ipv} = \sum_{k=0}^{v-1}\sum_{i=0}^{q-1} e_{p(k+iv)+1} = \sum_{j=0}^{n_1-1} e_{pj+1}.$$

Hence, $a = \sum_{j=0}^{n_1-1} e_{pj+1} = b$. This implies that the n-standard set $\mathcal{A}$ of type P is not linearly independent over $\mathbb{Z}$. Thus, n is not a special number of type P. □

Lemma 5.7. *Let $n = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$, where $s \geqslant 2$, $p_1, \dots, p_s$ are distinct prime numbers and $\alpha_1, \dots, \alpha_s$ are positive integers. Let $P = [p_1, \dots, p_s]$. If there exists $j_0 \in \{1, 2, \dots, s-1\}$ such that $\alpha_{j_0} \geqslant 2$, then n is not a special number of type P.*

Proof. If $j_0 = 1$ then the assertion follows from Lemma 5.6. Assume that $j_0 \geqslant 2$, and let $\mathcal{A}_1, \dots, \mathcal{A}_s$ be the n-standard sets of type P. Put $N = p_1^{\alpha_1} \cdots p_{j_0-1}^{\alpha_{j_0-1}}$, $p = p_{j_0}$, $q = p_{j_0+1}$, $u = \frac{n}{Np^2}$, $v = \frac{n}{Npq}$, $w = \frac{n}{pN}$, $a = \sum_{k=0}^{u-1} m(p, pNk+1)$, and $b = \sum_{k=0}^{v-1} m(q, pNk+1)$. Observe that a is a sum of elements from $\mathcal{A}_{j_0}$, and b is a sum of elements from $\mathcal{A}_{j_0+1}$. Moreover, $n_{j_0} = \frac{n}{p} = pNu$, $n_{j_0+1} = \frac{n}{q} = pNv$,

$$\begin{aligned} a &= \sum_{k=0}^{u-1}\sum_{i=0}^{p-1} e_{pNk+1+in_{j_0}} = \sum_{k=0}^{u-1}\sum_{i=0}^{p-1} e_{pNk+1+ipNu} \\ &= \sum_{k=0}^{u-1}\sum_{i=0}^{p-1} e_{pN(k+iu)+1} = \sum_{j=0}^{w-1} e_{pNj+1}, \\ b &= \sum_{k=0}^{v-1}\sum_{i=0}^{q-1} e_{pNk+1+in_{j_0+1}} = \sum_{k=0}^{v-1}\sum_{i=0}^{q-1} e_{pNk+1+ipNv} \\ &= \sum_{k=0}^{v-1}\sum_{i=0}^{q-1} e_{pN(k+iv)+1} = \sum_{j=0}^{w-1} e_{pNj+1}. \end{aligned}$$

Hence, $a = \sum_{j=0}^{w-1} e_{pNj+1} = b$, where $w = \frac{n}{pN}$. This implies that the n-standard set $\mathcal{A}$ of type P is not linearly independent over $\mathbb{Z}$. Thus, n is not a special number of type P. □

As a consequence of the above facts we obtain the following theorems.

Theorem 5.8. *An integer $n \geqslant 2$ is special if and only if $n = p_1 p_2 \cdots p_{s-1} p_s^{\alpha_s}$, where $p_1, \dots, p_s$ are distinct primes and $\alpha_s \geqslant 1$.*

Theorem 5.9. *An integer $n \geqslant 2$ is absolutely special if and only if either n is square-free or n is a power of a prime number.*

The smallest non-special positive integer $n \geqslant 2$ is $n = 36$. In the segment $[2, 100]$ there are 3 non-special numbers: 36, 72 and 100.

Let us recall that if n is a special number, then its n-standard set $\mathcal{A}$ is linearly independent over $\mathbb{Z}$. Now we will show that, in this case, the set $\mathcal{A}$ is a basis of $\mathcal{G}_n$. Let us denote by $\overline{\mathcal{A}}$ the subgroup of $\mathcal{G}_n$ generated by $\mathcal{A}$. Every element of $\overline{\mathcal{A}}$ is a finite combination over $\mathbb{Z}$ of some elements of $\mathcal{A}$.

We already know (see Theorem 3.5) that the group $\mathcal{G}_n$ is generated by all the standard minimal elements of $\mathcal{M}_n$. Thus, for a proof that $\mathcal{A}$ is a basis of $\mathcal{G}_n$, it suffices to prove that every standard minimal element of $\mathcal{M}_n$ belongs to $\overline{\mathcal{A}}$.

Theorem 5.10. *Let $n = p_1 \cdots p_{s-1} p_s^{\alpha}$, where $s \geqslant 1$, $\alpha \geqslant 1$, and $p_1, \dots, p_s$ are pairwise different primes. Let $P = [p_1, \dots, p_s]$, and let $\mathcal{A}$ be the n-standard set of type P. Then every standard minimal element of $\mathcal{M}_n$ belongs to $\overline{\mathcal{A}}$.*

Proof. First, all p_1-standard elements $m(p_1, r)$ with $0 \leqslant r < \frac{n}{p_1}$ belong to $\mathcal{A}_1$ and thus to $\overline{\mathcal{A}}$.

To go further, for $j > 1$, we will use the relations given in Proposition 3.3 and we define therefore the *height* of a p_j-standard element (that may not belong to $\mathcal{A}_j$) as the number of primes among $\{p_1, \cdots, p_{j-1}\}$ that divide r and denote it by $h(m(p_j, r))$. Elements of $\mathcal{A}_j$ have height 0. A p_j-standard element has an height at most $j - 1$.

By definition all standard elements of height 0 belong to $\mathcal{A}$ and thus to $\overline{\mathcal{A}}$.

To achieve the proof by induction, we use the following fact.

Key fact. For $j > 1$, let $m(p_j, r)$ be a p_j-standard element with a non-zero height. Then some of the $p_i, 1 \leq i < j$ divide r. Let then denote by p one of them and p_j by q.

As all prime factors but the last have exponent 1 in the decomposition of n, when we apply Proposition 3.3, $N = n/pq$ is coprime with p and a multiple of all p_l, $1 \leq l < j$, $l \neq i$.

For any k, $1 \leq k \leq p - 1$, $r + kN$ is coprime with p and keeps the same other divisors among the other $p_l, 1 \leq l < j, l \neq i$: the height $h(m(p_j, r + lN))$ is then $h(m(p_j, r)) - 1$.

Whence the following relation we get from Proposition 3.3

$$m(q, r) = \sum_{k=0}^{q-1} m(p, kN + r) - \sum_{k=1}^{p-1} m(q, kN + r).$$

which means

$$m(p_j, r) = \sum_{k=0}^{q-1} m(p_i, kN + r) - \sum_{k=1}^{p-1} m(p_j, kN + r).$$

and $m(p_j, r)$ is a $\mathbb{Z}$-linear combination of some $m(p_j, r')$ with a strictly smaller height and of some $m(p_i, r'')$ for an index $i < j$.

The proof is now a *double induction* with the following steps.

Let $j > 1$ and suppose that all $m(p_i, r)$ have been proven to belong to $\overline{\mathcal{A}}$ for all $i < j$.

All $m(p_j, r)$ with a 0 height belong to $\mathcal{A}_j$ and then to $\overline{\mathcal{A}}$.

For any $h', 1 \leq h' < j$, if we know that all $m(p_j, r)$ with $h(m(p_j, r)) < h'$ belong to $\overline{\mathcal{A}}$, then the same is true for all $m(p_j, r)$ with $h(m(p_j, r)) = h'$ according to the previous *key fact*. $\square$

6. The cyclotomic derivation d

Throughout this section $n \geqslant 3$ is an integer, K is a field of characteristic zero, $K[X] = K[x_0, \dots, x_{n-1}]$ is the polynomial ring over K in variables $x_0, \dots, x_{n-1}$, and $K(X) = K(x_0, \dots, x_{n-1})$ is the field of quotients of $K[X]$. We denote by $\mathbb{Z}_n$ the ring $\mathbb{Z}/n\mathbb{Z}$. The indexes of the variables $x_0, \dots, x_{n-1}$ are elements of $\mathbb{Z}_n$. We denote by d the cyclotomic derivation of $K[X]$, that is, d is the K-derivation of $K[X]$ defined by

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

We denote also by d the unique extension of d to $K(X)$. We denote by $K[X]^d$ and $K(X)^d$ the K-algebra of constants of d and the field of constants of d, respectively. Thus,

$$K[X]^d = \{F \in K[X];\ d(F) = 0\}, \quad K(X)^d = \{f \in K(X);\ d(f) = 0\}.$$

Now we recall from [10] some basic notions and facts concerning the derivation d. As in the previous sections, we denote by ε a primitive n-th root of unity, and first we assume that $\varepsilon \in K$.

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

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

Observe that $\varrho d \varrho^{-1} = d$. We denote by $u_0, u_1, \dots, u_{n-1}$ the linear forms, belonging to $K[X]$, defined by

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

Then we have the equalities

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

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,

$$\tau(u_j) = u_{j+1}, \quad \varrho(u_j) = \varepsilon^{-j}u_j, \quad d(u_j) = \varepsilon^{-j}u_j,$$

for all $j \in \mathbb{Z}_n$.

It follows from the last equality 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 $K[X]$.

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 Section 2) that $H_\alpha(t)$ is the polynomial $\alpha_0 + \alpha_1 t^1 + \cdots + \alpha_{n-1}t^{n-1}$ belonging to $\mathbb{Z}[t]$. Since $d(u_j) = \varepsilon^{-j}u_j$ for all $j \in \mathbb{Z}_n$, we have

$$d(u^\alpha) = H_\alpha(\varepsilon^{-1})u^\alpha, \quad \text{for all } \alpha \in \mathbb{Z}^n.$$

Note that ε^{-1} is also a primitive n-th root of unity. Hence, by Proposition 2.1, we have the equivalence $H_\alpha(\varepsilon^{-1}) = 0 \iff H_\alpha(\varepsilon) = 0$, and so, 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 $F = b_1u^{\alpha^{(1)}} + \cdots + b_ru^{\alpha^{(r)}}$, where $b_1, \dots, b_r \in K$ and $\alpha^{(1)}, \dots, \alpha^{(r)}$ are pairwise different elements of $\mathbb{N}^n$, then $d(F) = 0$ if and only if $d\left(b_iu^{\alpha^{(i)}}\right) = 0$ for every $i = 1, \dots, r$. In [10] we proved the following proposition.

Proposition 6.1 ([10]). *If the primitive n-th root ε belongs to K, then:*

(1) *the ring $K[X]^d$ is generated over K by all elements of the form u^α with $\alpha \in \mathcal{M}_n$;*

(2) *the ring $K[X]^d$ is generated over K by all elements of the form u^β, where β is a minimal element of the monoid $\mathcal{M}_n$;*

(3) *the field $K(X)^d$ is generated over K by all elements of the form u^γ with $\gamma \in \mathcal{G}_n$;*

(4) *the field $K(X)^d$ is the field of quotients of the ring $K[X]^d$.*

Let $m = n - \varphi(n)$, and let $\gamma_0, \dots, \gamma_{m-1}$ be the elements of $\mathcal{G}_n$ introduced in Section 2. We know (see Theorem 2.3) that these elements form a basis of the group $\mathcal{G}_n$. Consider now the rational monomials $w_0, \dots, w_{m-1}$ defined by

$$w_j = u^{\gamma_j} \quad \text{for } j = 0, 1, \dots, m-1.$$

It follows from Proposition 6.1, that these monomials belong to $K(X)^d$ and they generate the field $K(X)^d$. We proved in [10] that they are algebraically independent over K. Moreover, in [10] proved the following theorem.

Theorem 6.2. *If the primitive n-th root ε belongs to K, then 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,*

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

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

7. The polynomials $S_{p,m}$

In this section we use the notations from the previous section, and we again assume that K is a field of characteristic zero containing ε. Let us recall that if p is a prime divisor of n and $0 \leqslant r \leqslant \frac{n}{p} - 1$, then $m(p,r)$, is the standard minimal element of the monoid $\mathcal{M}_n$ defined by $m(p,r) = \sum_{i=0}^{p-1} e_{r+i\frac{n}{p}}$. Observe that if a, b are integers such that $a \equiv b \,(\mathrm{mod}\ \frac{n}{p})$, then $\sum_{i=0}^{p-1} e_{a+i\frac{n}{p}} = \sum_{i=0}^{p-1} e_{b+i\frac{n}{p}}$. Thus, we may define

$$m(p,a) := \sum_{i=0}^{p-1} e_{a+i\frac{n}{p}}, \quad \text{for} \quad a \in \mathbb{Z}.$$

Note, that if $a \in \mathbb{Z}$, then $m(p,a) = m(p,r)$, where r is the remainder of division of a by $\frac{n}{p}$. Moreover, $\zeta^{\frac{n}{p}}\Big(m(p,b)\Big) = m(p,b)$ for $b \in \mathbb{Z}$, and more general, $\zeta^a\Big(m(p,b)\Big) = m(p, a+b)$ for all $a, b \in \mathbb{Z}$ (see Proposition 3.4).

For every integer a, we define

$$S_{p,a} := u^{m(p,a)} = \prod_{i=0}^{p-1} u_{a+i\frac{n}{p}}.$$

Observe that $S_{p,a} = S_{p,r}$, where r is the remainder of division of a by $\frac{n}{p}$. Each $S_{p,a}$ is a monomial belonging to $K[U] = K[u_0, \dots, u_{n-1}]$. Since $m(p,a) \in \mathcal{M}_n \subset \mathcal{G}_n$, each $S_{p,a}$ belongs to the constant field $K(X)^d$.

Recall (see Section 6) that ϱ is the K-automorphism of the field $K(X)$, defined by

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

We have $\varrho(u_j) = \varepsilon^{-j} u_j$ for $j \in \mathbb{Z}_n$. In particular, $\varrho(u_0) = u_0$. The proof of the following proposition is an easy exercise.

Proposition 7.1. *If $a \in \mathbb{Z}$, then $\varrho\left(S_{p,a}\right) = \varepsilon^{-b} S_{p,a}$, where $b = pa + \frac{(p-1)n}{2}$. In particular, if p is odd then $\varrho\left(S_{p,a}\right) = \varepsilon^{-ap} S_{p,a}$. If $p = 2$, then n is even and $\varrho\left(S_{2,a}\right) = \varepsilon^{-\left(2a + \frac{n}{2}\right)} S_{2,a}$.*

Recall the following well known lemma, which appears in many books of linear algebra.

Lemma 7.2. *For any integer $n \geqslant 2$,*

$$u_0u_1\dots u_{n-1} = \begin{vmatrix} x_0 & x_1 & \cdots & x_{n-1} \\ x_{n-1} & x_0 & \cdots & x_{n-2} \\ \vdots & \vdots & & \vdots \\ x_1 & x_2 & \cdots & x_0 \end{vmatrix}.$$

In particular, the product $u_0u_1\dots u_{n-1}$ is a polynomial belonging to $\mathbb{Z}[X]$.

Using this lemma we obtain the following proposition.

Proposition 7.3. *The polynomial $S_{p,0}$ belongs to $\mathbb{Z}[X]$.*

Proof. Put $b = \frac{n}{p}$, $\eta = \varepsilon^b$, and $v_i = u_{ib}$, $y_i = \sum_{j=0}^{b-1} x_{i+jp}$ for all $i = 0, 1, \dots, p-1$, Then η is a primitive p-th root of unity, and $v_i = \sum_{k=0}^{p-1} \left(\eta^i\right)^k y_k$, for all $i = 0, 1, \dots, p-1$. Now we use Lemma 7.2, and we have

$$S_{p_j,0} = v_0v_1\cdots v_{p-1} = \begin{vmatrix} y_0 & y_1 & \cdots & y_{p-1} \\ y_{p-1} & y_0 & \cdots & y_{p-2} \\ \vdots & \vdots & & \vdots \\ y_1 & y_2 & \cdots & y_0 \end{vmatrix}.$$

Thus, $S_{p_j,0} \in \mathbb{Z}[X]$. □

Let $n = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$, where $p_1, \dots, p_s$ are distinct primes and $\alpha_1, \dots, \alpha_s$ are positive integers. Let $n_j = \frac{n}{p_j}$ for $j = 1, \dots, s$. Assume that $P = [p_1, \dots, p_n]$ is a fixed type, and $I_1, \dots, I_s$ are the n-sets of type P.

For every $j \in \{1, \dots, s\}$ we denote by $\mathcal{V}_j$ the K-subspace of $K[U]$ generated by all the monomials $S_{p_j,r}$ with $r \in I_j$. Let us remember

$$\mathcal{V}_j = \left\langle S_{p_j,r};\ r \in I_j \right\rangle, \quad \text{for} \quad j = 1, \dots, s.$$

We will say that $\mathcal{V}_1, \dots, \mathcal{V}_s$ are *n-spaces of type P*. As a consequence of Propositions 4.3 and 4.5 we obtain the following proposition.

Proposition 7.4. *If $\mathcal{V}_1, \dots, \mathcal{V}_s$ are n-spaces of type $P = [p_1, \dots, p_s]$, then $\dim_K \mathcal{V}_1 = n_1$, and $\dim_K \mathcal{V}_j = n_j \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_{j-1}}\right)$, for all $j = 2, 3, \dots, s$. Moreover,*

$$\dim_K \left(\mathcal{V}_1 \oplus \cdots \oplus \mathcal{V}_s\right) = n - \varphi(n).$$

Let $\mathcal{A}$ be the n-standard set of type P. Let us recall (see Section 5) that $\mathcal{A} = \mathcal{A}_1 \cup \cdots \cup \mathcal{A}_s$, where $\mathcal{A}_j = \{p(p_j, r);\ r \in I_j\}$ for $j = 1, \dots, s$. Hence, for each j we have the equality $\mathcal{V}_j = \langle u^a;\ a \in \mathcal{A}_j \rangle$. Let $\mathcal{S}$ the set of all the monomials u^a with $a \in \mathcal{A}$, that is,

$$\mathcal{S} = \Big\{S_{p_j,r};\ j \in \{1, \dots, s\},\ r \in I_j\Big\}.$$

Proposition 7.5. *If the number n is special of type P, then the above set $\mathcal{S}$ is algebraically independent over K, and $K(X)^d = K(\mathcal{S})$.*

Proof. Assume that n is special of type P. Let $\gamma_0, \dots, \gamma_{m-1}$ be the elements of $\mathcal{G}_n$ defined in Section 2, and let $w_i = u^{\gamma_i}$ for $i = 0, \dots, m-1$. Recall that $m = n - \varphi(n)$. Put $\Gamma = \{\gamma_0, \dots, \gamma_{m-1}\}$, and $W = \{w_0, \dots, w_{m-1}\}$. We know (see Theorem 2.3) that Γ is a basis of $\mathcal{G}_n$. Since n is special, the set $\mathcal{A}$ is also a basis of $\mathcal{G}_n$. This implies that $K(\mathcal{S}) = K(W)$. But, by Theorem 6.2, the set W is algebraically independent over K and $K(W) = K(X)^d$. Moreover, $|\mathcal{S}| = |W| = m$ Hence, the set $\mathcal{S}$ is also algebraically independent over K, and we have the equality $K(X)^d = K(\mathcal{S})$. □

In the above proposition we assumed that n is special of type P. This assumption is very important. Consider for example $n = 12$ and $P = [2, 3]$. We know (see Example 5.1) that 12 is not special of type P. In this case the set $\mathcal{S}$ is not algebraically independent over K. In fact, we have the polynomial equality $S_{2,1}S_{2,3}S_{2,5} = S_{3,1}S_{3,3}$.

8. The polynomials $\mathrm{T}_{p,m}$

Let $n = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$, where $p_1, \dots, p_s$ are distinct prime numbers and $\alpha_1, \dots, \alpha_s$ are positive integers. Let $n_j = \frac{n}{p_j}$ for $j = 1, \dots, s$. Assume that $P = [p_1, \dots, p_n]$ is a fixed type, and $I_1, \dots, I_s$ are the n-sets of type P.

Now assume that j is a fixed element from the set $\{1, \dots, s\}$, and a is an integer. Put

$$T_{p_j,a} = \sum_{r \in I_j} \left(\varepsilon^{-ap_j}\right)^r S_{p_j,r}.$$

Observe that $T_{p_j,a} = T_{p_j,m}$, where m is the remainder of division of a by n_j. Let us recall that $\varepsilon \in K$. Thus, every $T_{p_j,a}$ is a polynomial from $K[U]$ belonging to the subspace $\mathcal{V}_j$.

Proposition 8.1. *For every $j = 1, \dots, s$, all the polynomials $T_{p_j,m}$ with $0 \leqslant m < n_j$, generate the K-space $\mathcal{V}_j$.*

Proof. Let $q \in I_j$ and consider the sum $H = \sum_{m=0}^{n_j-1} \left(\varepsilon^{qp_j}\right)^m T_{p_j,m}$. Put $\eta = \varepsilon^{p_j}$. Then η is a primitive n_j-th root of unity, and we have

$$\begin{aligned} H &= \sum_{m=0}^{n_j-1} \left(\varepsilon^{qp_j}\right)^m \left(\sum_{r \in I_j} \varepsilon^{rp_jm} S_{p_j,r} \right) = \sum_{r \in I_j} \left(\sum_{m=0}^{n_j-1} \varepsilon^{(q-r)p_jm} \right) S_{p_j,r} \\ &= \sum_{r \in I_j} \left(\sum_{m=0}^{n_j-1} \eta^{(q-r)m} \right) S_{p_j,r} = n_j S_{p_j,q}. \end{aligned}$$

In the last equality we used Lemma 4.6. Thus, if $q \in I_j$, then $S_{p_j,q} = \frac{1}{n_j}\sum_{m=0}^{n_j-1} (\varepsilon^{qp_j})^m T_{p_j,m}$. But $\varepsilon \in K$, so now it is clear that all $T_{p_j,m}$ with $0 \leqslant m < n_j$, generate the K-space $\mathcal{V}_j$. □

Now we will prove that every polynomial $T_{p_j,a}$ belongs to the ring $\mathbb{Z}[X]$. For this aim first recall (see Section 6) that τ is a K-automorphism of $K(X)$ defined by

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

Since $\tau(u_i) = u_{i+1}$ for all $i \in \mathbb{Z}_n$, we have

$$S_{p_j,r} = \tau^r\left(S_{p_j,0}\right)$$

for $j \in \{1, \dots, s\}$ and $r \in \mathbb{Z}$ (in particular, for $r \in I_j$). We say (us in [10]) that a rational function $f \in K(X)$ is *τ-homogeneous*, if f is homogeneous in the ordinary sense and $\tau(f) = \varepsilon^c f$ for some $c \in \mathbb{Z}_n$. In this case we say that c is the τ-degree of f and we write $\deg_\tau(f) = c$. Note that $\deg_\tau(f)$ is an element of $\mathbb{Z}_n$. Every rational monomial $x^\alpha = x_0^{\alpha_0}\cdots x_{n-1}^{\alpha_{n-1}}$, where $\alpha = (\alpha_0, \dots, \alpha_{n-1}) \in \mathbb{Z}^n$, is τ-homogeneous and its τ-degree is equal to $\sum_{i=0}^{n-1} i\alpha_i \pmod{n}$.

Let j be a fixed number from $\{1, \dots, s\}$ and consider the polynomial $S_{p_j,0}$. We know by Proposition 7.3 that this polynomial belongs to $\mathbb{Z}[X]$. Hence, we have the unique determined polynomials $B_0, \dots, B_{n-1} \in \mathbb{Z}[X]$ such that $S_{p_j,0} = B_0 + \cdots + B_{n-1}$, and each B_i is τ-homogeneous of τ-degree i.

Put $C_i = \tau^{n_j}(B_i)$, for all $i = 0, \dots, n-1$. Since $\tau(B_i) = \varepsilon^i B_i$, we have $C_i = \varepsilon^{in_j} B_i$, and this implies that $\tau(C_i) = \varepsilon^i C_i$. In fact,

$$\tau(C_i) = \tau\left(\tau^{n_j}(B_i)\right) = \tau\left(\varepsilon^{in_j} B_i\right) = \varepsilon^{in_j}\tau(B_i) = \varepsilon^{in_j}\cdot\varepsilon^i B_i = \varepsilon^i\cdot\varepsilon^{in_j} B_i = \varepsilon^i C_i.$$

Thus, every polynomial C_i is τ-homogeneous of τ-degree i. Observe that

$$\tau^{n_j}\left(S_{p_j,0}\right) = S_{p_j,0}.$$

But $\tau^{n_j}\left(S_{p_j,0}\right) = \sum_{i=0}^{n-1} C_i$, so $C_i = \tau^{n_j}(B_i) = B_i$ and so, $\varepsilon^{in_j} B_i = B_i$, for all $i = 0, \dots, n-1$. Thus, if $B_i \neq 0$, then $n \mid in_j$. But $n = p_j n_j$ so, if $B_i \neq 0$, then i is divisible by p_j. Therefore,

$$S_{p_j,0} = \sum_{k=0}^{n_j-1} B_{kp_j},$$

where each B_{kp_j} is τ-homogeneous polynomial from $\mathbb{Z}[X]$ of τ-degree kp_j. Hence, for every $m \in \{0, \ldots, n-1\}$, we have

$$\begin{aligned} T_{p_j,m} &= \sum_{r\in I_j} \varepsilon^{-rp_jm} S_{p_j,r} = \sum_{r\in I_j} \varepsilon^{-rp_jm} \tau^r\left(S_{p_j,0}\right) \\ &= \sum_{r\in I_j} \varepsilon^{-rp_jm} \tau^r \left(\sum_{k=0}^{n_j-1} B_{kp_j}\right) = \sum_{r\in I_j} \varepsilon^{-rp_jm} \left(\sum_{k=0}^{n_j-1} \tau^r(B_{kp_j})\right) \\ &= \sum_{r\in I_j} \varepsilon^{-rp_jm} \left(\sum_{k=0}^{n_j-1} \varepsilon^{kp_jr} B_{kp_j}\right) = \sum_{k=0}^{n_j-1} B_{kp_j} \left(\sum_{r\in I_j} \varepsilon^{rp_j(k-m)}\right). \end{aligned}$$

Observe that, by Proposition 4.7, every sum $\sum_{r\in I_j} \varepsilon^{rp_j(k-m)}$ is an integer. Moreover, every polynomial B_{kp_j} belongs to $\mathbb{Z}[X]$. Hence, $T_{p_j,m} \in \mathbb{Z}[X]$.

Recall that $T_{p_j,a} = T_{p_j,m}$, where m is the remainder of division of a by n_j. Thus, we proved the following proposition.

Proposition 8.2. *For any $j \in \{1, \ldots, s\}$ and $a \in \mathbb{Z}$, the polynomial $T_{p_j,m}$ belongs to the polynomial ring $\mathbb{Z}[X]$.*

Now we will prove some additional properties of the polynomials $T_{p_j,a}$.

Proposition 8.3. *Assume that $s \geqslant 2$, and let $i, j \in \{1, \ldots, s\}$, $i < j$. Then*

$$\sum_{k=0}^{p_i-1} T_{p_j,\, k\frac{n}{p_ip_j}} = 0.$$

Proof. Put $p = p_i$, $q = p_j$, and $N = \frac{n}{pq}$. Then we have

$$\sum_{k=0}^{p_i-1} T_{p_j,\, k\frac{n}{p_ip_j}} = \sum_{k=0}^{p-1} T_{q,\, kN} = \sum_{k=0}^{p-1}\sum_{r\in I_j} \left(\varepsilon^{-kNq}\right)^r S_{q,r} = \sum_{r\in I_j}\left(\sum_{k=0}^{p-1}\left(\varepsilon^{-\frac{n}{p}r}\right)^k\right) S_{q,r}.$$

Let $\eta = \varepsilon^{-\frac{n}{p}}$. Then η is a primitive p-th root of unity. If $r \in I_j$, then $p \nmid r$ and, by Lemma 4.6, we have

$$\sum_{k=0}^{p-1}\left(\varepsilon^{-\frac{n}{p}r}\right)^k = \sum_{k=0}^{p-1} \eta^{rk} = 0.$$

Thus, $\sum_{k=0}^{p_i-1} T_{p_j,\, k\frac{n}{p_ip_j}} = \sum_{r\in I_j}\left(\sum_{k=0}^{p-1}\left(\varepsilon^{-\frac{n}{p}r}\right)^k\right) S_{q,r}. = \sum_{r\in I_j} 0\cdot S_{q,r} = 0.$ □

Proposition 8.4. *For any integer a, we have*

$$\varrho\left(T_{p_j,\,a}\right) = \begin{cases} T_{p_j,\,a+1}, & \text{when } p_j \neq 2, \\ -T_{p_j,\,a+1}, & \text{when } p_j = 2. \end{cases}$$

Proof. First assume that p_j is odd. In this case (see Proposition 7.1), $\varrho\left(S_{p_j\, r}\right) = \varepsilon^{-p_j r} S_{p_j\, r}$ for any $r \in \mathbb{Z}$. Hence,

$$\begin{aligned} \varrho\left(T_{p_j,\, a}\right) &= \sum_{r\in I_j} \left(\varepsilon^{-ap_j}\right)^r \varrho\left(S_{p_j\, r}\right) = \sum_{r\in I_j} \left(\varepsilon^{-ap_j}\right)^r \varepsilon^{-p_j r} S_{p_j\, r} \\ &= \sum_{r\in I_j} \left(\varepsilon^{-(a+1)p_j}\right)^r S_{p_j\, r} = T_{p_j,\, a+1}. \end{aligned}$$

Now let $p_j = 2$. Then, by Proposition 7.1, $\varrho\left(S_{p_j\, r}\right) = \varepsilon^{-\left(p_j r + \frac{n}{2}\right)} S_{p_j,\, r}$ for any $r \in \mathbb{Z}$. Moreover, $\varepsilon^{-\frac{n}{2}} = -1$. Thus, we have

$$\begin{aligned} \varrho\left(T_{p_j,\, a}\right) &= \sum_{r\in I_j} \left(\varepsilon^{-ap_j}\right)^r \varrho\left(S_{p_j\, r}\right) = \sum_{r\in I_j} \left(\varepsilon^{-ap_j}\right)^r \varepsilon^{-\left(p_j r + \frac{n}{2}\right)} S_{p_j,\, r} \\ &= \sum_{r\in I_j} \varepsilon^{-\frac{n}{2}} \left(\varepsilon^{-(a+1)p_j}\right)^r S_{p_j\, r} = -\sum_{r\in I_j} \left(\varepsilon^{-(a+1)p_j}\right)^r S_{p_j\, r} = -T_{p_j,\, a+1}. \end{aligned}$$

This completes the proof. $\square$

Proposition 8.5. *Assume that $s \geqslant 2$. Let $i, j \in \{1, \dots, s\}$, $i < j$, and let $a \in \mathbb{Z}$. Then*

$$T_{p_j,\, a} = -\sum_{k=1}^{p_i - 1} T_{p_j,\, a + k\frac{n}{p_i p_j}}.$$

Proof. It follows from Proposition 8.4 that $T_{p_j,\, a} = (-1)^{p_j - 1} \varrho^a\left(T_{p_j,\, 0}\right)$. Hence, using Proposition 8.3, we obtain

$$\begin{aligned} T_{p_j,\, a} &= (-1)^{p_j - 1} \varrho^a\left(T_{p_j,\, 0}\right) = (-1)^{p_j - 1} \varrho^a \left(-\sum_{k=1}^{p_i - 1} T_{p_j,\, k\frac{n}{p_i p_j}}\right) \\ &= (-1)^{p_j} \sum_{k=1}^{p_i - 1} \varrho^a \left(T_{p_j,\, k\frac{n}{p_i p_j}}\right) = (-1)^{p_j} \sum_{k=1}^{p_i - 1} (-1)^{p_j - 1} T_{p_j,\, a + k\frac{n}{p_i p_j}} \\ &= -\sum_{k=1}^{p_i - 1} T_{p_j,\, a + k\frac{n}{p_i p_j}}. \end{aligned}$$

This completes the proof. $\square$

For any $j \in \{1, \dots, s\}$, let us denote by $\mathcal{W}_j$ the $\mathbb{Z}$-module generated by all the polynomials $T_{p_j,\, r}$ with $r \in I_j$. It is clear that every polynomial $T_{p_1,\, a}$, for arbitrary integer a, belongs to $\mathcal{W}_1$.

Theorem 8.6. *If the number n is special, then for all $j \in \{1, \dots, s\}$ and $a \in \mathbb{Z}$, the polynomial $T_{p_j,\, a}$ belongs to $\mathcal{W}_j$.*

Proof. Let $n = p_1 \cdots p_{s-1} \cdot p_s^{\alpha}$, where $s \geqslant 1$, $\alpha \geqslant 1$, and $p_1, \dots, p_s$ are distinct primes. Let $n_j = \frac{n}{p_j}$ for $j = 1, \dots, s$. Assume that $P = [p_1, \dots, p_n]$ is a fixed type, and $I_1, \dots, I_s$ are the n-sets of type P.

Let j be a fixed element from $\{1, \dots, s\}$. If $s = 1$ or $j = 1$, then we are done. Assume that $s \geqslant 2$, $j \geqslant 2$, and a is an integer. Since $T_{p_j,\, a} = T_{p_j, m}$, where m is the remainder of division of a by n_j, we may assume that $0 \leqslant a < n_j$. We use the following notations:

$$M := \{p_1, p_2, \ldots, p_{j-1}\}, \quad q := p_j, \quad B_c := T_{p_j, c} \quad \text{for} \quad c \in \mathbb{Z}.$$

We will show that $B_a \in \mathcal{W}_j$. If $\gcd(a, p_1 \cdots p_{j-1}) = 1$, then $a \in I_j$ and so, $B_a \in \mathcal{W}_j$. Now let $\gcd(a, p_1 \cdots p_{j-1}) \geqslant 2$. In this case, a is divisible by some primes belonging to M.

Step 1. Assume that a is divisible by exactly one prime number p_i belonging to M. Then $i < j$ and, by Proposition 8.5, we have the equality

$$B_a = -\sum_{k=1}^{p_i - 1} B_{a + k\frac{n}{p_i q}}.$$

Let $k \in \{1, \ldots, p_i - 1\}$, and consider $c := a + k\frac{n}{p_i q}$. Since n is special, the number $k\frac{n}{p_i q}$ is not divisible by p_i. But $p_i \mid a$, so $p_i \nmid c$. If $p \in M$ and $p \neq p_i$, then $p \nmid a$ and $p \mid k\frac{n}{p_i q}$, so $p \nmid c$. Hence, the numbers c and $p_1 \cdots p_{j-1}$ are relatively prime. This implies that the element $c \pmod{n_j}$ belongs to I_j, and so, $B_c \in \mathcal{W}_j$. Therefore, by the above equality, $B_a \in \mathcal{W}_j$.

We see that if $s = 2$ or $j = 2$, then we are done. Now suppose that $s \geqslant 3$ and $j \geqslant 3$.

Step 2. Let $1 \leqslant t \leqslant j - 2$, and assume that we already proved that $B_c \in \mathcal{W}_j$ for every integer c which is divisible by exactly t primes belonging to M. Assume that a is divisible by exactly $t+1$ distinct primes $m_1, \ldots, m_{t+1}$ from M. We have: $m_i \mid a$ for $i = 1, \ldots, t+1$, and $m \nmid a$ for $m \in M \smallsetminus \{m_1, \ldots, m_{t+1}\}$. Put $p = m_{t+1}$. It follows from Proposition 8.5, that have the following equality:

$$B_a = -\sum_{k=1}^{p-1} B_{a + k\frac{n}{pq}}.$$

Let $k \in \{1, \ldots, p - 1\}$, and consider $c := a + k\frac{n}{pq}$. Since n is special, the number $k\frac{n}{pq}$ is not divisible by p. But $p \mid a$, so $p \nmid c$, and consequently, $m_{t+1} \nmid c$. It is clear that $m_i \mid c$ for all $i = 1, \ldots, t$, and $m \nmid c$ for all $m \in M \smallsetminus \{m_1, \ldots, m_t\}$. This means that c is divisible by exactly t primes from M. Thus, by our assumption, $B_c \in \mathcal{W}_j$. Therefore, by the above equality, $B_a \in \mathcal{W}_j$.

Now we use a simple induction and, by Steps 1 and 2, we obtain the proof of our theorem. $\square$

9. The main theorem

Assume that $n \geqslant 3$ is a special number of a type P. Let $I_1, \ldots, I_s$ be the n-sets of type P, let $\mathcal{A}$ be the n-standard set of type P, and let

$$\mathcal{S} = \Big\{ S_{p_j, r};\ j \in \{1, \ldots, s\},\ r \in I_j \Big\}, \quad \mathcal{T} = \Big\{ T_{p_j, r};\ j \in \{1, \ldots, s\},\ r \in I_j \Big\}.$$

Since n is special, we have the following sequence of important properties.

(1) *$\mathcal{A}$ is a basis of the group $\mathcal{G}_n$* (Theorems 5.8, 3.5 and 5.10).

(2) *$\mathcal{S}$ is algebraically independent over K, and $K(X)^d = K(\mathcal{S})$* (Proposition 7.5).

(3) $K(\mathcal{S}) = K(\mathcal{T})$ (Proposition 8.1 and Theorem 8.6).

We know also (see Proposition 8.2) that each element of $\mathcal{T}$ is a polynomial belonging to $\mathbb{Z}[X]$. Moreover, $|\mathcal{T}| = |\mathcal{S}| = |\mathcal{A}| = n - \varphi(n)$. In particular, the set $\mathcal{T}$ is algebraically independent over K. Put an order on the set $\mathcal{T}$. Let $\mathcal{T} = \{F_0, F_1, \ldots, F_{m-1}\}$ where $m = n - \varphi(n)$. Thus, if the number n is special, then $K(X)^d = K(F_0, \ldots, F_{m-1})$, where $F_0, \ldots, F_{m-1}$ are polynomials belonging to $\mathbb{Z}[X]$, and these polynomials are algebraically independent over $\mathbb{Q}$.

Let us recall, that K is a field of characteristic zero containing ε (where ε is a primitive n-th root of unity). But the polynomials $F_0, \ldots, F_{m-1}$ have integer coefficients, and they are constants of d. They are not dependent from the field K. Since the polynomials $d(x_0), \ldots, d(x_{n-1})$ belong to $\mathbb{Z}[X]$, we see that we may assume that K is a field of characteristic zero, without the assumption concerning ε. Thus, we proved the following theorem.

Theorem 9.1. *Let K be an arbitrary field of characteristic zero, $n \geqslant 3$ an integer, and $K[X] = K[x_0, \ldots, x_{n-1}]$ the polynomial ring in n variables over K. Let $d : K[X] \to K[X]$ be the cyclotomic derivation, that is, d is a K-derivation of $K[X]$ such that*

$$d(x_i) = x_{i+1} \quad \text{for} \quad i \in \mathbb{Z}_n.$$

Assume that $n = p_1 p_2 \cdots p_{s-1} p_s^{\alpha}$, where $s \geqslant 1$, $\alpha \geqslant 1$ and $p_1, \ldots, p_s$ are distinct primes. Let $m = n - \varphi(n)$, where φ is the Euler totient function. Then

$$K(X)^d = K(F_0, \ldots, F_{m-1}),$$

where $F_0, \ldots, F_{m-1}$ are algebraically independent over $\mathbb{Q}$ polynomials belonging to $\mathbb{Z}[X]$.

More exactly, $\{F_0, F_1, \ldots, F_{m-1}\} = \left\{T_{p_j, r};\ j \in \{1, \ldots, s\},\ r \in I_j\right\}$, where $I_1, \ldots, I_s$ are the n-sets of type $[p_1, \ldots, p_s]$.

We end this article with several examples illustrating the above theorem.

Example 9.2. *If $n = 4$, then $K(X)^d = K(F_0, F_1)$, where $F_0 = x_0^2 - 2x_1x_3 + x_2^2$, and $F_1 = \varrho(F_0)$.*

Example 9.3. *If $n = 8$, then $K(X)^d = K(F_0, F_1, F_2, F_3)$, where $F_1 = \varrho(F_0)$, $F_2 = \varrho^2(F_0)$, $F_3 = \varrho^3(F_0)$ and $F_0 = x_0^2 + x_4^2 - 2x_3x_5 - 2x_7x_1 + 2x_2x_6$.*

Example 9.4. *If* $n = 9$, *then* $K(X)^d = K(F_0, F_1, F_2)$, *where* $F_1 = \varrho(F_0)$, $F_2 = \varrho^2(F_0)$,

$$\begin{aligned} F_0 &= 3x_1x_4^2 + 3x_8^2x_2 + 3x_8x_5^2 - 3x_0x_4x_5 - 3x_1x_0x_8 - 3x_2x_4x_3 - 3x_2x_7x_0 \\ &\quad -3x_8x_6x_4 + 3x_2^2x_5 + 3x_7^2x_4 + 3x_1^2x_7 + x_6^3 + x_0^3 - 3x_1x_3x_5 + 6x_0x_6x_3 \\ &\quad -3x_8x_7x_3 - 3x_2x_1x_6 - 3x_5x_7x_6 + x_3^3. \end{aligned}$$

Example 9.5. *If* $n = 6$ *and* $P = [2, 3]$, *then* $K(X)^d = K(F_0, F_1, F_2, F_3)$, *where*

$$\begin{aligned} F_0 &= x_0^2 - 2x_1x_5 + 2x_2x_4 - x_3^2, \\ F_3 &= (x_1^2 + x_4x_3 - 2x_1x_4 + x_0x_1 + x_5^2 - x_5x_3 + x_2x_3 - 2x_2x_5 + x_0x_5 \\ &\quad -2x_0x_3 - x_0x_2 - x_4x_0 + x_4^2 - x_1x_3 + x_2^2 + x_4x_5 + x_1x_2 + x_0^2 \\ &\quad -x_1x_5 - x_4x_2 + x_3^2)(x_0 - x_1 + x_2 - x_3 + x_4 - x_5), \end{aligned}$$

and $F_1 = \varrho(F_0)$, $F_2 = \varrho^2(F_0)$.

Example 9.6. *If* $n = 6$ *and* $P = [3, 2]$, *then* $K(X)^d = K(F_0, F_1, F_2, F_3)$, *where*

$$\begin{aligned} F_0 &= x_0^3 + x_2^3 + x_4^3 + 3x_0x_3^2 + 3x_2x_5^2 + 3x_4x_1^2 - 3x_0x_2x_4 - 3x_5x_0x_1 \\ &\quad -3x_1x_2x_3 - 3x_3x_4x_5, \\ F_2 &= 2x_1^2 + x_2^2 - x_3^2 - 2x_4^2 - x_5^2 + x_0^2 \\ &\quad -2x_1x_3 + 2x_2x_4 + 4x_3x_5 + 2x_4x_0, -2x_5x_1 - 4x_2x_0. \end{aligned}$$

and $F_1 = \varrho(F_0)$, $F_3 = \varrho(F_2)$.

Example 9.7. *If* $n = 12$, *then* $K(X)^d = K(F_0, \dots, F_7)$, *where*

$$\begin{aligned} F_0 &= -3x_6x_2x_4 - 3x_6x_8x_{10} - 3x_4x_0x_8 + x_0^3 + 3x_6^2x_0 - 3x_1x_8x_3 + 3x_3^2x_6 \\ &\quad +3x_9^2x_6 + x_8^3 - 3x_1x_{11}x_0 + 6x_5x_{11}x_8 - 3x_1x_5x_6 + 3x_7^2x_{10} + 3x_{10}^2x_4 \\ &\quad +3x_{11}^2x_2 + 3x_1^2x_{10} + 3x_5^2x_2 + 3x_2^2x_8 + 6x_3x_0x_9 + 6x_1x_7x_4 - 3x_7x_{11}x_6 \\ &\quad -3x_7x_5x_0 - 3x_{10}x_{11}x_3 - 3x_{10}x_5x_9 - 3x_4x_{11}x_9 - 3x_4x_5x_3 - 3x_1x_2x_9 \\ &\quad -3x_7x_2x_3 - 3x_7x_8x_9 + x_4^3 - 3x_{10}x_2x_0, \\ F_4 &= 4x_6x_8 + x_3^2 - 2x_{10}x_8 + 2x_7x_3 + 2x_7x_{11} - 2x_{10}x_0 - 2x_4x_2 - 2x_4x_6 \\ &\quad +2x_1x_9 + 2x_1x_5 + 4x_0x_2 - 2x_0x_6 - 4x_3x_{11} - 2x_1^2 + x_{11}^2 + x_5^2 + 4x_4x_{10} \\ &\quad -2x_2x_8 - 2x_7^2 + x_9^2 - 4x_9x_5, \end{aligned}$$

and $F_1 = \varrho(F_0)$, $F_2 = \varrho^2(F_0)$, $F_3 = \varrho^3(F_0)$, $F_5 = \varrho(F_4)$, $F_6 = \varrho^3(F_4)$, $F_7 = \varrho^4(F_4)$.

References

[1] N.G. de Bruijn, *On the factorization of cyclic groups*, Indag. Math. 15 (1953), 370–377.

[2] A. van den Essen, *Polynomial Automorphisms and the Jacobian Conjecture*, Progress in Mathematics vol. 190, 2000.

[3] G. Freudenburg, *Algebraic Theory of Locally Nilpotent Derivations*, Encyclopedia of Mathematical Sciences 136, Springer, 2006.

[4] T.Y. Lam and K.H. Leung, *On the cyclotomic polynomial* $\Phi_{pq}(x)$, American Mathematical Monthly, 103(7) (1996), 562–564.

[5] T.Y. Lam and K.H. Leung, *On vanishing sums of roots of unity*, J. Algebra, 224 (2000), 91–109,

[6] S. Lang, *Algebra*, Second Edition, Addison-Wesley Publishing Company, 1984.

[7] S. Lang, *Undergraduate Algebra*, Second Edition, Springer, 1990.

[8] J. Moulin Ollagnier and A. Nowicki, *Derivations of polynomial algebras without Darboux polynomials*, J. Pure Appl. Algebra, 212 (2008), 1626–1631.
[9] J. Moulin Ollagnier and A. Nowicki, *Monomial derivations*, Communications in Algebra, 39 (2011), 3138–3150.
[10] J. Moulin Ollagnier and A. Nowicki, *Constants of cyclotomic derivations*, J. Algebra 394 (2013), 92–119.
[11] A. Nowicki, *Polynomial derivations and their rings of constants*, N. Copernicus University Press, Toruń, 1994.
[12] A. Nowicki and M. Nagata, *Rings of constants for k–derivations in $k[x_1, \dots, x_n]$*, J. Math. Kyoto Univ., 28 (1988), 111–118.
[13] L. Rédei, *Ein Beitrag zum Problem der Faktorisation von endlichen Abelschen Gruppen*, Acta Math. Hungar, 1 (1950), 197–207.
[14] A. Satyanarayan Reddy, *The lowest $0, 1$-polynomial divisible by cyclotomic polynomial*, arXiv: 1106.127v2 [math.NT] 15Nov 2011.
[15] I.J. Schoenberg, *A note on the cyclotomic polynomial*, Mathematika, 11 (1964), 131–136.
[16] J.P. Steinberger, *The lowest-degree polynomial with nonnegative coefficients divisible by the n-th cyclotomic polynomial*, The electronic journal of combinatorics 19(4) (2012), #P1
[17] J.P. Steinberger, *Minimal vanishing sums of roots of unity with large coefficients*, Proc. Lond. Math. Soc. (3) 97 (2008), 689–717.

(Jean Moulin Ollagnier) Laboratoire LIX, École Polytechnique, F 91128 Palaiseau Cedex, France

E-mail address: `Jean.Moulin-Ollagnier@polytechnique.edu`

(Andrzej Nowicki) Nicolaus Copernicus University, Faculty of Mathematics and Computer Science, ul. Chopina 12/18, 87-100 Toruń, Poland

E-mail address: `anow@mat.uni.torun.pl`