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 $n \geq 3$ 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

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

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 $\varphi$ 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

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

for some, algebraically independent, polynomials $F_0, \ldots, F_{m-1}$ belonging to the polynomial ring $\mathbb{Z}[X] = \mathbb{Z}[x_0, \ldots, x_{n-1}]$, 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 $n \geq 3$ is an integer, $\varepsilon$ 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, $K[X] = K[x_0, \ldots, x_{n-1}]$ is the polynomial ring over $K$ in variables $x_0, \ldots, x_{n-1}$, and $K(X) = K(x_0, \ldots, x_{n-1})$ is the field of quotients of $K[X]$. The indexes of the variables $x_0, \ldots, x_{n-1}$ are elements of the ring $\mathbb{Z}_n$. The cyclotomic derivation $d$ is the $K$-derivation of $K(X)$ defined by $d(x_i) = x_{i+1}$ for $i \in \mathbb{Z}_n$.

For every sequence $\alpha = (\alpha_0, \alpha_1, \ldots, \alpha_{n-1})$, 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 $G_n$ and $M_n$. The first subset is the set of all sequences $\alpha = (\alpha_0, \ldots, \alpha_{n-1})$ such that $\alpha_0, \ldots, \alpha_{n-1}$ are integers and

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

The second subset $M_n$ is the set of all such sequences $\alpha = (\alpha_0, \ldots, \alpha_{n-1})$ which belong to $G_n$ and the integers $\alpha_0, \ldots, \alpha_{n-1}$ are nonnegative, that is, they belong to the set of natural numbers $\mathbb{N} = \{0, 1, 2, \ldots\}$. To be precise,

$$G_n = \{ \alpha \in \mathbb{Z}^n; H_\alpha(\varepsilon) = 0 \}, \quad M_n = \{ \alpha \in \mathbb{N}^n; H_\alpha(\varepsilon) = 0 \} = G_n \cap \mathbb{N}^n.$$  

If $\alpha, \beta \in G_n$, then of course $\alpha \pm \beta \in G_n$, and if $\alpha, \beta \in M_n$, then $\alpha + \beta \in M_n$. Thus $G_n$ is an abelian group, and $M_n$ is an abelian monoid with zero $0 = (0, \ldots, 0)$.

Let us recall that $\varepsilon$ 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 $\varphi$ is the Euler totient function. This implies the following proposition.

**Proposition 2.1.** Let $\alpha \in \mathbb{Z}^n$. Then $\alpha \in G_n$ 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 \( e_0 = (1, 0, 0, \ldots, 0), e_1 = (0, 1, 0, \ldots, 0), \ldots, e_{n-1} = (0, 0, \ldots, 0, 1), \) and let 
\[ e = \sum_{i=0}^{n-1} e_i = (1, 1, \ldots, 1). \] Since \( \sum_{i=0}^{n-1} e_i = 0, \) the element \( e \) belongs to \( \mathcal{M}_n. \)

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

Let \( \alpha \in \mathcal{M}_n. \) We say that \( \alpha \) 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, \( \alpha \) is a minimal element of 
\( \mathcal{M}_n, \) if \( \alpha \neq 0 \) and \( \alpha \) is not a sum of two nonzero elements of \( \mathcal{M}_n. \)

We denote by \( \zeta, \) the rotation of \( \mathbb{Z}^n \) given by \( \zeta(\alpha) = (a_{n-1}, a_0, a_1, \ldots, a_{n-2}), \)
for \( a = (a_0, a_1, \ldots, a_{n-1}) \in \mathbb{Z}^n. \) The mapping \( \zeta \) is a \( \mathbb{Z} \)-module automorphism of 
\( \mathbb{Z}^n. \) Note that \( \zeta^{-1}(\alpha) = (a_1, \ldots, a_{n-1}, a_0), \) for all \( \alpha = (a_0, a_1, \ldots, a_{n-1}) \in \mathbb{Z}^n. \) If 
\( a, b \in \mathbb{Z} \) and \( a \equiv b \pmod{\mathbb{N}}, \) 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 \( \alpha^{(1)} \geq \alpha^{(2)} \geq \alpha^{(3)} \geq \ldots \) is a sequence 
of elements from \( \mathcal{M}_n, \) then there exists an integer \( s \) such that \( \alpha^{(j)} = \alpha^{(j+1)} \) for all 
\( j \geq s. \)
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 \( \beta \) such that \( \beta \leq \alpha. \) 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, \( \alpha \) 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 \( \Phi_n(t) = c_0 + c_1 t + \cdots + c_{\varphi(n)} t^{\varphi(n)}. \) All the coefficients \( c_0, \ldots, c_{\varphi(n)} \) are integers, and \( c_0 = c_{\varphi(n)} = 1. \) Put 
\( m = n - \varphi(n) \) and

\[ \gamma_0 = \left( c_0, c_1, \ldots, c_{\varphi(n)}, 0, \ldots, 0 \right)_{m-1}. \]

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 \( \gamma_j = \zeta^j(\gamma_0), \) for \( j = 0, 1, \ldots, m-1. \) Observe that \( H_{\gamma_j}(t) = \Phi_n(t) \cdot t^j \) for all \( j \in \{0, \ldots, m-1\}. \) Since \( \Phi_n(e) = 0, \) we have \( H_{\gamma_j}(e) = 0, \) and so, the elements 
\( \gamma_0, \ldots, \gamma_{m-1} \) 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 \( \gamma_0, \ldots, \gamma_{m-1}, \) 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 $r = 0, 1, \ldots, \frac{n}{p} - 1$. Observe that each $m(p, r)$ is equal to $\zeta^r (m(p, 0))$. 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 $r_1, r_2 \in \{0, 1, \ldots, \frac{n}{p} - 1\}$ and $r_1 \neq r_2$, then $m(p, r_1) \neq m(p, r_2)$.

If $\alpha = (\alpha_0, \ldots, \alpha_{n-1}) \in \mathbb{Z}^n$, 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 $r_1 \in \{0, \ldots, \frac{n}{p} - 1\}, r_2 \in \{0, 1, \ldots, \frac{n}{q} - 1\}$. Note the following two obvious propositions.

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

**Proposition 3.2.** If $p$ is a prime divisor of $n$, then the standard elements $m(p, 0), m(p, 1), \ldots, m(p, \frac{n}{p} - 1)$ 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 $\{0, 1, \ldots, m - 1\}$. First observe that $\left\{ k + ip; k \in [p], i \in [q] \right\} = \left\{ k + iq; k \in [q], i \in [p] \right\} = [pq]$. Hence,

$$\sum_{k=0}^{p-1} m(q, kN) = \sum_{k=0}^{p-1} \sum_{i=0}^{q-1} e^{kN + i \frac{p}{q}} = \sum_{k=0}^{p-1} \sum_{i=0}^{q-1} e^{N(k+ip)} = \sum_{k=0}^{pq-1} e_{Nk};$$

$$\sum_{k=0}^{q-1} m(p, kN) = \sum_{k=0}^{q-1} \sum_{i=0}^{p-1} e^{kN + i \frac{q}{p}} = \sum_{k=0}^{q-1} \sum_{i=0}^{p-1} e^{N(k+iq)} = \sum_{k=0}^{pq-1} e_{Nk}.$$  

Thus,

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

$\square$
Proposition 3.4. Let \( p \) be a prime divisor of \( n \). Let \( 0 \leq r < \frac{n}{p} \), and \( a \in \mathbb{Z} \). Then
\[
\zeta^a(m(p, r)) = m(p, b), \quad \text{where} \quad b = (a + r) \left( \text{mod} \frac{n}{p} \right).
\]

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

Hence,
\[
\zeta^a(m(p, r)) = \zeta^a\left( \sum_{i=0}^{p-1} e_{r+iw} \right) = \sum_{i=0}^{p-1} e_{a+r+iw} = \sum_{i=0}^{p-1} e_{b+cw+iw} = \sum_{i=0}^{p-1} e_{b+(c+i)w} = m(p, b),
\]
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 \( n \geq 3 \) be an integer, and 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 \( j = 1, \ldots, s \). Let \( I_1, \ldots, I_s \) be sets of integers defined as follows:

\[
I_1 = \left\{ r \in \mathbb{Z}; \ 0 \leq r < n_1 \right\},
\]

\[
I_2 = \left\{ r \in \mathbb{Z}; \ 0 \leq r < n_2, \ \gcd(r, p_1) = 1 \right\},
\]

\[
I_3 = \left\{ r \in \mathbb{Z}; \ 0 \leq r < n_3, \ \gcd(r, p_1p_2) = 1 \right\},
\]

\[
\vdots
\]

\[
I_s = \left\{ r \in \mathbb{Z}; \ 0 \leq r < n_s, \ \gcd(r, p_1p_2\cdots p_{s-1}) = 1 \right\}.
\]

That is, \( I_1 = \{r \in \mathbb{Z}; \ 0 \leq r < n_1\} \) and \( I_j = \{r \in \mathbb{Z}; \ 0 \leq r < n_j, \ \gcd(r, p_1\cdots p_{j-1}) = 1\} \) for \( j = 2, \ldots, s \). This definition depends of the fixed succession of primes. We will say that the above \( I_1, \ldots, I_s \) are the \emph{n-sets of type} \([p_1, \ldots, p_s]\).
Let for example \( n = 12 = 2^23 \). 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:

<table>
<thead>
<tr>
<th>type</th>
<th>( I_1 )</th>
<th>( I_2 )</th>
<th>( I_3 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>([2, 3, 5])</td>
<td>{0, 1, 2, ..., 14}</td>
<td>{1, 3, 5, 7, 9}</td>
<td>{1, 5}</td>
</tr>
<tr>
<td>([2, 5, 3])</td>
<td>{0, 1, 2, ..., 14}</td>
<td>{1, 3, 5}</td>
<td>{1, 3, 7, 9}</td>
</tr>
<tr>
<td>([3, 2, 5])</td>
<td>{0, 1, 2, ..., 9}</td>
<td>{1, 2, 4, 5, 7, 8, 10, 11, 13, 14}</td>
<td>{1, 5}</td>
</tr>
<tr>
<td>([3, 5, 2])</td>
<td>{0, 1, 2, ..., 9}</td>
<td>{1, 2, 4, 5}</td>
<td>{1, 2, 4, 7, 8, 11, 13, 14}</td>
</tr>
<tr>
<td>([5, 2, 3])</td>
<td>{0, 1, 2, 3, 4, 5}</td>
<td>{1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 13, 14}</td>
<td>{1, 3, 7, 9}</td>
</tr>
<tr>
<td>([5, 3, 2])</td>
<td>{0, 1, 2, 3, 4, 5}</td>
<td>{1, 2, 3, 4, 6, 7, 8, 9}</td>
<td>{1, 2, 4, 7, 8, 11, 13, 14}</td>
</tr>
</tbody>
</table>

Now we calculate the cardinality of the sets \( I_1, \ldots, I_s \). 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 \( \{1, 2, \ldots, ab\} \) there are exactly \( \varphi(ab) \) numbers relatively prime to \( a \). In fact, let \( u \in \{1, 2, \ldots, ab\} \). Then \( u = ka + r \), where \( 0 \leq k \leq b \) and \( 0 \leq r < a \), 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 \( 1 \leq r < a \), \( \gcd(r, a) = 1 \) and where \( k \) is an arbitrary number belonging to \( \{0, 1, \ldots, b - 1\} \). Hence, we have exactly \( b \) such numbers \( k \), and so, the number of integers in \( \{1, \ldots, ab\} \), relatively prime to \( a \), is equal to \( \varphi(ab) \). As a consequence of this fact we obtain

**Lemma 4.2.** Let \( a \geq 2 \), \( b \geq 2 \) be relatively prime integers. Then there are exactly \( \varphi(ab) \) such integers belonging to \( \{0, 1, \ldots, ab - 1\} \) 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 \( j = 2, 3, \ldots, s \).

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

\[
|I_j| = \varphi(a)b = p_1^{\alpha_1} \cdots p_{j-1}^{\alpha_{j-1}} \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_{j-1}}\right) \left(1 - \frac{1}{p_j}\right) = n_j \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_{j-1}}\right) \left(1 - \frac{1}{p_j}\right).
\]

This completes the proof. \( \Box \)

**Lemma 4.4.** Consider some nonzero numbers \( z_1, \ldots, z_s \). 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 \( j = 2, \ldots, s \). Then

\[
w_1 + w_2 + \cdots + w_s = 1 - \left(1 - \frac{1}{z_1}\right) \left(1 - \frac{1}{z_2}\right) \cdots \left(1 - \frac{1}{z_s}\right) = \frac{1}{z_1} \cdot \frac{1}{z_2} \cdots \frac{1}{z_s}.
\]
Proposition 4.5. 

Proof. The case $s = 1$ is obvious. Assume now that it is true for an integer $s \geq 1$, and consider nonzero numbers $z_1, \ldots, z_{s+1}$. Then we have
\[
1 - \left(1 - \frac{1}{z_1}\right) \cdots \left(1 - \frac{1}{z_{s+1}}\right) = \left(1 - \left(1 - \frac{1}{z_1}\right) \cdots \left(1 - \frac{1}{z_s}\right)\right) + \frac{1}{z_{s+1}} \left(1 - \frac{1}{z_1}\right) \cdots \left(1 - \frac{1}{z_s}\right).
\]
This completes the proof. □

Proposition 4.6. $|I_1| + |I_2| + \cdots + |I_s| = n - \varphi(n)$.

Proof. We know, by Proposition 4.3, that $|I_j| = nw_j$, for $j = 1, \ldots, s$, where $w_1 = \frac{1}{p_1}$ and $w_j = \frac{1}{p_1} \left(1 - \frac{1}{p_2}\right) \left(1 - \frac{1}{p_3}\right) \cdots \left(1 - \frac{1}{p_s}\right)$ for $j = 2, \ldots, s$. Thus, by Lemma 4.4,
\[
|I_1| + |I_2| + \cdots + |I_s| = n \left(1 - \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_s}\right)\right) = n - n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_s}\right) = n - \varphi(n).
\]
This completes the proof. □

Let us recall the following well-known lemma where $\varepsilon$ 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 $n \mid c$ then $U$ is equal to 0, and in the other case, when $n \nmid c$, 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 $j \in \{1, \ldots, s\}$, 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 $\eta$ is a primitive $n_1$-th root of unity, and $W_1 = \sum_{r=0}^{n_1-1} (\eta^r)^r$. It follows from Lemma 4.6 that $W_1$ is an integer.

Now assume that $j \geq 2$. Put $X = \{0, 1, \ldots, n_j - 1\}$, and $D_i = \{r \in X; \ p_i \mid r\}$ for $i = 1, \ldots, j - 1$. Then $I_j = X \setminus (D_1 \cup \cdots \cup D_{j-1})$, and then $W_j = U - V$, where
\[
U = \sum_{r \in X} (\varepsilon^{p_j c})^r, \quad V = \sum_{r \in D_1 \cup \cdots \cup D_{j-1}} (\varepsilon^{p_j c})^r.
\]
Observe that $U = \sum_{r=0}^{n_j-1} (\eta^r)^r$, 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
\[ V = \sum_{k=1}^{j-1} (-1)^{k+1} \sum_{i_1 < \cdots < i_k} \sum_{r \in D_{i_1 \cdots i_k}} (\varepsilon^{p,c})^r, \]
where the sum \( \sum_{i_1 < \cdots < i_k} \) runs through all integer sequences \( (i_1, \ldots, i_k) \) such that \( 1 \leq i_1 < \cdots < i_k \leq j - 1 \), and where \( D_{i_1 \cdots i_k} = D_{i_1} \cap \cdots \cap D_{i_k} \).

Let \( 1 \leq i_1 < \cdots < i_k \leq j - 1 \) be a fixed integer sequence. Then we have
\[ \sum_{r \in D_{i_1 \cdots i_k}} (\varepsilon^{p,c})^r = \sum_{r=0}^{u-1} (\eta^r)^r, \]
where \( \eta = \varepsilon^{p_1^{n_1} \cdots p_k^{n_k}} \), and \( u = \sum_{j=i}^{n} n_j = \frac{n}{p_j^{n_j} - 1} \). Since \( \eta \) 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 \( \sum_{r \in D_{i_1 \cdots i_k}} (\varepsilon^{p,c})^r \) 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.

\[ \square \]

5. Special numbers

As in the previous section, let \( n = p_1^{n_1} \cdots p_s^{n_s} \), where \( p_1, \ldots, p_s \) are distinct primes and \( n_1, \ldots, n_s \) are positive integers. Put \( n_j = \frac{n}{p_j^{n_j}} \) for \( j = 1, \ldots, s \). Assume that \( [p_1, \ldots, p_s] \) 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 \( 0 \leq r < n_j \), 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 \( A_1, \ldots, A_s \), which are subsets of the monoid \( \mathcal{M}_n \). We define these subsets as follows
\[ A_j = \left\{ m(p_j, r); \ r \in I_j \right\}, \]
for all \( j = 1, \ldots, s \). We denote by \( A \) the union \( A = A_1 \cup \cdots \cup A_s \). Note that the above sets \( A \) and \( A_1, \ldots, A_s \) are determined by the fixed succession \( P = [p_1, \ldots, p_s] \) of the primes \( p_1, \ldots, p_s \). In our case we will say that \( A \) is the \( n \)-standard set of type \( P \).

Observe that the sets \( A_1, \ldots, A_s \) are pairwise disjoint, and as a consequence of Proposition 4.5 we have the equality \( |A| = n - \varphi(n) \).

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 \( |A| \). We are interested in finding conditions for \( A \) to be a basis of \( \mathcal{G}_n \). First we need \( A \) 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 absolutely 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 $n = 12 = 2^3$ 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:

\[
\begin{align*}
m(2, 0) &= (1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0), \\
m(2, 1) &= (0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0), \\
m(2, 2) &= (0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0), \\
m(2, 3) &= (0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0), \\
m(2, 4) &= (0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0), \\
m(2, 5) &= (0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1), \\
m(3, 1) &= (0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0), \\
m(3, 3) &= (0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1).
\end{align*}
\]

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 $I_2 = \{1, 2, 5\}$. The 12-standard set $\mathcal{A}$ of type $[3, 2]$ is in this case the set of the following 8 sequences:

\[
\begin{align*}
m(3, 0) &= (1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0), \\
m(3, 1) &= (0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0), \\
m(3, 2) &= (0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1), \\
m(3, 3) &= (0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1), \\
m(2, 1) &= (0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0), \\
m(2, 2) &= (0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0), \\
m(2, 4) &= (0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0), \\
m(2, 5) &= (0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1).
\end{align*}
\]

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 $[2, 3]$.

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 $n = p_1p_2 \cdots p_{s-1}p_s^{\alpha_s}$, where $p_1, \ldots, p_s$ are distinct primes and $\alpha_s \geq 1$.

**Proposition 5.2.** Every power of a prime is an absolutely special number.
Proof. Let \( n = p^m \), where \( p \) is a prime and \( m \geq 1 \). 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, \( A = A_1 \) and, by Proposition 3.2, the set \( A \) is linearly independent over \( \mathbb{Z} \). \( \square \)

**Lemma 5.3.** Let \( p \) be a prime number, and let \( N \geq 2 \) 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 \( r + c_rN \) is divisible by \( p \). Moreover, all numbers of the form \( r + c_rN \) with \( 0 \leq r < N \) 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 \( r + c_rN = 0 \mod p \). 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, \( r_1 = r_2 \). \( \square \)

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

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

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

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, \( S(u) = \{ k \in \{0, 1, \ldots, n-1\}; u_k = 1 \} \).

Consider the case \( j = 1 \). Put \( p = p_1 \) and \( N = n_1 = n \cdot p = p_2 p_3 \cdots p_{s-1} \cdot p_s^\alpha \). 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 \( j \geq 2 \). 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 \( S(m(p_1, r)) = \{ r, r + N, r + 2N, \ldots, r + (p - 1)N \} \). It follows from Lemma 5.3 that in this support there exists exactly one element divisible by \( p \). Let us denote this element by \( r + c_rN \).
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 \( 2 \leq j_0 < s \), 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

\[
(b) \quad \sum_{j=j_0}^s \left( \sum_{r \in I_j} \gamma_r^{(j)} m(p_j, r) \right) = (0, 0, \ldots, 0),
\]

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

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

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

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

Look at the support of \( m(p_{j_0}, r) \) with \( r \in I_{j_0} \). We have \( S(m(p_{j_0}, r)) = \{ r, r + N, r + 2N, \ldots, r + (p - 1)N \} \}. 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 \( \gamma_r^{(j_n)} \), with \( r \in I_{j_n} \), are equal to zero.

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

\[
\sum_{r \in I_s} \gamma_r^{(s)} m(p_s, r) = (0, 0, \ldots, 0),
\]

where each \( \gamma_r^{(s)} \) is an integer. Now we use Proposition 3.2 and we have \( \gamma_r^{(s)}(s) = 0 \) for all \( r \in I_s \). Thus, we proved that in the equality (a) all the integers of the form \( \gamma_j \), where \( j \in \{1, \ldots, s\} \) 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 \( n \geq 2 \) is absolutely special.

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

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

\[ A_2. \text{ Moreover, } n_1 = \frac{p}{p} = pu, n_2 = \frac{q}{q} = pv, \]

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

\[ b = \sum_{k=0}^{v-1} q^{-1} p^{k+1+in_2} = \sum_{k=0}^{v-1} q^{-1} p^{k+1+ipw} = \sum_{k=0}^{v-1} \sum_{i=0}^{q} p^{k+1+ipw} = \sum_{k=0}^{v-1} e_{qj+1} = \sum_{j=0}^{n_1-1} e_{pj+1}. \]

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

**Lemma 5.7.** Let \( n = p_1^{\alpha_1} \cdots p_s^{\alpha_s} \), where \( s \geq 2 \), \( p_1, \ldots, p_s \) are distinct prime numbers and \( \alpha_1, \ldots, \alpha_s \) are positive integers. Let \( P = [p_1, \ldots, p_s] \). If there exists \( j_0 \in \{1, 2, \ldots, s-1\} \) such that \( \alpha_{j_0} \geq 2 \), 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 \( j_0 \geq 2 \), and let \( A_1, \ldots, A_s \) be the \( n \)-standard sets of type \( P \). Put \( N = p_1^{\alpha_1} \cdots p_{j_0-1}^{\alpha_{j_0-1}} \),

\[ p = p_{j_0}, \quad q = p_{j_0+1}, \quad u = \frac{n}{Np}, \quad v = \frac{n}{Npq}, \quad w = \frac{n}{pN}, \quad a = \sum_{k=0}^{u-1} m(p, pNk + 1), \quad \text{and} \]

\[ b = \sum_{k=0}^{v-1} m(q, pNk + 1). \]

Observe that \( a \) is a sum of elements from \( A_{j_0} \), and \( b \) is a sum of elements from \( A_{j_0+1} \). Moreover, \( n_{j_0} = \frac{p}{p} = pN, n_{j_0+1} = \frac{q}{q} = pNv, \)

\[ a = \sum_{k=0}^{u-1} p^{k+1+in_{j_0}} = \sum_{k=0}^{u-1} p^{k+1+iupN} = \sum_{k=0}^{u-1} p^{(k+iu)+1} = \sum_{j=0}^{n_1-1} e_{pj+1}, \]

\[ b = \sum_{k=0}^{v-1} q^{-1} p^{k+1+in_{j_0+1}} = \sum_{k=0}^{v-1} q^{-1} p^{k+1+iqv} = \sum_{k=0}^{v-1} p^{(k+iv)+1} = \sum_{j=0}^{n_1-1} e_{pj+1}. \]

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

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

**Theorem 5.8.** An integer \( n \geq 2 \) is special if and only if \( n = p_1p_2 \cdots p_s-1p_s^{\alpha_s} \), where \( p_1, \ldots, p_s \) are distinct primes and \( \alpha_s \geq 1 \).
Theorem 5.9. An integer \( n \geq 2 \) 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 \( n \geq 2 \) 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 \( G_n \).

Let us denote by \( \mathcal{A} \) the subgroup of \( G_n \) generated by \( \mathcal{A} \). Every element of \( \mathcal{A} \) is a finite combination over \( \mathbb{Z} \) of some elements of \( \mathcal{A} \).

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

Theorem 5.10. Let \( n = p_1 \cdots p_s - 1 \), \( \alpha \geq 1 \), and \( p_1, \ldots, p_s \) are pairwise different primes. Let \( P = [p_1, \ldots, p_s] \), and let \( \mathcal{A} \) be the \( n \)-standard set of type \( P \). Then every standard minimal element of \( M_n \) belongs to \( \mathcal{A} \).

Proof. First, all \( p_1 \)-standard elements \( m(p_1, r) \) with \( 0 \leq r < \frac{n}{p_1} \) belong to \( A_1 \) and thus to \( \mathcal{A} \).

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 \( A_j \)) as the number of primes among \( \{p_1, \ldots, p_j\} \) that divide \( r \) and denote it by \( h(m(p_j, r)) \). Elements of \( A_j \) 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 \( \mathcal{A} \).

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 \( h(m(p_j, r + kN)) \) 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 \( \mathcal{A} \) for all \( i < j \).

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

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 \( \mathcal{A} \), 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 \( n \geq 3 \) is an integer, \( K \) is a field of characteristic zero, \( K[X] = K[x_0, \ldots, x_{n-1}] \) is the polynomial ring over \( K \) in variables \( x_0, \ldots, x_{n-1} \), and \( K(X) = K(x_0, \ldots, x_{n-1}) \) 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 \( x_0, \ldots, x_{n-1} \) 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 \( \varepsilon \) a primitive \( n \)-th root of unity, and first we assume that \( \varepsilon \in K \).

The letters \( \varrho \) and \( \tau \) 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 \( u_0, u_1, \ldots, u_{n-1} \) the linear forms, belonging to \( K[X] \), defined by
\[ u_j = \sum_{i=0}^{n-1} (\varepsilon^j)^i x_i, \quad \text{for} \quad j \in \mathbb{Z}_n. \]
Then we have the equalities
\[ x_i = \frac{1}{n} \sum_{j=0}^{n-1} (\varepsilon^{-i})^j u_j, \]
for all \( i \in \mathbb{Z}_n \). Thus, \( K[X] = K[u_0, \ldots, u_{n-1}] \), \( K(X) = K(u_0, \ldots, u_{n-1}) \), and the forms \( u_0, \ldots, u_{n-1} \) are algebraically independent over \( K \). Moreover,
\[ \tau(u_j) = u_{j+1}, \quad \varphi(u_j) = \varepsilon^{-j} u_j, \quad d(u_j) = \varepsilon^{-j} u_j, \]
for all \( j \in \mathbb{Z}_n \).

It follows from the last equality that \( d \) is a diagonal derivation of the polynomial ring \( K[U] = K[u_0, \ldots, u_{n-1}] \) which is equal to the ring \( K[X] \).

If \( \alpha = (\alpha_0, \ldots, \alpha_{n-1}) \in \mathbb{Z}^n \), then we denote by \( u^\alpha \) 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 \( \varepsilon^{-1} \) 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 \( F = b_1 u^{\alpha^{(1)}} + \cdots + b_r u^{\alpha^{(r)}} \), where \( b_1, \ldots, b_r \in K \) and \( \alpha^{(1)}, \ldots, \alpha^{(r)} \) are pairwise different elements of \( \mathbb{N}^n \), then \( d(F) = 0 \) if and only if \( d(b_i u^{\alpha^{(i)}}) = 0 \) for every \( i = 1, \ldots, r \). In [10] we proved the following proposition.

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

1. the ring \( K[X]^d \) is generated over \( K \) by all elements of the form \( u^\alpha \) with \( \alpha \in \mathcal{M}_n \);
2. the ring \( K[X]^d \) is generated over \( K \) by all elements of the form \( u^\beta \), where \( \beta \) 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 \( u^\gamma \) 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 \( \gamma_0, \ldots, \gamma_{m-1} \) 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 \( w_0, \ldots, w_{m-1} \) defined by
\[ w_j = u^{\gamma_j} \quad \text{for } j = 0, 1, \ldots, m - 1. \]

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 $\varepsilon$ 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 $\varphi$ is the Euler totient function. More precisely,

$$K(X)^d = K\left(w_0, \ldots, w_{m-1}\right),$$

where the elements $w_0, \ldots, w_{m-1}$ 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 $\varepsilon$. Let us recall that if $p$ is a prime divisor of $n$ and $0 \leq r \leq \frac{n}{p} - 1$, then $m(p, r)$ is the standard minimal element of the monoid $\mathcal{M}_n$ defined by $m(p, r) = \sum_{i=0}^{p-1} e_{r+i} \frac{p}{n}$. Observe that if $a, b$ are integers such that $a \equiv b (\text{mod} \frac{n}{p})$, then $\sum_{i=0}^{p-1} e_{a+i} \frac{p}{n} = \sum_{i=0}^{p-1} e_{b+i} \frac{p}{n}$. Thus, we may define

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

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, $\zeta^a \left(m(p, b)\right) = m(p, b)$ for $b \in \mathbb{Z}$, and more general, $\zeta^a \left(m(p, b)\right) = m(p, a + b)$ for all $a, b \in \mathbb{Z}$ (see Proposition 3.4).

For every integer $a$, we define

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

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 $K[U] = K[w_0, \ldots, w_{m-1}]$. 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 $\varrho$ 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 $\varrho(S_{p,a}) = \varepsilon^{-b} S_{p,a}$, where $b = pa + \frac{(p-1)n}{2}$. In particular, if $p$ is odd then $\varrho(S_{p,a}) = \varepsilon^{-a} S_{p,a}$. If $p = 2$, then $n$ is even and $\varrho(S_{2,a}) = \varepsilon^{-2a+\frac{n}{2}} S_{2,a}$.

Recall the following well known lemma, which appears in many books of linear algebra.
Lemma 7.2. For any integer \( n \geq 2 \),

\[
u_0 u_1 \cdots u_{n-1} = \begin{vmatrix}
  x_0 & x_1 & \cdots & x_{n-1} \\
  x_{n-1} & x_0 & \cdots & x_{n-2} \\
  \vdots & \vdots & \ddots & \vdots \\
  x_1 & x_2 & \cdots & x_0 
\end{vmatrix}.
\]

In particular, the product \( u_0 u_1 \cdots u_{n-1} \) 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 \( b = \frac{n}{p} \), \( \eta = \zeta^b \), and \( v_i = u_{ib}, y_i = \sum_{j=0}^{p-1} x_i + j p \) for all \( i = 0, 1, \ldots, p-1 \). Then \( \eta \) is a primitive \( p \)-th root of unity, and \( v_i = \sum_{k=0}^{p-1} (\eta^j)^k y_k \), for all \( i = 0, 1, \ldots, p-1 \). Now we use Lemma 7.2, and we have

\[
S_{p,0} = v_0 v_1 \cdots v_{p-1} = \begin{vmatrix}
  y_0 & y_1 & \cdots & y_{p-1} \\
  y_{p-1} & y_0 & \cdots & y_{p-2} \\
  \vdots & \vdots & \ddots & \vdots \\
  y_1 & y_2 & \cdots & y_0 
\end{vmatrix}.
\]

Thus, \( S_{p,0} \in \mathbb{Z}[X] \). \( \square \)

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. Let \( n_j = \frac{n}{p_j} \) for \( j = 1, \ldots, s \). Assume that \( P = [p_1, \ldots, p_s] \) is a fixed type, and \( I_1, \ldots, I_s \) are the \( n \)-sets of type \( P \).

For every \( j \in \{1, \ldots, s\} \) we denote by \( V_j \) the \( K \)-subspace of \( K[U] \) generated by all the monomials \( S_{p,0} \) with \( r \in I_j \). Let us remember

\[
V_j = \langle S_{p,0}; r \in I_j \rangle, \quad \text{for} \quad j = 1, \ldots, s.
\]

We will say that \( V_1, \ldots, V_s \) 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 \( V_1, \ldots, V_s \) are \( n \)-spaces of type \( P = [p_1, \ldots, p_s] \), then \( \dim_K V_1 = n_1 \) and \( \dim_K V_j = n_j \left( \frac{1}{p_1} - \frac{1}{p_j} \right) \left( \frac{1}{p_2} - \frac{1}{p_j} \right) \cdots \left( \frac{1}{p_{j-1}} - \frac{1}{p_j} \right) \), for all \( j = 2, 3, \ldots, s \). Moreover,

\[
\dim_K (V_1 \oplus \cdots \oplus V_s) = n - \varphi(n).
\]

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 \( j = 1, \ldots, s \). Hence, for each \( j \) we have the equality \( V_j = \langle u^a; a \in \mathcal{A}_j \rangle \). Let \( \mathcal{S} \) the set of all the monomials \( u^a \) with \( a \in \mathcal{A} \), that is,

\[
\mathcal{S} = \left\{ S_{p,0}; j \in \{1, \ldots, s\}, \ r \in I_j \right\}.
\]
Proposition 7.5. If the number $n$ is special of type $P$, then the above set $S$ is algebraically independent over $K$, and $K(X)^d = K(S)$.

Proof. Assume that $n$ is special of type $P$. Let $\gamma_0, \ldots, \gamma_{m-1}$ be the elements of $G_n$ defined in Section 2, and let $w_i = u^{\gamma_i}$ for $i = 0, \ldots, m - 1$. Recall that $m = n - \varphi(n)$. Put $\Gamma = \{\gamma_0, \ldots, \gamma_{m-1}\}$, and $W = \{w_0, \ldots, w_{m-1}\}$. We know (see Theorem 2.3) that $\Gamma$ is a basis of $G_n$. Since $n$ is special, the set $\mathcal{A}$ is also a basis of $G_n$. 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, $|S| = |W| = m$ Hence, the set $S$ 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 $S$ 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 $T_{p,m}$

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

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

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

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 $j = 1, \ldots, s$, all the polynomials $T_{p_j,m}$ with $0 \leq m < n_j$, generate the $K$-space $\mathcal{V}_j$.

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

$$H = \sum_{m=0}^{n_j-1} (\varepsilon^{mp_j})^m \left( \sum_{r \in I_j} \varepsilon^{p_j,m} S_{p_j,r} \right) = \sum_{r \in I_j} \left( \sum_{m=0}^{n_j-1} \varepsilon^{mp_j,m} \right) S_{p_j,r}$$

$$= \sum_{r \in I_j} \left( \sum_{m=0}^{n_j-1} \eta^{mp_j,m} \right) S_{p_j,r} = n_j S_{p_j,q}.$$
In the last equality we used Lemma 4.6. Thus, if \( q \in I_j \), then \( S_{p_j,q} = \frac{1}{n_j} \sum_{m=0}^{n_j-1} (\varepsilon^{p_j})^m T_{p_j,m} \). But \( \varepsilon \in K \), so now it is clear that all \( T_{p_j,m} \) with \( 0 \leq m < n_j \), generate the \( K \)-space \( V_j \). \( \square \)

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 \( \tau \) 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

\[
S_{p_j} = \tau(S_{p_j,0})
\]

for \( j \in \{1, \ldots, s\} \) 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 \( \tau \)-homogeneous, if \( f \) is homogeneous in the ordinary sense and \( \tau(f) = \varepsilon^r f \) for some \( c \in \mathbb{Z}_n \). In this case we say that \( c \) is the \( \tau \)-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 \( \alpha = (\alpha_0, \ldots, \alpha_{n-1}) \in \mathbb{Z}^n \), is \( \tau \)-homogeneous and its \( \tau \)-degree is equal to \( \sum_{i=0}^{n-1} i \alpha_i \) (mod \( n \)).

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

Put \( C_i = \tau^{n_j}(B_i) \), for all \( i = 0, \ldots, n-1 \). 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,

\[
\tau(C_i) = \tau(\tau^{n_j}(B_i)) = \tau(\varepsilon^{in_j} B_i) = \varepsilon^{in_j} \tau(B_i) = \varepsilon^{in_j} \cdot \varepsilon^i B_i = \varepsilon^i \cdot \varepsilon^{in_j} B_i = \varepsilon^i C_i.
\]

Thus, every polynomial \( C_i \) is \( \tau \)-homogeneous of \( \tau \)-degree \( i \). Observe that

\[
\tau^{n_j}(S_{p_j,0}) = S_{p_j,0}.
\]

But \( \tau^{n_j}(S_{p_j,0}) = \sum_{i=0}^{n-1} C_i \), so \( C_i = \tau^{n_j}(B_i) = B_i \) and so, \( \varepsilon^{in_j} B_i = B_i \), for all \( i = 0, \ldots, n-1 \). 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,

\[
S_{p_j,0} = \sum_{k=0}^{n_j-1} B_k p_j,
\]
where each $B_{kp_j}$ is $\tau$-homogeneous polynomial from $\mathbb{Z}[X]$ of $\tau$-degree $kp_j$. Hence, for every $m \in \{0, \ldots, n - 1\}$, we have

$$T_{p_j, m} = \sum_{r \in I_j} \varepsilon^{-rp_j m} S_{p_j, r} = \sum_{r \in I_j} \varepsilon^{-rp_j m} \tau^r (S_{p_j, 0})$$

$$= \sum_{r \in I_j} \varepsilon^{-rp_j m} \tau^r \left( \sum_{k=0}^{n_j-1} B_{kp_j} \right) = \sum_{r \in I_j} \varepsilon^{-rp_j m} \left( \sum_{k=0}^{n_j-1} \tau^r (B_{kp_j}) \right)$$

$$= \sum_{r \in I_j} \varepsilon^{-rp_j m} \left( \sum_{k=0}^{n_j-1} \varepsilon^{kp_j r} B_{kp_j} \right) = \sum_{r \in I_j} B_{kp_j} \left( \sum_{r \in I_j} \varepsilon^{rp_j (k-m)} \right).$$

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 $s \geq 2$, and let $i, j \in \{1, \ldots, s\}$, $i < j$. Then

$$\sum_{k=0}^{p_j - 1} T_{p_j, k} = 0.$$

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

$$\sum_{k=0}^{p_j - 1} T_{p_j, k} \cdot \tau^{k/p_j} = \sum_{k=0}^{p_i - 1} T_{p_i, k} \cdot \tau^{k/p_i} \cdot \sum_{r \in I_j} \left( \varepsilon^{-kNq} \right)^r S_{q, r} = \sum_{r \in I_j} \left( \sum_{k=0}^{p_i - 1} \left( \varepsilon^{-k r/p_i} \right)^k \right) S_{q, r}.$$

Let $\eta = \varepsilon^{-1/p_i}$. Then $\eta$ is a primitive $p$-th root of unity. If $r \in I_j$, then $p \nmid r$ and, by Lemma 4.6, we have

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

Thus,

$$\sum_{k=0}^{p_i - 1} T_{p_j, k} \cdot \tau^{k/p_j} = \sum_{r \in I_j} \left( \sum_{k=0}^{p_j - 1} \left( \varepsilon^{-k r/p_j} \right)^k \right) S_{q, r} = \sum_{r \in I_j} 0 \cdot S_{q, r} = 0. \quad \square$$

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

$$\varphi(T_{p_j, a}) = \begin{cases} T_{p_j, a+1}, & \text{when } p_j \neq 2, \\ -T_{p_j, a+1}, & \text{when } p_j = 2. \end{cases}$$
RATIONAL CONSTANTS OF CYCLOMATIC DERIVATIONS

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

\[
\varrho(T_{p_j}, a) = \sum_{r \in I_j} (e^{-ap_j})^r \varrho(S_p, r) = \sum_{r \in I_j} (e^{-ap_j})^r e^{-p_j r} S_p, r = \sum_{r \in I_j} (e^{-(a+1)p_j})^r S_p, r = T_{p_j, a+1}.
\]

Now let \( p_j = 2 \). Then, by Proposition 7.1, \( \varrho(S_p, r) = e^{-(n_j r + \frac{n_j}{2})} S_p, r \) for any \( r \in \mathbb{Z} \). Moreover, \( e^{-\frac{n_j}{2}} = -1 \). Thus, we have

\[
\varrho(T_{p_j}, a) = \sum_{r \in I_j} (e^{-ap_j})^r \varrho(S_p, r) = \sum_{r \in I_j} (e^{-ap_j})^r e^{-(n_j r + \frac{n_j}{2})} S_p, r = - \sum_{r \in I_j} (e^{-(a+1)p_j})^r S_p, r = -T_{p_j, a+1}.
\]

This completes the proof. \( \square \)

Proposition 8.5. Assume that \( s \geq 2 \). Let \( i, j \in \{1, \ldots, s\} \), \( i < j \), and let \( a \in \mathbb{Z} \). Then

\[
T_{p_j, a} = - \sum_{k=1}^{p_j-1} T_{p_i, a+k \frac{n_j}{p_j r_j}}.
\]

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

\[
T_{p_j, a} = (-1)^{p_j-1} \varrho^a(T_{p_j, 0}) = (-1)^{p_j-1} \varrho^a \left( - \sum_{k=1}^{p_j-1} T_{p_j, k \frac{n_j}{p_j r_j}} \right)
= (-1)^{p_j} \sum_{k=1}^{p_j-1} \varrho^a \left( T_{p_j, k \frac{n_j}{p_j r_j}} \right) = (-1)^{p_j} \sum_{k=1}^{p_j-1} (-1)^{p_j-1} T_{p_j, a+k \frac{n_j}{p_j r_j}}
= - \sum_{k=1}^{p_j-1} T_{p_j, a+k \frac{n_j}{p_j r_j}},
\]

This completes the proof. \( \square \)

For any \( j \in \{1, \ldots, s\} \), let us denote by \( W_j \) the \( \mathbb{Z} \)-module generated by all the polynomials \( T_{p_j, r} \) with \( r \in I_j \). It is clear that every polynomial \( T_{p_j, a} \), for arbitrary integer \( a \), belongs to \( W_j \).

Theorem 8.6. If the number \( n \) is special, then for all \( j \in \{1, \ldots, s\} \) and \( a \in \mathbb{Z} \), the polynomial \( T_{p_j, a} \) belongs to \( W_j \).

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

Let \( j \) be a fixed element from \( \{1, \ldots, s\} \). If \( s = 1 \) or \( j = 1 \), then we are done. Assume that \( s \geq 2, j \geq 2 \), and \( a \) is an integer. Since \( T_{p_j, a} = T_{p_i, m} \), where \( m \) is
the remainder of division of $a$ by $n_j$, we may assume that $0 \leq a < n_j$. 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 $B_a \in W_j$. If $\gcd(a, p_1 \cdots p_{j-1}) = 1$, then $a \in I_j$ and so, $B_a \in W_j$. Now let $\gcd(a, p_1 \cdots p_{j-1}) \geq 2$. 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

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

Let $k \in \{1, \ldots, p_i-1\}$, and consider $c := a + k \frac{n}{p_i}$. Since $n$ is special, the number $k \frac{n}{p_i}$ 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 $p \mid k \frac{n}{p_i}$, 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, $B_c \in W_j$. Therefore, by the above equality, $B_a \in W_j$.

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

**Step 2.** Let $1 \leq t \leq j - 2$, and assume that we already proved that $B_c \in W_j$ 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: $m_1 \mid a$ for $i = 1, \ldots, t+1$, and $m \nmid a$ for $m \in M \setminus \{m_1, \ldots, m_{t+1}\}$. Put $p = m_{t+1}$.

It follows from Proposition 8.5, that have the following equality:

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

Let $k \in \{1, \ldots, p-1\}$, and consider $c := a + k \frac{n}{p}$. Since $n$ is special, the number $k \frac{n}{p}$ is not divisible by $p$. But $p \nmid a$, 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 $m \in M \setminus \{m_1, \ldots, m_t\}$. This means that $c$ is divisible by exactly $t$ primes from $M$. Thus, by our assumption, $B_c \in W_j$. Therefore, by the above equality, $B_a \in W_j$.

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 $n \geq 3$ is a special number of a type $P$. Let $I_1, \ldots, I_s$ be the $n$-sets of type $P$, let $A$ be the $n$-standard set of type $P$, and let

$$S = \left\{ S_{p_j, r}; \ j \in \{1, \ldots, s\}, \ r \in I_j \right\}, \quad T = \left\{ T_{p_j, r}; \ j \in \{1, \ldots, s\}, \ r \in I_j \right\}.$$
Since $n$ is special, we have the following sequence of important properties.

1. $A$ is a basis of the group $G_n$ (Theorems 5.8, 3.5 and 5.10).

2. $S$ is algebraically independent over $K$, and $K(X)^d = K(S)$ (Proposition 7.5).

3. $K(S) = K(T)$ (Proposition 8.1 and Theorem 8.6).

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

Let us recall, that $K$ is a field of characteristic zero containing $\varepsilon$ (where $\varepsilon$ 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 $Z[X]$, we see that we may assume that $K$ is a field of characteristic zero, without the assumption concerning $\varepsilon$. Thus, we proved the following theorem.

**Theorem 9.1.** Let $K$ be an arbitrary field of characteristic zero, $n \geq 3$ 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 $n = p_1 p_2 \cdots p_s$, where $s \geq 1$, $\alpha \geq 1$ and $p_1, \ldots, p_s$ are distinct primes. Let $m = n - \varphi(n)$, where $\varphi$ 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 $Q$ polynomials belonging to $Z[X]$.

More exactly, $\{F_0, F_1, \ldots, F_{m-1}\} = \{T_{p_j^r}; \ j \in \{1, \ldots, s\}, r \in I_j\}$, 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 $F_0 = x_0^2 - 2x_1 x_3 + x_2^2$, and $F_1 = \varphi(F_0)$.

**Example 9.3.** If $n = 8$, then $K(X)^d = K(F_0, F_1, F_2, F_3)$, where $F_1 = \varphi(F_0)$, $F_2 = \varphi^2(F_0)$, $F_3 = \varphi^3(F_0)$ and $F_0 = x_0^2 + x_2^2 - 2x_3 x_5 - 2x_7 x_1 + 2x_2 x_6$. 


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

\[
F_0 = 3x_1x_2^2 + 3x_3x_2 + 3x_8x_3^2 - 3x_0x_4x_5 - 3x_1x_0x_8 - 3x_2x_4x_3 - 3x_2x_7x_0 - 3x_8x_0x_4 + 3x_2x_5 + 3x_7x_6 + x_6^2 + 3x_1x_3x_9 + 6x_9x_6x_3 - 3x_8x_7x_3 - 3x_2x_1x_6 - 3x_5x_7x_6 + x_3^2.
\]

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

\[
F_0 = x_0^2 - 2x_1x_5 + 2x_2x_4 - x_3^2,
F_1 = (x_1^2 + x_4x_3 - x_0x_4 + x_1x_2 + x_3^2 - x_5x_3 + x_2x_3 - 2x_2x_5 + x_0x_5 - 2x_0x_3 - x_2x_2 - x_4x_0 + x_4^2 - x_1x_3 + x_2^2 + 4x_5 + x_1x_2 + x_0^2 - x_1x_5 - x_4x_2 + x_3^2)(x_0 - x_1 - x_2 - x_3 + x_4 - x_5),
\]

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 \( F_0 \), \( F_1 \), \( F_2 \), \( F_3 \) are as follows,

\[
F_0 = x_0^2 + x_1^2 + x_4^2 + 3x_0x_2^2 + 3x_2x_3^2 + 3x_4x_7^2 - 3x_0x_2x_4 - 3x_5x_0x_1 - 3x_1x_2x_3 - 3x_3x_4x_5,
F_1 = 2x_1^2 + x_4^2 - x_3^2 - 2x_1x_4 + x_3^2 + x_0^2 - 2x_1x_3 + 2x_2x_4 + 4x_3x_5 + 2x_4x_0 - 2x_5x_1 - 4x_2x_0,
\]

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

Example 9.7. If \( n = 12 \), then \( K(X)^d = K(F_0, \ldots, F_7) \), where \( F_0 \), \( F_1 \), \( F_2 \), \( F_3 \), \( F_4 \), \( F_5 \), \( F_6 \), \( F_7 \) are as follows,

\[
F_0 = -3x_0x_2x_4 - 3x_0x_8x_{10} - 3x_4x_0x_8 + x_0^3 + 3x_0^2x_0 - 3x_1x_8x_3 + 3x_0^2x_6 + 3x_2x_6 + 3x_3x_11x_0 + 6x_5x_11x_8 - 3x_1x_5x_6 + 3x_2^2x_10 + 3x_2x_4^2 - 3x_2x_7x_6 - 3x_7x_1x_3 - 3x_10x_11x_3 - 3x_10x_5x_9 - 3x_4x_11x_9 - 3x_4x_5x_3 - 3x_1x_2x_9 - 3x_5x_3x_2 - 3x_7x_2x_9 + x_7^2 - 3x_10x_2x_0,
F_1 = 4x_8x_8 + x_9^2 - 2x_10x_8 + 2x_7x_3 + 2x_7x_11 - 2x_10x_0 - 2x_4x_2 - 2x_4x_6 + 2x_1x_3 + 2x_1x_5 + 4x_0x_2 - 2x_0x_6 - 4x_3x_11 - 2x_7^2 + x_7^2 + 4x_4x_10 - 2x_2x_4 - 2x_7^2 + x_6^2 - 4x_9x_5,
\]

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

RATIONAL CONSTANTS OF CYCLOTOMIC DERIVATIONS


(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