AUTOMORPHISMS WITH EIGENVALUES IN $S^1$ OF A $\mathbb{Z}$-LATTICE WITH CYCLIC FINITE MONODROMY

CLAUS HERTLING

Abstract. For any finite set $M \subset \mathbb{Z}_{\geq 1}$ of positive integers, there is up to isomorphism a unique $\mathbb{Z}$-lattice $H_M$ with a cyclic automorphism $h_M : H_M \to H_M$ whose eigenvalues are the unit roots with orders in $M$ and have multiplicity 1. The paper studies the automorphisms of the pair $(H_M, h_M)$ which have eigenvalues in $S^1$. The main result are necessary and sufficient conditions on the set $M$ such that the only such automorphisms are $\pm h_M^k, k \in \mathbb{Z}$. The proof uses resultants and cyclotomic polynomials. It is elementary, but involved. Special cases of the main result have been applied to the study of the automorphisms of Milnor lattices of isolated hypersurface singularities.

Contents

1. Introduction and main result 1
2. Resultants of unitary polynomials in $\mathbb{Z}[x]$ 6
3. Some tie between cyclotomic polynomials 13
4. Necessity of the conditions in the main result in the connected case 18
5. Sufficiency of the conditions in the main result in the connected case 23
6. The proof of the main result in the disconnected case 29
References 33

1. Introduction and main result

In the study of the Milnor lattices of isolated hypersurface singularities, triples $(H_M, h_M, S)$ with the following properties arise (e.g. [He11]).

Date: January 24, 2018.
2010 Mathematics Subject Classification. 15B36, 13F20, 15A27, 32S40.
Key words and phrases. resultants, cyclotomic polynomials, cyclic monodromy, automorphisms respecting monodromy and bilinear form, Milnor lattice.

This work was supported by the DFG grant He2287/4-1 (SISYPH).
$H_M$ is a $\mathbb{Z}$-lattice of a finite rank $n \in \mathbb{Z}_{\geq 1}$. It comes with an automorphism $h_M : H_M \to H_M$, which is called monodromy, and with an $h_M$-invariant bilinear form $S$. The monodromy is quasiumipotent, i.e. its eigenvalues are unit roots, all eigenvalues have multiplicity 1, and $H_M$ has a cyclic generator with respect to $h_M$, i.e. an element $e_1 \in H_M$ with

$$H_M = \bigoplus_{i=1}^{n} \mathbb{Z} \cdot h_M^{i-1}(e_1).$$  \hspace{1cm} (1.1)

The restriction of the bilinear form to the sum $\bigoplus_{\lambda \neq \pm 1} H_{\lambda}$ is nondegenerate. Here $H_\mathbb{C} := H_M \otimes \mathbb{C}$ and $H_{\lambda} := \ker(h_M - \lambda \text{id} : H_\mathbb{C} \to H_\mathbb{C})$ is the eigenspace with eigenvalue $\lambda$.

The pair $(H_M, h_M)$ up to isomorphism is determined by the set $M := \{ m \in \mathbb{Z}_{\geq 1} \mid e^{2\pi i / m} \text{ is an eigenvalue of } h_M \}$. \hspace{1cm} (1.2)

The characteristic polynomial is $\prod_{m \in M} \Phi_m$. Here $\Phi_m$ is the cyclotomic polynomial whose zeros are the unit roots of order $m$. In the singularity case, the bilinear form may be the intersection form or the Seifert form. For the following problem, the precise form of the bilinear form $S$ does not matter, only the properties above. Lemma 4.1 will show

$$\text{Aut}(H_M, h_M, S) = \{ a \in \text{Aut}(H_M, h_M) \mid \text{all eigenvalues of } a \text{ are in } S^1 \}. \hspace{1cm} (1.3)$$

The problem is to determine the conditions on the eigenvalues of $h_M$ such that $\text{Aut}(H_M, h_M, S) = \{ \pm h_M^k \mid k \in \mathbb{Z} \}$. Theorem 1.2 gives the complete answer. The conditions are involved and are given as properties of a graph $G(M)$. The graph and the conditions are formulated in the following definition.

**Definition 1.1.** Let $M \subset \mathbb{Z}_{\geq 1}$ be a finite set of positive integers.

(a) A graph $G(M) = (M, E(M))$ is associated to it as follows. $M$ itself is the set of vertices. The edges in $E(M)$ are directed. The set $E(m)$ is defined as follows. From a vertex $m_1 \in M$ to a vertex $m_2 \in M$ there is no edge if at least one of the following two conditions holds:

(i) $m_1/m_2$ is not a power of a prime number.
(ii) An $m_3 \in M - \{ m_1, m_2 \}$ with $m_2|m_3|m_1$ exists.

If $m_1/m_2$ is a power $p^k$ with $k \in \mathbb{Z}_{\geq 1}$ of a prime number $p$ and if no $m_3 \in M - \{ m_1, m_2 \}$ with $m_2|m_3|m_1$ exists, then there is a directed edge from $m_1$ to $m_2$, which is additionally labelled with $p$. It is called a $p$-edge. Together such edges form the set $E(M)$ of all edges.
(b) For any prime number $p$ the components of the graph $(M, E(M) - \{p\text{-edges}\})$ which is obtained by deleting all $p$-edges, are called the $p$-planes of the graph. A $p$-plane is called a highest $p$-plane if no $p$-edge ends at a vertex of the $p$-plane. A $p$-edge from $m_1$ to $m_2$ is called a highest $p$-edge if no $p$-edge ends at $m_1$.

(c) A property $(T_p)$ for a prime number $p$ and a property $(S_2)$ for the prime number 2:

$(T_p) :$ The graph $\mathcal{G}(M)$ has only one highest $p$-plane.  \hfill (1.4)

$(S_2) :$ The graph $(M, E(M) - \{\text{highest } 2\text{-edges}\})$ has only 1 or 2 components.  \hfill (1.5)

(d) The least common multiple of the numbers in $M$ is denoted \(\text{lcm}(M) \in \mathbb{Z}_{\geq 1}\). For any prime number $p$ denote

\[
l(m, p) := \max(l \in \mathbb{Z}_{\geq 0} \mid p^l \text{ divides } m) \quad \text{for any } m \in \mathbb{Z}_{\geq 1},
\]

\[
l(M, p) := \max(l(m, p) \mid m \in M) = l(\text{lcm}(M), p).
\]

Then $m = \prod_{p \text{ prime number}} p^{l(m, p)}$.

The conditions will be discussed after theorem 1.2 in the remarks 1.3. Examples will be given in 1.4. The following theorem is the main result of this paper.

**Theorem 1.2.** Let $M \subset \mathbb{Z}_{\geq 1}$ be a finite set of positive integers, and let $(H_M, h_M, S)$ be a triple as above such that $M$ is the set of orders of the eigenvalues of $h_M$. Then

\[\text{Aut}(H_M, h_M, S) = \{\pm h_M^k \mid k \in \mathbb{Z}\}\]  \hfill (1.6)

holds if and only if the graph $\mathcal{G}(M)$ satisfies one of the following two properties.

(I) $\mathcal{G}(M)$ is connected. It satisfies $(S_2)$. It satisfies $(T_p)$ for any prime number $p \geq 3$.

(II) $\mathcal{G}(M)$ has two components $M_1$ and $M_2$. The graphs $\mathcal{G}(M_1)$ and $\mathcal{G}(M_2)$ are 2-planes of $\mathcal{G}(M)$ and satisfy $(T_p)$ for any prime number $p \geq 3$. Furthermore

\[
gcd(\text{lcm}(M_1), \text{lcm}(M_2)) \in \{1; 2\},
\]

\[
l(M_1, 2) > l(M_2, 2) \in \{0; 1\}.  \hfill (1.7)
\]

The theorem will be proved in the sections 4, 5 and 6.

**Remarks 1.3.** Let $M$ and $\mathcal{G}(M)$ be as in definition 1.1.

(i) For any $l \in \mathbb{Z}_{\geq 1}$ and any prime number $p$, the set $\{m \in M \mid l(m, p) = l\}$ consists of finitely many $p$-planes.
(ii) From $G(M)$ and a prime number $p$, one obtains a smaller graph $G(M)^{(p)}$ as follows. Its vertices are the $p$-planes of $G(M)$. There is a directed edge from a $p$-plane $E_1$ to a $p$-plane $E_2$ if $E(M)$ contains a $p$-edge from a vertex in $E_1$ to a vertex in $E_2$.

(iii) The condition $(T_p)$ is equivalent to the condition that there is a vertex in $G(M)^{(p)}$ from which one can reach all other vertices in $G(M)^{(p)}$ if one follows some directed edges. Especially, $(T_p)$ implies that $G(M)$ is connected.

(iv) Any highest 2-plane is a component of the graph $(M, E(M) - \{\text{highest 2-edges}\})$. Therefore, if $(S_2)$ holds and $G(M)$ is connected, also $(T_2)$ holds. If $(S_2)$ holds and $G(M)$ is not connected, then $G(M)$ has 2 components and each of them is a 2-plane (and thus there are no 2-edges).

Examples 1.4. (i) The graph $G(M)$ for $M := \{12, 6, 4, 3, 2\}$ has the 2-edges: $(12, 6), (6, 3), (4, 2)$, 2-planes: $\{12, 4\}, \{6, 2\}, \{3\}$, 3-edges: $(12, 4), (6, 2)$, 3-planes: $\{12, 6, 3\}, \{4, 2\}$.

For all prime numbers $p \geq 5$, $M$ itself is the only $p$-plane, and there are no $p$-edges. Case (I) of theorem 1.2 holds. The highest 2-edges are $(12, 6), (12, 3), (4, 2)$, and all 3-edges are highest 3-edges. The graphs $G(M)^{(2)}$ and $G(M)^{(3)}$ are just directed chains with 3 respectively 2 vertices.

For all prime numbers $p \geq 7$ $M$ itself is the only $p$-plane, and there are no $p$-edges. For any $p \in \{2, 3, 5\}$, the $p$-edge is a highest $p$-edge.
(iii) Case (II) of theorem 1.2 holds for the graph $G(M)$ of the set $M = \{45, 15, 14, 5, 3, 2\}$ with $M_1 = \{14, 2\}$ and $M_2 = \{45, 15, 5, 3\}$.

M in (iii)  

\[
\begin{array}{c}
14 & 45 & 3 \\
7 & & \\
2 & 15 & 3 \\
3 & & \\
\end{array}
\]

M in (iv)  

\[
\begin{array}{c}
20 & 5 & 4 \\
2 & & \\
5 & 6 & \\
3 & & \\
\end{array}
\]

(iv) The graph $G(M)$ of the set $M = \{24, 20, 6, 5, 4, 3, 2\}$ is connected and satisfies $(T_3)$ and $(T_5)$, but not $(T_2)$ and thus not $(S_2)$. It has the 2-planes: \{24\}, \{20, 4\}, \{6, 2\}, \{5\}, \{3\}.

3-planes: \{24, 6, 3\}, \{20, 5, 4, 2\}.

5-planes: \{20, 5\}, \{24, 6, 4, 3, 2\}.

The 2-planes \{24\} and \{20, 4\} are both highest 2-planes. Theorem 1.2 says $\text{Aut}(H_M, h_M, S) \supseteq \{\pm h_M^k | k \in \mathbb{Z}\}$.

(v) The graph $G(M)$ of the set $M = \{2^6, 3^7, 5^8\}$ has 3 components. Theorem 1.2 says $\text{Aut}(H_M, h_M, S) \supseteq \{\pm h_M^k | k \in \mathbb{Z}\}$.

(vi) Lemma 8.2 in [He11] gives the following sufficient condition for $\text{Aut}(H_M, h_M, S) = \{\pm h_M^k | k \in \mathbb{Z}\}$. It is a special case of case (I) in theorem 1.2. M contains a largest number $m_1$ such that $G(M)$ is a directed graph with root $m_1$. This implies $(T_p)$ for any $p$. Additionally, a chain of 2-edges exists which connects all 2-planes. This implies $(S_2)$. The more special case where $M$ is a 2-plane and a directed graph with root $m_1$, was considered and applied in the proof of [He98, proposition 6.3].

The special case [He11, lemma 8.2] of theorem 1.2 was applied in [He98], [He11], [GH16] and [GH17] in order to study automorphism groups of Milnor lattices of isolated hypersurface singularities. Though often not the full Milnor lattice is a triple $(H_M, h_M, S)$ as above, but it contains sublattices which are such triples. In this form, [He11, lemma 8.2] applies also to some singularities whose monodromy is not semisimple (the $T_{pq}$ in [GH16]). But we expect that for other singularities the more general conditions in theorem 1.2 will be needed, and
we hope that they will be satisfied. Conjecture 1.4 in \cite{HZ18} makes our expectations for quasihomogeneous singularities precise.

The paper is organized as follows. Section 2 studies the resultant of unitary polynomials $f$ and $g$ with coefficients in $\mathbb{Z}[x]$ and its relation to the sublattices $(f, g) \cap \mathbb{Z}[x]_{\leq k}$ of the lattices $\mathbb{Z}[x]_{\leq k} := \{a \in \mathbb{Z}[x] \mid \deg a \leq k\}$ for $k \in \mathbb{Z}_{\geq 0}$. Lemma 2.3 gives fundamental properties, the lemmata 2.4 and 2.5 give statements which will be applied in the proof of theorem 1.2. Section 3 recalls in theorem 3.1 basic properties of the cyclotomic polynomials $\Phi_m$, including the values $\Phi_m(1)$ and Apostol’s formulas for the resultant of two cyclotomic polynomials \cite{Ap70}. Theorem 3.4 gives a tie between different cyclotomic polynomials which is crucial for the proof of the sufficiency of the conditions in theorem 1.2. It was stated before as lemma 6.5 in \cite{He98}. Section 4 proves the necessity of the conditions in theorem 1.2 in the case when $G(M)$ is connected. Section 5 proves the sufficiency of the conditions in this case. Section 6 proves theorem 1.2 in the case when $G(M)$ is not connected.

**Notations 1.5.** For any polynomial $f \in \mathbb{C}[x] - \{0\}$, the coefficients are denoted $f_0, \ldots, f_{\deg f} \in \mathbb{C}$. If $f = 0$, then $f_0 := 0$ and $\deg f := -\infty$.

The empty product has value 1. The empty sum has value 0.

$\lambda$ will always denote a unit root in $S^1 \subset \mathbb{C}$, and $\text{ord}(\lambda)$ will be its order, i.e. the minimal $k \in \mathbb{Z}_{\geq 1}$ with $\lambda^k = 1$.

$e(z)$ for $z \in \mathbb{C}$ will denote $e^{2\pi iz} \in \mathbb{C}$, so for example $e(r)$ for $r \in \mathbb{Q}$ is a unit root.

For $m \in \mathbb{Z}_{\geq 1}$ denote $\mathbb{Z}/m\mathbb{Z} =: \mathbb{Z}_m$, and for $a \in \mathbb{Z}$ denote its class in $\mathbb{Z}_m$ by $[a]_m$.

---

2. Resultants of unitary polynomials in $\mathbb{Z}[x]$  

The resultant of two polynomials is a very classical object. One reference for the following definition is \cite{vW71} §34.

**Definition 2.1.** The resultant of two polynomials $f = \sum_{i=0}^m f_ix^i \in \mathbb{C}[x] - \{0\}$ and $g = \sum_{j=0}^n g_jx^j \in \mathbb{C}[x] - \{0\}$ of degrees $\deg f = m$, $\deg g = n$ with $m + n \geq 1$ is $R(f, g) := \det A(f, g) \in \mathbb{C}$ where
AUTOMORPHISMS OF A $Z$-LATTICE WITH CYCLIC FINITE MONODROMY

$A(f, g) \in M((m + n) \times (m + n), \mathbb{C})$ is the matrix

$$A(f, g) = \begin{pmatrix} f_0 & 0 & \cdots & 0 & g_0 & 0 & \cdots & 0 \\ f_1 & f_0 & \cdots & g_1 & g_0 & \cdots & \\ \vdots & f_1 & \cdots & 0 & g_1 & \cdots & \\ \vdots & \vdots & \cdots & f_0 & \cdots & g_0 & \\ f_m & \cdots & f_1 & g_n & \cdots & g_1 \\ 0 & \cdots & 0 & 0 & \cdots & \cdots & \\ \vdots & \vdots & \cdots & \vdots & \cdots & \cdots & \\ 0 & \cdots & 0 & f_m & 0 & \cdots & 0 & g_n \end{pmatrix} \quad (2.1)$$

whose first $n$ columns contain the coefficients of $f$ and whose last $m$ columns contain the coefficients of $g$. In other words, it is the matrix with

$$(f, xf, \ldots, x^{n-1}f, g, xg, \ldots, x^{m-1}g) = (1, x, \ldots, x^{m+n-1}) \cdot A(f, g). \quad (2.2)$$

In the case $m + n = 0$ one defines $R(f, g) := 1$.

The basic properties of the resultant are well known.

Proposition 2.2. (a) Let $f$ and $g \in \mathbb{C}[x]$ be as in definition 2.1. Let $a_1, \ldots, a_m \in \mathbb{C}$ and $b_1, \ldots, b_n \in \mathbb{C}$ be the zeros of $f$ and $g$, so

$$f = f_0 \prod_{i=1}^{m} (x - a_i), \quad g = g_0 \prod_{j=1}^{n} (x - b_j).$$

Then

$$R(f, g) = f_0^n g_0^m \cdot \prod_{i=1}^{m} \prod_{j=1}^{n} (a_i - b_j) \quad (2.3)$$

$$R(f, g) \neq 0 \iff \gcd(f, g)_{\mathbb{C}[x]} = 1. \quad (2.4)$$

(b) If $f, g, h \in \mathbb{C}[x] - \{0\}$ then

$$R(f, gh) = R(f, g) \cdot R(f, h). \quad (2.5)$$

If $f^{(1)}, \ldots, f^{(r)}$, $g^{(1)}, \ldots, g^{(s)} \in \mathbb{C}[x] - \{0\}$ then

$$R(\prod_{i=1}^{r} f^{(i)}, \prod_{j=1}^{s} g^{(j)}) = \prod_{i=1}^{r} \prod_{j=1}^{s} R(f^{(i)}, g^{(j)}). \quad (2.6)$$

(2.3) is proved for example in [vW71, §35], (2.4), (2.5) and (2.6) follow from (2.3), and (2.7) follows from (2.6) and (2.4).
We are mainly interested in $R(f, g)$ where $f$ and $g$ are unitary polynomials (i.e. $f_{\text{deg } f} = 1, g_{\text{deg } g} = 1$) in $\mathbb{Z}[x]$. We denote for $k \in \mathbb{Z}_{\geq -1}$
\begin{align*}
\mathbb{C}[x]_{\leq k} & := \{ h \in \mathbb{C}[x] | \deg h \leq k \}, \\
\mathbb{Z}[x]_{\leq k} & := \mathbb{C}[x]_{\leq k} \cap \mathbb{Z}[x]
\end{align*}
(2.8)
(since $\mathbb{C}[x]_{\leq -1} = \mathbb{Z}[x]_{\leq -1} = \{ 0 \}$).

**Lemma 2.3.** Let $f, g \in \mathbb{Z}[x]$ be unitary polynomials of degrees $m = \text{deg } f, n = \text{deg } g$. They generate an ideal $(f, g) \subset \mathbb{Z}[x]$ (here $\mathbb{Z}[x]$ is also considered as an ideal).

(a) $Z[x]_{\leq n-1} \cdot f + Z[x]_{\leq m-1} \cdot g = (f, g) \cap Z[x]_{\leq m+n-1}$. 

(b) The $\mathbb{Z}$-lattice in (2.9) has rank $m + n$ if and only if $R(f, g) \neq 0$, and then
\[ |R(f, g)| = \frac{Z[x]_{\leq m+n-1}}{(f, g) \cap Z[x]_{\leq m+n-1}} \in \mathbb{Z}_{>0}. \]  

(2.10)

(c) Suppose that $R(f, g) \neq 0$. Then polynomials $h^{(0)}_0, h^{(1)}_1, \ldots, h^{(m+n-1)}_{m+n-1} \in \mathbb{Z}[x]$ with the properties in (2.11) -- (2.14) exist:
\begin{equation}
(f, g) \cap Z[x]_{\leq m+n-1} = \bigoplus_{i=0}^{m+n-1} \mathbb{Z} \cdot h^{(i)}_i, 
\end{equation}
(2.11)
\[ \deg h^{(i)}_i = i \text{ for any } i, \]  

(2.12)
\[ h^{(i)}_i > 0 \text{ for any } i, \quad h^{(i+1)}_i | h^{(i)}_i \text{ for any } i < m + n - 1, \]  

(2.13)
\[ h^{(i)}_i = 1 \text{ for all } i \geq \min(\text{deg } f, \text{deg } g). \]  

(2.14)
The coefficients $h^{(0)}_0, h^{(1)}_1, \ldots, h^{(m+n-1)}_{m+n-1}$ are unique.
\begin{equation}
|R(f, g)| = \prod_{i=0}^{m+n-1} h^{(i)}_i. 
\end{equation}
(2.15)

(d) $|R(f, g)| = 1 \iff (f, g) = \mathbb{Z}[x]$. 

**Proof:** In the case $m = n = 0 \ f = g = 1$ and all statements are trivial. So we restrict to the case $m + n \geq 1$.

(a) The ideal is $(f, g) = \mathbb{Z}[x] \cdot f + \mathbb{Z}[x] \cdot g \subset$ is obvious.

(b) For any $h \in (f, g) \cap Z[x]_{\leq m+n-1}$ let $a, b \in Z[x]$ be such that $h = a \cdot f + b \cdot g$
and such max$(m + \deg a, n + \deg b)$ is minimal. We have to show max$(m + \deg a, n + \deg b) < m + n$. Suppose that max$(m + \deg a, n + \deg b) \geq m + n$.

...
This finishes the inductive proof. The case $i \geq m + n$ for some $h \in (f, g) \cap \mathbb{Z}[x]_{\leq m+n-1}$. As $\deg h \leq m + n - 1$ and $f$ and $g$ are unitary, $m + \deg a = n + \deg b$ and $a_{\deg a} + b_{\deg b} = 0$. Therefore

$$h = (a - a_{\deg a} \cdot x^{\deg a - n} \cdot g) \cdot f + (b - b_{\deg b} \cdot x^{\deg b - m} \cdot f) \cdot g.$$ Obviously $\deg(a - a_{\deg a} \cdot x^{\deg a - n} \cdot g) < \deg a$ and $\deg(b - b_{\deg b} \cdot x^{\deg b - m} \cdot f) < \deg b$. This is a contradiction to the minimality of $\max(m + \deg a, n + \deg b)$. Thus $\max(m + \deg a, n + \deg b) < m + n$.

(b) This follows immediately from (2.9), (2.12) and $R(f, g) = \det A(f, g)$.

(c) $R(f, g) \neq 0$ implies $\gcd_{\mathbb{C}[x]}(f, g) = 1$. Thus $(f, g) \cap \mathbb{Z} \supseteq \{0\}$ and $(f, g) \cap \mathbb{Z}[x]_{\leq k}$ is a $\mathbb{Z}$-lattice of rank $k + 1$ for any $k \in \mathbb{Z}[x]_{\geq 0}$. For $i = 0, 1, \ldots, m + n - 1$, let $h^{(i)}$ be an element of $(f, g) \cap \mathbb{Z}[x]_{\leq i} - \mathbb{Z}[x]_{\leq i - 1}$ (respectively $(f, g) \cap \mathbb{Z}$ if $i = 0$) such that $h^{(i)}_{\deg} \in \mathbb{Z}$ is positive and minimal.

We show inductively for $i = 0, 1, \ldots, m + n - 1$, that $h^{(0)}, \ldots, h^{(i)}$ is a $\mathbb{Z}$-basis of $(f, g) \cap \mathbb{Z}[x]_{\leq i}$. The case $i = 0$ is clear. Suppose it is true for some $i < m + n - 1$. Let $a \in (f, g) \cap \mathbb{Z}[x]_{\leq i+1}$. We have to show $a \in (f, g) \cap \mathbb{Z}[x]_{\leq i} \oplus \mathbb{Z} \cdot h^{(i+1)}$. The case $\deg a \leq i$ is trivial, so suppose $\deg a = i + 1$. The minimality of $h^{(i+1)}_{\deg}$ shows $h^{(i+1)}_{\deg} | a_{i+1}$. Thus

$$a - \frac{a_{i+1}}{h^{(i+1)}_{\deg}} \cdot h^{(i+1)} \in (f, g) \cap \mathbb{Z}[x]_{\leq i}.$$ This finishes the inductive proof. The case $i = m + n - 1$ is (2.11), (2.12) and $h^{(i)}_{\deg} > 0$ hold by definition of $h^{(i)}$. Observe $\deg(x \cdot h^{(i)}) = i + 1$. This and the minimality of $h^{(i+1)}_{\deg}$ show $h^{(i+1)}_{\deg} | h^{(i)}_{\deg}$. (2.14) holds because of $f, g \in (f, g)$ and because they are unitary. The equations

$$\prod_{j=0}^{i} h^{(j)}_{\deg} = \left\lvert \frac{\mathbb{Z}[x]_{\leq i}}{(f, g) \cap \mathbb{Z}[x]_{\leq i}} \right\rvert \quad \text{for } i = 0, \ldots, m + n - 1 \quad (2.17)$$

hold because $h^{(0)}, \ldots, h^{(i)}$ is a $\mathbb{Z}$-basis of $(f, g) \cap \mathbb{Z}[x]_{\leq i}$ and because the matrix which expresses them as linear combinations of $x^0, x^1, \ldots, x^i$, is triangular. Together they show the uniqueness of $h^{(0)}, h^{(1)}_{\deg}, \ldots, h^{(m+n-1)}_{\deg}$. The case $i = m + n - 1$ and (2.10) give (2.15).

(d) By (2.15) and (2.13),

$$|R(f, g)| = 1 \iff h^{(0)}_{\deg} = 1 \iff (f, g) = \mathbb{Z}[x]$$

$\square$
Lemma 2.4, lemma 2.5 and lemma 3.2 will be used in section 4 in order to show that the condition \((S_2)\) is necessary in case (I) in theorem 1.2. So, there only the case \(p = 2\) will be used. Though lemma 2.4 is fairly interesting in its own right.

**Lemma 2.4.** Let \(f, g \in \mathbb{Z}[x]\) be unitary polynomials of degrees \(m = \deg f, n = \deg g\). Suppose \(m \geq n\). Let \(p\) be a prime number. Consider the following four conditions.

1. \(|R(f, g)| = p^n\).
2. \((f, g) = (p, g)\).
3. \(p \in (f, g)\).
4. \(f \in (p, g)\).

Then

\[(2) \iff (3) \& (4) \iff (1) \& (3) \iff (1) \& (4)\] (2.18)

**Proof:** In the case \(m = n = 0\) \(f = g = 1\) and \(1)-(4)\) hold trivially. So we restrict to the case \(m + n \geq 1\).

First we show

\[\mathbb{Z}[x]_{\leq n-1} \cdot p \oplus \mathbb{Z}[x]_{\leq m-1} \cdot g = (p, g) \cap \mathbb{Z}[x]_{\leq m+n-1}\] (2.19)

\(\subset\) is trivial. The proof of \(\supset\) is similar to the one of \(\supset\) in (2.9): For any \(h \in (p, g) \cap \mathbb{Z}[x]_{\leq m+n-1}\) let \(a, b \in \mathbb{Z}[x]\) be such that

\[h = a \cdot p + b \cdot g\]

and such that \(\deg a\) is minimal. We will show \(\deg a \leq n - 1\). Suppose \(\deg a \geq n\). Then

\[h = (a - a_{\deg a} \cdot x^{\deg a-n} \cdot g) \cdot p + (b + a_{\deg a} \cdot p \cdot x^{\deg a-n}) \cdot g,\]

and \(\deg(a - a_{\deg a} \cdot x^{\deg a-n} \cdot g) < \deg a\), a contradiction. Thus \(\deg a \leq n - 1\). But now \(\deg h \leq m + n - 1\) and \(\deg g = n\) imply immediately \(\deg b \leq m - 1\). This shows (2.19).

(2.19) implies

\[|\mathbb{Z}[x]_{\leq m+n-1} | = p^n.\] (2.20)

Now the equivalences in (2.18) will be proved. (2) \iff (3) \& (4) is trivial.

If (1) holds, then by (2.10) and (2.20)

\[|\frac{\mathbb{Z}[x]_{\leq m+n-1}}{(f, g) \cap \mathbb{Z}[x]_{\leq m+n-1}}| = p^n = |\frac{\mathbb{Z}[x]_{\leq m+n-1}}{(p, g) \cap \mathbb{Z}[x]_{\leq m+n-1}}|.\] (2.21)
Therefore, if (1) holds and if one of the two sets \((f, g) \cap \mathbb{Z}[x]_{\leq m+n-1}\) and \((p, g) \cap \mathbb{Z}[x]_{\leq m+n-1}\) is a subset of the other, they are equal. This shows (1)\&(3) \iff (1)\&(4) \Rightarrow (2).

Finally, if (2) holds, then (2.10) and (2.20) imply (1). \(\square\)

Lemma 2.5 will be used in the case \(p = 2\) in section 4 for the treatment of the condition \((S_2)\).

Lemma 2.5. Let \(p\) be a prime number, and let \(f^{(1)}, ..., f^{(a)}, f^{(a+b)}, g^{(1)}, ..., g^{(a)}, g^{(a+c)} \in \mathbb{Z}[x]\) (with \(a \geq 1, b \geq 0, c \geq 0\)) be unitary polynomials. For \(i \in \{1, ..., a\}\) define polynomials \(h^{(i)}\) by

\[
h^{(i)} := \begin{cases} f^{(i)} & \text{if } \deg f^{(i)} < \deg g^{(i)}, \\ g^{(i)} & \text{if } \deg f^{(i)} \geq \deg g^{(i)}. \end{cases}
\]

Suppose

\[
|R(f^{(i)}, g^{(j)})| = 1 \quad \text{for any } i \neq j \text{ and for } i = j \geq a + 1, \quad (2.22)
\]

\[
(f^{(i)}, g^{(i)}) = (p, h^{(i)}) \quad \text{for } i \in \{1, ..., a\}. \quad (2.23)
\]

Then

\[
\prod_{i=1}^{a+b} f^{(i)} \prod_{j=1}^{a+c} g^{(j)} = (p, \prod_{i=1}^{a} h^{(i)}). \quad (2.24)
\]

**Proof:** First we consider the special case \(b = c = 0\) and \(h^{(i)} = g^{(i)}\). Define

\[
f := \prod_{i=1}^{a} f^{(i)}, \quad g := \prod_{j=1}^{a} g^{(j)}.
\]

Because of (2.23), \(f^{(i)}\) and \(g^{(i)}\) satisfy all conditions in lemma 2.4, especially condition (1):

\[
|R(f^{(i)}, g^{(i)})| = p^{\deg g^{(i)}}.
\]

This and (2.22) and (2.7) imply

\[
|R(f, g)| = p^{\deg g},
\]

which is condition (1) in lemma 2.4 for \(f\) and \(g\). Because \(f^{(i)}\) and \(g^{(i)}\) satisfy all conditions in lemma 2.4 and because of (2.19), there exist polynomials \(q^{(i)} \in \mathbb{Z}[x]_{\leq m-1}\) and \(r^{(i)} \in \mathbb{Z}[x]_{\leq \deg g^{(i)} - 1}\) with

\[
f^{(i)} = q^{(i)} \cdot g^{(i)} + p \cdot r^{(i)}.
\]

Therefore

\[
f = \prod_{i=1}^{a} (q^{(i)} \cdot g^{(i)} + p \cdot r^{(i)}) = \left(\prod_{i=1}^{a} q^{(i)}\right) \cdot g + p \cdot \tilde{r}
\]
for some polynomial \( \overline{r} \in \mathbb{Z}[x]_{\leq \deg g-1} \). This is condition (4) in lemma 2.4 for \( f \) and \( g \). Therefore \( f \) and \( g \) satisfy all conditions in lemma 2.4. Condition (2) is (2.24) in the special case.

Now we consider the general case. We can suppose that the polynomials are numbered such that

\[
g^{(i)} = h^{(i)} \text{ for } 1 \leq i \leq d \leq a,
\]

\[
f^{(i)} = h^{(i)} \text{ for } d + 1 \leq i \leq a.
\]

Define

\[
a^{(1)} := \prod_{i=1}^{d} f^{(i)}, \quad a^{(2)} := \prod_{i=d+1}^{a} f^{(i)}, \quad a^{(3)} := \prod_{i=a+1}^{b} f^{(i)},
\]

\[
b^{(1)} := \prod_{i=1}^{d} g^{(i)}, \quad b^{(2)} := \prod_{i=d+1}^{a} g^{(i)}, \quad b^{(3)} := \prod_{i=a+1}^{c} g^{(i)},
\]

\[
h := \prod_{i=1}^{a} h^{(i)}, \quad \text{thus } h = b^{(1)} \cdot a^{(2)}.
\]

(2.22), (2.7) and (2.16) tell

\[
(a^{(3)}, b^{(3)}) = \mathbb{Z}[x] \quad \text{and} \quad (b^{(1)}, a^{(2)}) = \mathbb{Z}[x].
\]

The special case above tells

\[
(a^{(1)}, b^{(1)}) = (p, b^{(1)}) \quad \text{and} \quad (a^{(2)}, b^{(2)}) = (p, a^{(2)}).
\]

The product of the three ideals \((a^{(i)}, b^{(i)})\) for \( i = 1, 2, 3 \) is

\[
(a^{(1)}, b^{(1)}) \cdot (a^{(2)}, b^{(2)}) \cdot (a^{(3)}, b^{(3)})
\]

\[
= (a^{(1)}, b^{(1)}) \cdot (a^{(2)}, b^{(2)})
\]

\[
= (p, b^{(1)}) \cdot (p, a^{(2)}) = (p^2, p \cdot b^{(1)}, p \cdot a^{(2)}, h)
\]

\[
= (p, h) \quad \text{(this used } (b^{(1)}, a^{(2)}) = \mathbb{Z}[x]).
\]

The left hand side contains the ideal \((a^{(1)}a^{(2)}a^{(3)}, b^{(1)}b^{(2)}b^{(3)})\), thus

\[
(a^{(1)}a^{(2)}a^{(3)}, b^{(1)}b^{(2)}b^{(3)}) \subseteq (p, h).
\]

(2.25)

The special case above also tells

\[
|R(a^{(1)}, b^{(1)})| = p^{\deg b^{(1)}}, \quad |R(a^{(2)}, b^{(2)})| = p^{\deg a^{(2)}}.
\]

Together with (2.22) and (2.7) this implies

\[
|R(a^{(1)}a^{(2)}a^{(3)}, b^{(1)}b^{(2)}b^{(3)})| = p^{\deg b^{(1)}} \cdot p^{\deg a^{(2)}} = p^{\deg h}.
\]
with \(g = h\), \(n = \deg g = \deg h\) and \(m\) such that

\[
m + n = \sum_{i=1}^{3} (\deg a^{(i)} + \deg b^{(i)})
\]
shows

\[
\left| \frac{\mathbb{Z}[x]_{\leq m+n-1}}{(p, h) \cap \mathbb{Z}[x]_{\leq m+n-1}} \right| = p^{\deg h}.
\]

(2.27)

Comparison with (2.26) and (2.10) shows

\[
\left| \frac{\mathbb{Z}[x]_{\leq m+n-1}}{(p, h) \cap \mathbb{Z}[x]_{\leq m+n-1}} \right| = \left| \frac{\mathbb{Z}[x]_{\leq m+n-1}}{(a^{(1)}a^{(2)}a^{(3)}, b^{(1)}b^{(2)}b^{(3)}) \cap \mathbb{Z}[x]_{\leq m+n-1}} \right|
\]

(2.28)

Together with (2.25) this gives

\[
(p, h) = (a^{(1)}a^{(2)}a^{(3)}, b^{(1)}b^{(2)}b^{(3)}),
\]

which is (2.24).

\[\square\]

3. SOME TIE BETWEEN CYCLOTOMIC POLYNOMIALS

Recall from the notations 1.5 that \(\lambda\) denotes always a unit root in \(S^1 \subset \mathbb{C}\) and that its order is \(\text{ord}(\lambda) \in \mathbb{Z}_{\geq 1}\).

For \(m \in \mathbb{Z}_{\geq 1}\), the cyclotomic polynomial \(\Phi_m\) is the polynomial

\[
\Phi_m(x) := \prod_{\lambda: \text{ord} \lambda = m} (x - \lambda),
\]

(3.1)

whose zeros are the \(m\)-th primitive unit roots. It is a unitary and irreducible polynomial in \(\mathbb{Z}[x]\) of degree \(\deg \Phi_m = \varphi(m) \in \mathbb{Z}_{\geq 1}\), where \(\varphi : \mathbb{Z}_{\geq 1} \to \mathbb{Z}_{\geq 1}\) is the Euler phi-function (see e.g. [Wa82, Ch 1,2]).

Except for the irreducibility, this follows easily inductively from the formula

\[
x^m - 1 = \prod_{k|m} \Phi_k.
\]

(3.2)

Using this formula, one can compute the \(\Phi_k\) inductively. For example for \(p\) a prime number and \(k, m \in \mathbb{Z}_{\geq 1}\) with \(p \not| m\)

\[
\Phi_{pk+1m}(x) = \Phi_{pkm}(x^p) = \Phi_{pm}(x^{pk-1}) \quad \text{and} \quad \Phi_{pm}(x) = \frac{\Phi_{m}(x^p)}{\Phi_{m}(x)}.
\]

(3.3)

Recall (see e.g. [Wa82, Ch 1,2]) that \(\mathbb{Z}[e(\frac{1}{m})]\) is the ring of the algebraic integers within \(\mathbb{Q}[e(\frac{1}{m})]\) and that

\[
\mathbb{Z}[e(\frac{1}{m})] \cap S^1 = \{ \pm e(\frac{k}{m}) \mid k \in \mathbb{Z} \}.
\]

(3.4)
We will also use the norm

$$\text{Norm}_m : \mathbb{Z}[\epsilon(\frac{1}{m})] \rightarrow \mathbb{Z}, \quad g(\epsilon(\frac{1}{m})) \mapsto \prod_{\lambda: \text{ord}(\lambda) = m} g(\lambda). \quad (3.5)$$

An element of $\mathbb{Z}[\epsilon(\frac{1}{m})]$ has norm in $\{\pm 1\}$ if and only if it is a unit in $\mathbb{Z}[\epsilon(\frac{1}{m})]$.

Part (c) of the following theorem is the main result of [Ap70]. It gives the resultants of the cyclotomic polynomials. The proof here is much shorter than that in [Ap70].

**Theorem 3.1.**

(a) $\Phi_m(1) = 1$ if $m \geq 2$ and $m$ is not a power of a prime number. $\Phi_{pk}(1) = p$ if $p$ is a prime number and $k \in \mathbb{Z}_{\geq 1}$.

(b) $1 - \lambda$ is a unit in $\mathbb{Z}[\lambda]$ if and only if $\text{ord}(\lambda)$ is not a power of a prime number and not equal to 1.

(c) [Ap70] For $m, n \in \mathbb{Z}_{\geq 1}$,

$$R(\Phi_m, \Phi_n) = \begin{cases} 0 & \text{if } m = n, \\ 1 & \text{if neither } \frac{m}{n} \text{ nor } \frac{n}{m} \text{ is a power of a prime number}. \end{cases} \quad (3.6)$$

$$R(\Phi_{pk}, \Phi_n) = R(\Phi_n, \Phi_{pk}) = p^{\varphi(n)} \text{ if } p \text{ is a prime number and } k \in \mathbb{Z}_{\geq 1} \text{ and } (p, k, n) \neq (2, 1, 1). \quad (3.7)$$

$$R(1, 2) = -R(2, 1) = 2. \quad (3.8)$$

**Proof:** (a) If $p$ is a prime number and $k \in \mathbb{Z}_{\geq 1}$ then

$$\Phi_{pk}(x) = x^{(p-1)p^{k-1}} + x^{(p-2)p^{k-1}} + \ldots + x^{p^{k-1}} + 1, \quad (3.10)$$

so $\Phi_{pk}(1) = p$. \quad (3.11)

If one divides both sides of (3.2) by $\Phi_1 = (x - 1)$ and then puts $x = 1$, then one obtains

$$m = \prod_{k: k|m, k \neq 1} \Phi_k(1). \quad (3.12)$$

This and (3.11) and induction show $\Phi_m(1) = 1$ for any $m \in \mathbb{Z}_{\geq 2}$ which is not a power of a prime number.

(b) Let $\lambda$ be a unit root with order $\text{ord}(\lambda) = m$.

$$\text{Norm}_m(1 - \lambda) = \prod_{\mu: \text{ord}(\mu) = m} (1 - \mu) = \Phi_m(1). \quad (3.13)$$

This and part (a) show that $1 - \lambda$ is a unit in $\mathbb{Z}[\lambda]$ if and only if $m$ is not a power of a prime number and not equal to 1.
Lemma 3.2. Let \( p \) be a prime number, let \( m, n \in \mathbb{Z}_{\geq 1} \) with \( p \nmid m \), and let \( k, l_1, \ldots, l_r \in \mathbb{Z}_{\geq 0} \) with \( k > l_1 > \ldots > l_r \) for some \( r \in \mathbb{Z}_{\geq 1} \). Define
\[
f := \Phi_{p^k m}, \quad g := \Phi_{p^{l_1} m} \cdots \Phi_{p^{l_r} m}.
\]
Then \( f \) and \( g \) satisfy all properties (1)–(4) in lemma 2.4, especially \((f, g) = (p, g)\).

**Proof:** Because of lemma 2.4, it will be sufficient to show \( \deg f \geq \deg g \) and the properties (1) and (3) in lemma 2.4.

\( \deg f \geq \deg g \):

\[
\deg f = \varphi(p^km) = \varphi(p^k) \cdot \varphi(m) = (p - 1)p^{k-1} \cdot \varphi(m),
\]

\[
\deg g \leq \deg(\Phi_{p^{k-1}m} \cdot \Phi_{p^{k-2}m} \cdot \ldots \cdot \Phi_{p^m})
= ((p - 1)(p^{k-2} + p^{k-3} + \ldots + 1) + 1) \cdot \varphi(m)
= p^{k-1} \cdot \varphi(m) \leq \deg f.
\]

Property (1), \( |R(f, g)| = p^{\deg g} \): This uses (3.8) and possibly (3.9) (if \( p = 2 \) and \( m = 1 \)).

\[
|R(f, g)| = \prod_{i=1}^{r} |R(\Phi_{p^i}, \Phi_{p^i})| = \prod_{i=1}^{r} p^{\varphi(p^i)} = p^{\deg g}.
\]

Property (3), \( p \in (f, g) \): \( f \) divides

\[
\tilde{f} := \prod_{a|m} \Phi_{p^a} = \frac{x^{p^km} - 1}{x^{p^km} - 1} = x^{(p-1)p^{k-1}m} + x^{(p-2)p^{k-1}m} + \ldots + 1,
\]

and \( g \) divides

\[
\tilde{g} := \prod_{b|p^{k-1}m} \Phi_b = x^{p^{k-1}m} - 1,
\]

thus \((f, g) \supset (\tilde{f}, \tilde{g})\). Observe

\[
\tilde{f} \equiv p \mod (\tilde{g}),
\]

so \((p, \tilde{g}) = (\tilde{f}, \tilde{g}) \subset (f, g)\). This shows (3). \(\square\)

Lemma 3.3 will be used in the proof of theorem 3.4.

**Lemma 3.3.** (a) Let \( p \) be a prime number and \( k, m \in \mathbb{Z}_{\geq 1} \). Then

\[
\Phi_{p^km}(e^{\frac{1}{m}}) = p \cdot \text{unit}. \tag{3.15}
\]

Here and in the proof unit means an invertible element in \( \mathbb{Z}[\lambda] \) for a suitable unit root \( \lambda \).

(b) Let \( \lambda \) be a unit root and \( m = \text{ord}(\lambda) \) its order. The set \( \{\text{Norm}_m(1 - \lambda^k) \mid k \in \mathbb{Z}\} \) is the union of the set \( \{0\} \), the set

\[
\{p^{\varphi(p^l)} \mid l \geq 1 \text{ and } p \text{ a prime number such that } p^l \mid m\},
\]

and, if and only if \( m \) is not a power of a prime number, the set \( \{1\} \).
Proof: (a) If $p_i$ are different prime numbers and $k_i \geq 1$, then
\[
\Phi_{p_1^{k_1} \ldots p_t^{k_t}}(x) = \Phi_{p_1^{k_1} \ldots p_t^{k_t}}(x^{p_1^{k_1-1} \ldots p_t^{k_t-1}}).
\]
Hence (3.15) can be reduced to the statement
\[
\Phi_{p_1^{k_1} \ldots p_t^{k_t}}(e(\frac{1}{p_2 \ldots p_t})) = p_1 \cdot \text{unit}. \tag{3.16}
\]

If $p, q$ are prime numbers and if they and $m \in \mathbb{Z}_{\geq 1}$ are such that $p \neq q$ and $p$ and $q$ do not divide $m$, then
\[
\Phi_{pm}(e(\frac{1}{qm})) = \prod_{\text{ord}(\lambda) = pm} (e(\frac{1}{qm}) - \lambda) = e\left(\frac{\varphi(pm)}{qm}\right) \cdot \prod_{\text{ord}(\lambda) = pm} (1 - \lambda \cdot e(\frac{1}{qm}))
\]
is a unit, because the order $\text{ord}(\lambda \cdot e(\frac{1}{qm}))$ is not a power of a prime number. Using $\Phi_{pm}(x^q) = \Phi_{pm}(x) \cdot \Phi_{pm}(x^q)$, we get
\[
\Phi_{pm}(e(\frac{1}{qm})) = \Phi_{pm}(e(\frac{1}{m})) \cdot \text{unit}.
\]
Thus (3.17) can be reduced to the trivial case $\Phi_p(1) = p$.

(b) If $\text{ord}(\lambda^k)$ is not a power of a prime number, then $\text{Norm}_m(1 - \lambda^k) = 1$ because $\Phi_{\text{ord}(\lambda^k)}(1) = 1$. If $\text{ord}(\lambda^k) = p^l$ then
\[
\text{Norm}_m(1 - \lambda^k) = (\Phi_{p^l}(1))^\varphi(m) = p^{\varphi(m)}.
\]

Theorem 3.4 gives a tie between different cyclotomic polynomials. It will be crucial for the proof in section 5 of the sufficiency of the conditions in case (I) in theorem 1.2. It was stated before as lemma 6.5 in [He98].

**Theorem 3.4.** Let $p$ be a prime number, $k, m \in \mathbb{Z}_{\geq 1}$, $c(x) \in \mathbb{Z}[x]$ such that $c(e(\frac{1}{p^k m})) = 1$ and $|c(e(\frac{1}{m}))| = 1$.

(a) If $p \geq 3$ then $c(e(\frac{1}{m})) = 1$.
(b) If $p = 2$ then $c(e(\frac{1}{m})) = \pm 1$.
(c) If $p = 2$ and $c(e(\frac{1}{p^k m})) = 1$ for some $l \neq k$ then $c(e(\frac{1}{m})) = 1$.

**Proof:** (a) Let $p, k, m, c(x)$ be as in the theorem, with $p \geq 3$. There exists a polynomial $r(x) \in \mathbb{Z}[x]$ such that $1 - c(x) = \Phi_{p^k m}(x) \cdot r(x)$. Then
\[
\text{Norm}_m(1 - c(e(\frac{1}{m}))) = \text{Norm}_m(\Phi_{p^k m}(e(\frac{1}{m}))) \cdot \text{Norm}_m(r(e(\frac{1}{m}))) = (\pm 1) \cdot p^{\varphi(m)} \cdot \text{Norm}_m(r(e(\frac{1}{m}))).
\]
The second equality uses lemma 3.3 (a). From (3.1) and $|c(e(\frac{1}{m}))| = 1$ we obtain
\[ c(e(\frac{1}{m})) \in \{\pm e(\frac{1}{m}) \mid l \in \mathbb{Z}\}. \]

**Case 1**, $m$ is odd: Then $\mathbb{Z}[e(\frac{1}{m})] = \mathbb{Z}[e(\frac{1}{2m})]$, $\text{Norm}_m = \text{Norm}_{2m}$,
\[ \{\pm e(\frac{1}{m}) \mid l \in \mathbb{Z}\} = \{e(\frac{1}{m}) \mid l \in \mathbb{Z}\} \]. Because of lemma 3.3 (b) and
\[ \varphi(p') > 1 \text{ for } l \geq 1, \text{ the only number in } \{\text{Norm}_m(1 - e(\frac{1}{2m})) \mid l \in \mathbb{Z}\}, \]
which is divisible by $p^{\varphi(m)(2m)} = p^{\varphi(m)}$, is 0. Thus $\text{Norm}_m(1 - c(e(\frac{1}{m}))) = 0$
and $c(e(\frac{1}{m})) = 1$. This proves part (a).

(b) Let $p, k, m, c(x)$ be as in the theorem, with $p = 2$. The proof proceeds as the proof of part (a). Only the statement $\varphi(p') > 1$ becomes
wrong if $l = 1$. Then $\text{Norm}_m(1 - e(\frac{1}{2m})) = 2^{\varphi(m)}$ in case 1 respectively
\[ \text{Norm}_m(1 - e(\frac{1}{m})) = 2^{\varphi(m)} \text{ in case 2 is possible, but only in the case } e(\frac{1}{m}) = -1 \text{ in case 1 respectively } e(\frac{1}{m}) = -1 \text{ in case 2, as the proof of lemma 3.3 (b) shows.} \]

(c) Let $p, k, m, c(x)$ be as in the theorem, with $p = 2$ and $c(e(\frac{1}{p'm})) = 1$ for some $l \neq k$. There exists a polynomial $r(x) \in \mathbb{Z}[x]$ such that
\[ 1 - c(x) = \Phi_{p^k}m(x) \cdot \Phi_{p've}(x) \cdot r(x). \]
Then
\[ \text{Norm}_m(1 - c(e(\frac{1}{m}))) = \text{Norm}_m(\Phi_{p^k}m(e(\frac{1}{m}))) \cdot \text{Norm}_m(\Phi_{p've}(e(\frac{1}{m}))) \cdot \text{Norm}_m(r(e(\frac{1}{m}))) \]
\[ = (\pm 1) \cdot p^{\varphi(m)} \cdot (\pm 1) \cdot p^{\varphi(m)} \cdot \text{Norm}_m(r(e(\frac{1}{m}))). \]
The last equality uses lemma 3.3 (a). Now one has again to go through the two cases and apply lemma 3.3 (b). As $2^{\varphi(m)}$ is bigger than
\[ \varphi(m)/\varphi(p') \text{ in any case, } \text{Norm}_m(1 - c(e(\frac{1}{m}))) = 0 \text{ and } c(e(\frac{1}{m})) = 1. \]

4. Necessity of the conditions in the main result in the connected case

Let $(H_M, h_M, S)$ be a triple as in the introduction and let $M$ be the set of orders of the eigenvalues of $h_M$. The main point in this section is the
Thus commutativity of the triple $(\mathcal{H}, \mathcal{M}, S)$ in the next lemma shows that the precise form of the bilinear form $S$ in $\text{Aut}((M, h_M, S))$ is unimportant. Recall that $\prod_{m \in M} \Phi_m$ is the characteristic polynomial of $h_M$ and that $(\prod_{m \in M} \Phi_m)$ denotes its ideal in $\mathbb{Z}[x]$.

**Lemma 4.1.**

\[
\text{End}(H_M, h_M) = \{c(h_M) \mid c(x) \in \mathbb{Z}[x]\}, \quad (4.1)
\]
\[
\text{Aut}(H_M, h_M, S) = \{c(h_M) \mid c(x) \in \mathbb{Z}[x] \text{ with } |c(\lambda)| = 1 \text{ for any eigenvalue } \lambda \text{ of } h_M\}, \quad (4.2)
\]

Thus
\[
\text{Aut}(H_M, h_M, S) = \{\pm h_M^k \mid k \in \mathbb{Z}\} \iff \{c(x) \in \mathbb{Z}[x] \mid |c(\lambda)| = 1 \text{ for any eigenvalue } \lambda \text{ of } M\} = \{\pm x^k \mid k \in \mathbb{Z}\} + (\prod_{m \in M} \Phi_m). \quad (4.3)
\]

**Proof:** Due to (1.7), for any $B \in \text{End}(H_M, h_M)$ a unique polynomial $b(x) = \sum_{i=0}^{n-1} b_i x^i \in \mathbb{Z}[x]$ with $B(e_1) = \sum_{i=0}^{n-1} b_i h_M^i(e_1)$ exists. The commutativity $h_M \circ B = B \circ h_M$ implies $B = b(h_M)$. This proves (4.1).

Any eigenspace $H_\lambda$ of $h_M$ is 1-dimensional by hypothesis. Two eigenspaces $H_\lambda$ and $H_\mu$ are orthogonal with respect to $S$ if $\mu \neq \overline{\lambda}$, because $S$ is $h_M$-invariant. By hypothesis, the restriction of $S : H_\lambda \times H_{\overline{\lambda}} \rightarrow \mathbb{C}$ is nondegenerate if $\lambda \notin \{\pm 1\}$.

Now consider an automorphism $b(h_M) \in \text{Aut}(H_M, h_M, S)$ for some $b(x) \in \mathbb{Z}[x]$. The space $H_\lambda$ is also an eigenspace of $b(h_M)$, and it has eigenvalue $b(\lambda)$ on $H_\lambda$. As $b(h_M)$ is an automorphism of $H_M$, its eigenvalue on $H_1$ if $H_1 \neq \{0\}$ and its eigenvalue on $H_{-1}$ if $H_{-1} \neq \{0\}$ must be in $\{\pm 1\}$. It respects $S$ on $\bigoplus_{\lambda \neq \pm 1} H_\lambda$ if and only if $|b(\lambda)| = 1$ for any eigenvalue $\lambda \neq \pm 1$. Therefore $|b(\lambda)| = 1$ for any eigenvalue.

Vice versa, suppose that $b(h_M) \in \text{End}(H_M, h_M)$ for some $b(x) \in \mathbb{Z}[x]$ with $|b(\lambda)| = 1$ for any eigenvalue $\lambda$ of $h_M$. Then $b(h_M)$ respects $S$, and $\text{det } b(h_M) \in \{\pm 1\}$, and thus $b(h_M) \in \text{Aut}(H_M, h_M, S)$. This completes the proof of (4.2).

(4.3) is an immediate consequence of (4.2). \(\square\)

Suppose now that $\mathcal{G}(M)$ is connected. We will show $\exists \mathcal{G}$ in (4.3) if $(T_p)$ does not hold for some prime number $p \geq 3$ (1st case) or if $(S_2)$ does not hold (2nd case).

**1st case**, $(T_p)$ does not hold for some prime number $p \geq 3$: Let $E_1, \ldots, E_r$ with $r \geq 2$ be the highest $p$-planes. Let $F_1 \subset M$ be the union
of all \( p \)-planes which can be reached within the graph \( \mathcal{G}(M)^{(p)} \) (whose vertices are all the \( p \)-planes in \( \mathcal{G}(M) \), see remark 1(iii)) by starting at \( E_1 \) and following some directed edges. Let \( F_2 \) be the union of all \( p \)-planes which can be reached within the graph \( \mathcal{G}(M)^{(p)} \) by starting at one of the points \( E_2, \ldots, E_r \) and following some directed edges. As \( E_1, \ldots, E_r \) are all highest \( p \)-planes, \( F_1 \cup F_2 = M \). As \( \mathcal{G}(M) \) is connected, \( F_1 \cap F_2 \neq \emptyset \). Define

\[
G_1 := F_1 - F_1 \cap F_2, \quad G_2 := F_2 - F_1 \cap F_2, \quad G_3 := F_1 \cap F_2,
\]
so that \( G_1 \cup G_2 \cup G_3 = M \). Also

\[
(F_1 \cap F_2) \cap E_1 = \emptyset \quad \text{and} \quad (F_1 \cap F_2) \cap (E_2 \cup \ldots \cup E_r) = \emptyset
\]
are obvious, and they imply

\[
\begin{align*}
l(G_3, p) &< l(E_1, p) = l(F_1, p) = l(G_1, p), \quad \text{(4.4)} \\
l(G_3, p) &< l(E_2 \cup \ldots \cup E_r, p) = l(F_2, p) = l(G_2, p).
\end{align*}
\]

By definition of \( G_1 \) and \( G_2 \), there are no edges at all between vertices in \( G_1 \) and vertices in \( G_2 \). With (3.7) and (2.7), the resultant of the following polynomials is in \( \{\pm 1\} \),

\[
R( \prod_{m \in G_1} \Phi_m, \prod_{m \in G_2} \Phi_m ) = \pm 1.
\]

By (2.16), there exist \( a_1, a_2 \in \mathbb{Z}[x] \) with

\[
1 = a_1 \cdot \prod_{m \in G_1} \Phi_m + a_2 \cdot \prod_{m \in G_2} \Phi_m.
\]

Write \( d := \text{lcm}(G_3) \) (so that \( l(G_3, p) = l(d, p) \)). Then

\[
x^d - 1 = a_1 \cdot (x^d - 1) \cdot \prod_{m \in G_1} \Phi_m + a_2 \cdot (x^d - 1) \cdot \prod_{m \in G_2} \Phi_m
\]

\[
= b_1 \cdot \prod_{m \in G_1 \cup G_3} \Phi_m + b_2 \cdot \prod_{m \in G_2 \cup G_3} \Phi_m
\]

for some \( b_1, b_2 \in \mathbb{Z}[x] \). Define

\[
c(x) := x^d - b_1 \cdot \prod_{m \in G_1 \cup G_3} \Phi_m = 1 + b_2 \cdot \prod_{m \in G_2 \cup G_3} \Phi_m \in \mathbb{Z}[x]. \quad \text{(4.5)}
\]

We want to show that there do not exist \( \varepsilon \in \{\pm 1\} \) and \( k \in \mathbb{Z}_{\geq 0} \) with

\[
c(x) \equiv \varepsilon \cdot x^k \mod ( \prod_{m \in M} \Phi_m ). \quad \text{(4.6)}
\]
We suppose that $\varepsilon \in \{\pm 1\}$ and $k \in \mathbb{Z}$ with (4.6) exist. We want to arrive at a contradiction. (4.5) and (4.6) give

$$e\left(\frac{d}{m}\right) = c\left(e\left(\frac{1}{m}\right)\right) = \varepsilon \cdot e\left(\frac{k}{m}\right) \quad \text{for } m \in G_1 \cup G_3,$$

$$1 = c\left(e\left(\frac{1}{m}\right)\right) = \varepsilon \cdot e\left(\frac{k}{m}\right) \quad \text{for } m \in G_2 \cup G_3,$$

thus

$$d \equiv \frac{m}{2} \cdot \delta_{-1,\varepsilon} + k \mod m\mathbb{Z} \quad \text{for } m \in G_1 \cup G_3,$$

$$0 \equiv \frac{m}{2} \cdot \delta_{-1,\varepsilon} + k \mod m\mathbb{Z} \quad \text{for } m \in G_2 \cup G_3.$$

If $\varepsilon = -1$ this shows that $m \in G_1 \cup G_2 \cup G_3$ is even. Recall $m = \prod_{q \text{ prime number}} q^{l(m,q)}$. In any case, whether $\varepsilon = -1$ or $\varepsilon = 1$,

$$d \equiv k \mod p^{l(m,p)}\mathbb{Z} \quad \text{for } m \in G_1 \cup G_3,$$

$$0 \equiv k \mod p^{l(m,p)}\mathbb{Z} \quad \text{for } m \in G_2 \cup G_3,$$

as $p \geq 3$, so

$$d \equiv k \mod p^{l(G_1,p)}\mathbb{Z}$$

$$0 \equiv k \mod p^{l(G_2,p)}\mathbb{Z}$$

As $l(G_1,p) > l(G_3,p) = l(d,p)$ and $l(G_2,p) > l(G_3,p)$ by (4.4),

$$d \equiv k \equiv 0 \mod p^{l(d,p)+1}.$$

But this is impossible, as it contradicts the definition of $l(d,p)$. Therefore $\varepsilon \in \{\pm 1\}$ and $k \in \mathbb{Z}$ with (4.6) do not exist. Thus $c(h_M) \notin \{\pm h_M^k \mid k \in \mathbb{Z}\}$. On the other hand, (4.5) and lemma 4.1 tell $c(h_M) \in \text{Aut}(H_M,h_M,S)$. This proves the necessity of $(T_p)$ for $p \geq 3$ in theorem 1.2 in the case when $G(M)$ is connected.

2nd case, $(S_2)$ does not hold: Let $E_1, \ldots, E_r$ with $r \geq 3$ be the components of the graph $(M, E(M) - \{\text{highest 2-edges}\})$. As $G(M)$ has at least one highest 2-plane, by remark 1.3 (iv) we can suppose that $E_1$ is a highest 2-plane and that $l(E_1, 2) = l(M, 2)$. As $G(M)$ is connected, we can also suppose that $E_2$ is a component such that there exists a highest 2-edge from a vertex in $E_1$ to a vertex in $E_2$. Define $F_1 := E_1 \cup E_2 \neq \emptyset$ and $F_2 := E_3 \cup \ldots \cup E_r \neq \emptyset$. Then $M = F_1 \cup F_2$. Consider for any odd $a \in \mathbb{Z}_{\geq 1}$ the sets

$$B_a := \{2^k a \mid k \in \mathbb{Z}_{\geq 0}\}, \quad B_{1,a} := B_a \cap F_1, \quad B_{2,a} := B_a \cap F_2.$$
The construction of \( E_1, \ldots, E_r \) and of \( F_1 \) and \( F_2 \) tells
\[
B_{1,a} \neq \emptyset \quad \text{and} \quad B_{2,a} \neq \emptyset
\]
\[
\Rightarrow \left\{ \begin{array}{l}
\text{either } B_{1,a} = \{m_1\} \quad \text{and} \quad m_1 > m \forall m \in B_{2,a} \quad (4.7) \\
\text{or } B_{2,a} = \{m_1\} \quad \text{and} \quad m_1 > m \forall m \in B_{1,a}.
\end{array} \right.
\]
Define
\[
A_{12} := \{ a \in \mathbb{Z}_{\geq 1} \mid \text{a odd, } B_{1,a} \neq \emptyset, B_{2,a} \neq \emptyset \}, \\
A_1 := \{ a \in \mathbb{Z}_{\geq 1} \mid \text{a odd, } B_{1,a} \neq \emptyset, B_{2,a} = \emptyset \}, \\
A_2 := \{ a \in \mathbb{Z}_{\geq 1} \mid \text{a odd, } B_{1,a} = \emptyset, B_{2,a} \neq \emptyset \}.
\]
Define
\[
f_a := \prod_{m \in B_{1,a}} \Phi_m \quad \text{for } a \in A_{12} \cup A_1, \\
g_a := \prod_{m \in B_{2,a}} \Phi_m \quad \text{for } a \in A_{12} \cup A_2.
\]
If \( a \in A_{12} \), then either the pair \((f_a, g_a)\) or the pair \((g_a, f_a)\) satisfies the properties of the pair \((f, g)\) in lemma 3.2 with \( p = 2 \), because of (4.7). Furthermore, observe that the sets of vertices \( F_1 \) and \( F_2 \) are connected only by some highest 2-edges and not by any other edges. This implies \(|R(f_1, g_2)| = 1\) for \( a_1 \neq a_2 \) by (3.7). Therefore the polynomials \( f_a, a \in A_{12} \cup A_1 \), and the polynomials \( g_a, a \in A_{12} \cup A_2 \), satisfy all properties of the polynomials \( f^{(1)}, \ldots, f^{(a+b)}, g^{(1)}, \ldots, g^{(a+c)} \) in lemma 2.5 with the obvious differences in the notations. (2.24) in lemma 2.5 tells that there exist polynomials \( b_1, b_2 \in \mathbb{Z}[x] \) with
\[
2 = b_1 \cdot \prod_{a \in A_{12} \cup A_1} f_a + b_2 \cdot \prod_{a \in A_{12} \cup A_2} g_a
\]
\[
= b_1 \cdot \prod_{m \in F_1} \Phi_m + b_2 \cdot \prod_{m \in F_2} \Phi_m.
\]
Now define
\[
c(x) := 1 - b_1 \cdot \prod_{m \in F_1} \Phi_m = -1 + b_2 \cdot \prod_{m \in F_2} \Phi_m, \quad (4.8)
\]
The rest of the argument is similar to the 1st case. We want to show that there do not exist \( \varepsilon \in \{ \pm 1 \} \) and \( k \in \mathbb{Z}_{\geq 0} \) with
\[
c(x) \equiv \varepsilon \cdot x^k \mod (\prod_{m \in M} \Phi_m), \quad (4.9)
\]
We suppose that $\varepsilon \in \{\pm 1\}$ and $k \in \mathbb{Z}$ with (4.9) exist. We want to arrive at a contradiction. (4.8) and (4.9) give
\[ 1 = c(e(\frac{1}{m})) = \varepsilon \cdot e(\frac{k}{m}) \quad \text{for } m \in F_1, \]
\[ -1 = c(e(\frac{1}{m})) = \varepsilon \cdot e(\frac{k}{m}) \quad \text{for } m \in F_2, \]
thus
\[ 0 \equiv \frac{m}{2} \cdot \delta_{-1,\varepsilon} + k \mod m\mathbb{Z} \quad \text{for } m \in F_1, \]
\[ \frac{m}{2} \equiv \frac{m}{2} \cdot \delta_{-1,\varepsilon} + k \mod m\mathbb{Z} \quad \text{for } m \in F_2. \]
If $\varepsilon = -1$ then any $m \in F_1$ is even so $l(m, 2) \geq 1$. In any case, whether $\varepsilon = -1$ or $\varepsilon = 1$,
\[ 0 \equiv 2^{l(m,2)-1} \cdot \delta_{-1,\varepsilon} + k \mod 2^{l(m,2)}\mathbb{Z} \quad \text{for } m \in F_1. \quad (4.10) \]
Observe that $F_1$ contains elements $m_1 \in E_1$ and $m_2 \in E_2$ with $l(m_1, 2) > l(m_2, 2)$ as there is a highest 2-edge from $E_1$ to $E_2$. This and (4.10) show $\varepsilon = 1$. Now
\[ 0 \equiv k \mod 2^{l(m,2)}\mathbb{Z} \quad \text{for } m \in F_1, \]
\[ 2^{l(m,2)-1} \equiv k \mod 2^{l(m,2)}\mathbb{Z} \quad \text{for } m \in F_2 \]
follows. With $l(F_1, 2) = l(M, 2)$, the first congruence says $2^{l(M,2)}|k$, the second congruence contradicts this, a contradiction. Therefore $\varepsilon \notin \{\pm 1\}$ and $k \in \mathbb{Z}$ with (4.9) do not exist. One concludes as in the 1st case. $(S_2)$ is necessary in theorem 1.2 in the case when $G(M)$ is connected.

5. **Sufficiency of the conditions in the main result in the connected case**

The aim of this section is to show that the conditions in case (I) in theorem 1.2 are sufficient for (1.6) if $G(M)$ is connected. Let $(H_M, h_M, S)$ be a triple as in the introduction and let $M$ be the set of orders of $h_M$. Suppose that $G(M)$ is connected and satisfies $(S_2)$ and $(T_p)$ for any prime number $p \geq 3$. Let $c(x) \in \mathbb{Z}[x]$ be a polynomial with $|c(\lambda)| = 1$ for any eigenvalue $\lambda$ of $h_M$. We want to show that $\varepsilon \in \{\pm 1\}$ and $k \in \mathbb{Z}_{\geq 0}$ with
\[ c(x) \equiv \varepsilon \cdot x^k \mod \left( \prod_{m \in M} \Phi_m \right). \quad (5.1) \]
exist. With lemma 4.1 this implies (1.6).
First, a sign $\alpha(m) \in \{\pm 1\}$ and a number $a(m) \in \{0, 1, ..., m-1\}$ are associated to any $m \in M$ by requiring

\[ c(e(\frac{1}{m})) = \alpha(m) \cdot e\left(\frac{a(m)}{m}\right) \quad (5.2) \]

and additionally $\alpha(m) = 1$ if $m$ is even. (5.3)

They exist and are unique by (3.4).

Now we have to apply theorem 3.4 in order to link the pairs $(\alpha(m), a(m))$ for different $m$ and for varying prime numbers $p$. This will prepare the choice of $\varepsilon \in \{\pm 1\}$ and $k \in \mathbb{Z}$ such that (5.1) holds.

We consider the same cases as in theorem 3.4. Lemma 5.1 is a straightforward application of it.

**Lemma 5.1.** (a) Let $p \geq 3$ be a prime number. Suppose that a $p$-edge goes from $m_1 \in M$ to $m_2 \in M$. Then

\[ \alpha(m_1) = \alpha(m_2), \quad (5.4) \]
\[ a(m_1) \equiv a(m_2) \mod m_2\mathbb{Z}. \quad (5.5) \]

(b) Suppose that a 2-edge goes from $m_1 \in M$ to $m_2 \in M$. Then $\alpha(m_1) = 1$ (by definition) and

\[ a(m_1) \equiv \frac{m_2}{2} \cdot \delta_{-1, \beta(m_1, m_2)} + a(m_2) \mod m_2\mathbb{Z} \quad (5.6) \]

for some $\beta(m_1, m_2) \in \{\pm 1\}$ if $m_2$ is even,

\[ a(m_1) \equiv a(m_2) \mod m_2\mathbb{Z} \quad \text{if} \ m_2 \text{ is odd}. \quad (5.7) \]

(c) Let $m_1, m_2, m_3 \in M$ be such that a 2-edge goes from $m_1$ to $m_2$ and a 2-edge goes from $m_2$ to $m_3$. Then $\alpha(m_1) = \alpha(m_2) = 1$ (by definition) and

\[ \beta(m_1, m_2) = \beta(m_1, m_3) = \beta(m_2, m_3) \quad \text{if} \ m_3 \text{ is even}, \quad (5.8) \]
\[ \beta(m_1, m_2) = \alpha(m_3) \quad \text{if} \ m_3 \text{ is odd}. \quad (5.9) \]

**Proof:** (a) Define

\[ c_2(x) := \alpha(m_1) \cdot x^{m_1 - a(m_1)} \cdot c(x) \in \mathbb{Z}[x]. \]

Then

\[ c_2\left(\frac{1}{m_1}\right) = 1, \]
\[ c_2\left(\frac{1}{m_2}\right) = \alpha(m_1)\alpha(m_2) \cdot e\left(\frac{-a(m_1) + a(m_2)}{m_2}\right) = 1 \quad \text{(by theorem 3.4 (a))}. \]
If $m_1$ and $m_2$ are even then $\alpha(m_1) = \alpha(m_2) = 1$ by definition. If $m_1$ and $m_2$ are odd then $\alpha(m_1)\alpha(m_2) = 1$ because $-1 \notin \{e(\frac{k}{m_2}) \mid k \in \mathbb{Z}\}$. In any case (5.4) and (5.5) hold.

(b) $m_1$ is even, thus $\alpha(m_1) = 1$. Define

$$c_3(x) := x^{m_1-a(m_1)} \cdot c(x) \in \mathbb{Z}[x].$$

Then

$$c_3(e(\frac{1}{m_1})) = 1,$$

$$c_3(e(\frac{1}{m_2})) = \alpha(m_2) \cdot e(-a(m_1) + a(m_2)) = \beta \quad \text{for some } \beta \in \{\pm 1\} \quad \text{(by theorem 3.4 (b)).}$$

If $m_2$ is even, then $\alpha(m_2) = 1$ and

$$a(m_1) \equiv \frac{m_2}{2} \cdot \delta_{-1,\beta} + a(m_2) \mod m_2\mathbb{Z}.$$ If $m_2$ is odd, then $\alpha(m_2) = \beta$ because $-1 \notin \{e(\frac{k}{m_2}) \mid k \in \mathbb{Z}\}$, and then

$$a(m_1) \equiv a(m_2) \mod m_2\mathbb{Z}.$$ (c) $m_1$ and $m_2$ are even, thus $\alpha(m_1) = \alpha(m_2) = 1$. Define

$$c_4(x) := \beta(m_1, m_2) \cdot x^{7+\beta(m_1,m_2)-m_1/4-a(m_1)} \cdot c(x).$$

Then

$$c_4(e(\frac{1}{m_1})) = 1,$$

$$c_4(e(\frac{1}{m_2})) = \beta(m_1, m_2) \cdot e(-a(m_1) + a(m_2)) = 1 \quad \text{(by 5.6),}$$

$$c_4(e(\frac{1}{m_3})) = \beta(m_1, m_2)\alpha(m_3) \cdot e(-a(m_1) + a(m_3))$$

$$= 1 \quad \text{(by theorem 3.4 (c)).}$$

If $m_3$ is even then $\alpha(m_3) = 1$ and (5.6) for $m_1$ and $m_3$ gives $\beta(m_1, m_2) = \beta(m_1, m_3)$. If $m_3$ is odd then (5.7) for $m_1$ and $m_3$ gives $\beta(m_1, m_2) = \alpha(m_3)$.

As $m_3|m_2$, (5.6) also says $a(m_1) \equiv a(m_2) \mod m_3\mathbb{Z}$. This shows $\beta(m_1, m_3) = \beta(m_2, m_3)$ if $m_3$ is even. \hfill \Box

**Corollary 5.2.** Let $p$ and $q$ be prime numbers with $q \geq 3$ (here $p = q$ as well as $p \neq q$ are possible). Suppose that a $p$-edge goes from $m_1 \in M$
to \( m_2 \in M \). Then

\[
\begin{align*}
(a(m_1)) & \equiv a(m_2) \mod q^{l(m_2, q)}Z, & (5.10) \\
(a(m_1)) & \equiv a(m_2) \mod 2^{l(m_2, 2)}Z \quad \text{if } p \geq 3, & (5.11) \\
(a(m_1)) & \equiv a(m_2) \mod 2^{l(m_2, 2)}Z \quad \text{if } p = 2 \text{ and } m_2 \text{ is odd}, (5.12) \\
(a(m_1)) & \equiv 2^{l(m_2, 2) - 1} \cdot \delta_{-1, b(m_1, m_2)} + a(m_2) \mod 2^{l(m_2, 2)}Z & (5.13)
\end{align*}
\]

\[ \text{if } p = 2 \text{ and } m_2 \text{ is even.} \]

**Proof:** If \( p \geq 3 \) (5.10) and (5.11) follow from (5.5). If \( p = 2 \) (5.10) follows from (5.6) and (5.7). (5.12) follows from (5.7). (5.13) follows from (5.6). \( \square \)

By hypothesis, \( G(M) \) is connected and satisfies \( (S_2) \) and \( (T_p) \) for any prime number \( p \geq 3 \). Therefore \( (M, E(M) - \{ \text{highest 2-edges} \}) \) has either 1 or 2 components. \( (S_2) \) and remark 1.3 (iv) say about the two cases the following.

**Case (1),** there is only 1 component \( M \): It is a single 2-plane. Then choose \( m_1^{(2)} \in M \) arbitrary.

**Case (2),** there are 2 components: One of them is the unique highest 2-plane \( E_1 \), and the other component \( E_2 \) satisfies \( l(E_2, 2) < l(E_1, 2) \). Furthermore, there is a highest 2-edge from a vertex \( m_1^{(2)} \in E_1 \) to a vertex \( m_2^{(2)} \in E_2 \). Observe also that \( l(m_1^{(2)}, 2) = l(E_1, 2) = l(M, 2) \) as \( l(m, 2) \) is constant for all vertices \( m \) within one 2-plane.

In both cases, choose for any prime number \( q \geq 3 \) a vertex \( m_1^{(q)} \) in the unique highest \( q \)-plane. Then \( l(m_1^{(q)}, q) = l(M, q) \). Now we define candidates \( \varepsilon \) and \( k \) which shall satisfy (5.1). Define

\[
\varepsilon := \begin{cases} 
\alpha(m_1^{(2)}) & \in \{\pm 1\} \quad \text{in case (1)}, \\
\beta(m_1^{(2)}, m_2^{(2)}) & \in \{\pm 1\} \quad \text{in case (2) if } m_2^{(2)} \text{ is even}, (5.14) \\
\alpha(m_2^{(2)}) & \in \{\pm 1\} \quad \text{in case (2) if } m_2^{(2)} \text{ is odd},
\end{cases}
\]

\[
k \in \mathbb{Z}_{\geq 0} \quad \text{such that}
\]

\[
k \equiv a(m_1^{(q)}) \mod q^{l(M, q)} \quad \text{for any prime number } q \geq 3, \quad (5.15)
\]

\[
k \equiv \begin{cases} 
\alpha(m_1^{(2)}) \mod 2^{l(M, 2)} \quad & \text{in case (1)}, \\
2^{l(M, 2) - 1} \cdot \delta_{-1, \varepsilon} + a(m_1^{(2)}) \mod 2^{l(M, 2)} \quad & \text{in case (2)}, (5.16)
\end{cases}
\]

Here observe that for any prime number \( p \) \( l(m_1^{(p)}, p) = l(M, p) \) because \( m_1^{(p)} \) is in the unique highest \( p \)-plane. \( k \in \mathbb{Z} \) can be chosen as in (5.15) and (5.16) because of the Chinese remainder theorem. We want to show that these \( \varepsilon \) and \( k \) satisfy (5.1).
**Case (1):** Then $M$ is a single 2-plane, there are no 2-edges, and $l(m, 2) = l(M, 2)$ for any $m \in M$. As $G(M)$ is connected, (5.16) and (5.11) imply
\[
k \equiv a(m) \mod 2^{l(m, 2)} \quad \text{for any } m \in M.
\] (5.17)
As $G(M)$ is connected, (5.14) and (5.1) imply
\[
\epsilon = \alpha(m) \quad \text{for any } m \in M.
\] (5.18)
Let $q \geq 3$ be a prime number. As $G(M)$ is connected and satisfies $(T_q)$ (compare the remarks 1.3 (ii) and (iii)), (5.15) and (5.10) imply
\[
k \equiv a(m) \mod q^{l(m, q)} \quad \text{for any } m \in M.
\] (5.19)
Together (5.17) and (5.19) give
\[
k \equiv a(m) \mod m \quad \text{for any } m \in M.
\] (5.20)
Together (5.18) and (5.20) and (5.2) say
\[
c(e\left(\frac{1}{m}\right)) = \epsilon \cdot e\left(\frac{k}{m}\right). \quad \text{for any } m \in M.
\] (5.21)
This implies (5.1).

**Case (2):** As $G(M)$ is connected and satisfies $(T_q)$ for any prime number $q \geq 3$ (compare the remarks 1.3 (ii) and (iii)), (5.15) and (5.10) imply for any prime number $q \geq 3$
\[
k \equiv a(m) \mod q^{l(m, q)} \quad \text{for any } m \in M.
\] (5.22)
Below we will show inductively
\[
k \equiv 2^{l(m, 2) - 1} \cdot \delta_{-1, \epsilon} + a(m) \mod 2^{l(m, 2)} \quad \text{for even } m \in M,
\] (5.23)
\[
\left\{ \begin{array}{l}
k \equiv a(m) \mod 2^{l(m, 2)} \\
\epsilon = \alpha(m)
\end{array} \right\} \quad \text{for odd } m \in M.
\] (5.24)
Together (5.22), (5.23) and (5.24) give
\[
k \equiv \frac{m}{2} \cdot \delta_{-1, \epsilon} + a(m) \mod m \quad \text{for even } m \in M,
\] (5.25)
\[
\left\{ \begin{array}{l}
k \equiv a(m) \mod m \\
\epsilon = \alpha(m)
\end{array} \right\} \quad \text{for odd } m \in M.
\] (5.26)
Together (5.25), (5.26) and (5.2) say
\[
c(e\left(\frac{1}{m}\right)) = \epsilon \cdot e\left(\frac{k}{m}\right). \quad \text{for any } m \in M.
\] (5.27)
This implies (5.1).
Therefore it rests for the proof in case (2) to show (5.23) and (5.24). The proof of (5.23) and (5.24) will consist of two inductions. The first induction will show the following slightly weaker statements:

\[ k \equiv 2^{l(m, 2) - 1} \cdot \delta_{-1, \gamma(m)} + a(m) \mod 2^{l(m, 2)} \] for even \( m \), (5.28)

\[ k \equiv a(m) \mod 2^{l(m, 2)} \] for odd \( m \in M \), (5.29)

with a unique \( \gamma(m) \in \{ \pm 1 \} \) for even \( m \in M \). The second induction will show \( \gamma(m) = \varepsilon \) for even \( m \in M \) and \( \alpha(m) = \varepsilon \) for odd \( m \in M \). This and (5.28) and (5.29) give (5.23) and (5.24).

The first induction: \((S_2)\) and \( G(M) \) connected imply \((T_2)\), see remark 1.3 (iv). Therefore starting at \( m_1^{(2)} \), one can reach any \( m \in M \) going through a chain of edges, in correct direction through 2-edges and in any direction through \( p \)-edges for \( p \geq 3 \). \( m_1^{(2)} \) satisfies (5.28) with \( \gamma(m_1^{(2)}) = \varepsilon \) by (5.16).

If a \( p \)-edge for some \( p \geq 3 \) goes from \( m_1 \) to \( m_2 \) and one of them satisfies (5.28) or (5.29), then the other satisfies (5.28) or (5.29) too, and \( \gamma(m_1) = \gamma(m_2) \). This follows from (5.11) and \( l(m_1, 2) = l(m_2, 2) \).

If a 2-edge goes from \( m_1 \) to \( m_2 \) and \( m_1 \) satisfies (5.28), then \( m_2 \) satisfies (5.29) if \( m_2 \) is odd, because of (5.12). It satisfies (5.28) with \( \gamma(m_2) = \beta(m_1, m_2) \) if \( m_2 \) is even, because of (5.13).

This finishes the inductive proof of (5.28) and (5.29), and it gives some additional information on \( \gamma(m) \): All elements \( m \) in one 2-plane have the same value \( \gamma(m) \) if they are even. If \( m_2 \) is even and is at the end of a 2-edge which starts at \( m_1 \) then \( \gamma(m_2) = \beta(m_1, m_2) \).

The second induction: We saw already \( \gamma(m_1^{(2)}) = \varepsilon \). Therefore \( \gamma(m) = \varepsilon \) for all \( m \) in the 2-plane \( E_1 \). (5.14) gives \( \varepsilon = \beta(m_1^{(2)}, m_2^{(2)}) = \gamma(m_2^{(2)}) \) if \( m_2^{(2)} \) is even and \( \varepsilon = \alpha(m_2^{(2)}) \) if \( m_2^{(2)} \) is odd. \((S_2)\) says that all 2-planes in \( E_2 \) are connected by 2-edges which are not highest 2-edges. If there is a 2-edge from \( m_1 \) to \( m_2 \) and a 2-edge from \( m_2 \) to \( m_3 \) then (5.8) and (5.9) show:

If \( m_3 \) is even: \( \gamma(m_2) = \varepsilon \iff \gamma(m_3) = \varepsilon \).

If \( m_3 \) is odd: \( \gamma(m_2) = \varepsilon \iff \alpha(m_3) = \varepsilon \).

Therefore \( \gamma(m) = \varepsilon \) for all even \( m \in M \) and \( \alpha(m) = \varepsilon \) for all odd \( m \in M \). This finishes the second induction and the proof of (5.23) and (5.24) and the discussion of case (2). \( \square \)
6. The proof of the main result in the disconnected case

The aim of this section is to prove theorem 1.2 in the case when \( G(M) \) is not connected. But before, we consider a more general situation and state a lemma.

For any unitary polynomial \( f \in \mathbb{C}[x] \) of degree \( \deg f \geq 1 \), let

\[
H_f := \frac{\mathbb{Z}[x]}{(f)} \cong \mathbb{Z}^{\deg f} \quad (6.1)
\]

\[
h_f := \text{multiplication by } x : H_f \to H_f.
\]

Then \((H_f,h_f)\) is a \( \mathbb{Z} \)-lattice \( H_f \) of rank \( \deg f \) with a cyclic automorphism \( h_f \), i.e.

\[
H_f = \bigoplus_{i=0}^{n-1} \mathbb{Z} \cdot h_f^i(e_1) \quad (6.2)
\]

for some \( e_1 \in H_f \). In fact, here one can choose \( e_1 = 1 \).

Part (b) of the following lemma is a kind of chinese remainder theorem for such pairs.

**Lemma 6.1.** Let \( f, g \in \mathbb{Z}[x] \) be unitary polynomials of degrees \( \geq 1 \).

(a) \( H_{fg} \) contains a unique primitive sublattice which is \( h_{fg} \)-invariant and such that the characteristic polynomial of \( h_{fg} \) on it is \( f \). It is \( (g)/(fg) \subset H_{fg} \), and \( (\mathbb{Z}/(fg), h_{fg}) \cong (H_f, h_f) \).

(b) \( (H_{fg}, h_{fg}) \cong (H_f, h_f) \times (H_g, h_g) \iff |R(f, g)| = 1. \quad (6.3) \)

If this holds then

\[
\text{Aut}(H_{fg}, h_{fg}) \cong \text{Aut}(H_f, h_f) \times \text{Aut}(H_g, h_g). \quad (6.4)
\]

**Proof:** (a) Over \( \mathbb{Q} \) instead of \( \mathbb{Z} \), the equality

\[
(\ker f(h_{fg}) : H_{fg} \otimes \mathbb{Z} \mathbb{Q} \to H_{fg} \otimes \mathbb{Z} \mathbb{Q}) = (g)/(fg) \otimes \mathbb{Z} \mathbb{Q}
\]

is obvious. Of course, there is a unique primitive sublattice \( U \) of \( H_{fg} \) with \( U \otimes \mathbb{Z} \mathbb{Q} = (g)/(fg) \otimes \mathbb{Z} \mathbb{Q} \). It is \( U = ((g)/(fg) \otimes \mathbb{Z} \mathbb{Q}) \cap H_{fg} \).

Consider the isomorphism of \( \mathbb{Z} \)-lattices

\[
\Phi : \mathbb{Z}[x]_{\leq \deg(fg)-1} \to H_{fg}, \quad a(x) \mapsto a(x) \mod (fg). \quad (6.5)
\]

Then \( \Phi^{-1}((g)/(fg)) = \mathbb{Z}[x]_{\leq \deg f-1} \cdot g \) is a primitive sublattice of \( \mathbb{Z}[x]_{\leq \deg(fg)-1} \), as

\[
\mathbb{Z}[x]_{\leq \deg(fg)-1} = \mathbb{Z}[x]_{\leq \deg f-1} \cdot g \oplus \mathbb{Z}[x]_{\leq \deg g-1}.
\]

Therefore \( (g)/(fg) \) is a primitive sublattice of \( H_{fg} \). The monodromy \( h_{fg} \) on it is cyclic with generator \( g \mod (fg) \). This shows the isomorphism \( ((g)/(fg), h_{fg}) \cong (H_f, h_f) \).
(b) In \((H_f, h_f) \times (H_g, h_g) = (H_f \times H_g, h_f \times h_g), (H_f, h_f)\) and \((H_g, h_g)\) are primitive \(h_f \times h_g\)-invariant sublattices such that the characteristic polynomial of \(h_f \times h_g\) on them is \(f\) respectively \(g\). Together they generate the full \(\mathbb{Z}\)-lattice \(H_f \times H_g\).

In \((H_{fg}, h_{fg})\), the sum of the primitive sublattices \((g) / (fg)\) and \((f) / (fg)\) is \((f, g) / (fg)\) and \((f) / (fg)\). It is a sublattice of \(H_{fg}\) of full rank \(\text{deg}(fg)\) if and only if \(R(f, g) \neq 0\) by lemma \(2.3\) (b). Then it is a direct sum of the sublattices \((g) / (fg)\) and \((f) / (fg)\), and then it is of index \(|R(f, g)|\) in \(H_{fg}\) by \(2.10\).

Therefore \((H_{fg}, h_{fg}) \cong (H_f \times H_g, h_f \times h_g)\) if and only if \(|R(f, g)| = 1\).

\((6.4)\) is an immediate consequence of \((6.3)\). \(\square\)

Now we return to the situation in section 1. The following elementary observations will be useful.

**Remarks 6.2.** Let \(M \subset \mathbb{Z}_{\geq 1}\) be a finite set of positive integers. Let \((H_M, h_M, S)\) be a triple as in section 1 such that \(M\) is the set of orders of the eigenvalues of \(h_M\).

\(-\text{id} \in \{h_M^k \mid k \in \mathbb{Z}\} \iff \exists l \in \mathbb{Z}_{\geq 1} \text{ mit } \forall m \in M \ l(m, 2) = l. \ (6.6)\)

\(|\{\pm h_M^k \mid k \in \mathbb{Z}\}| = \begin{cases} \text{lcm}(M) & \text{if } \exists l \in \mathbb{Z}_{\geq 1} \text{ mit } \forall m \in M \ l(m, 2) = l, \\ 2 \text{lcm}(M) & \text{else}. \end{cases} \ (6.7)\)

**Necessity of the conditions in case (II) in theorem 1.2.** Let \(M \subset \mathbb{Z}_{\geq 1}\) be a finite set of positive integers, and let \((H_M, h_M, S)\) be a triple as in section 1 such that \(M\) is the set of orders of the eigenvalues of \(h_M\). Suppose that \(\mathcal{G}(M)\) is not connected and that \(\text{Aut}(H_M, h_M, S) = \{\pm h_M^k \mid k \in \mathbb{Z}\}\). We will show that all conditions in case (II) in theorem 1.2 hold.

Let \(M_1, ..., M_r\) with \(r \geq 2\) be the components of \(\mathcal{G}(M)\). Define

\[ f_j := \prod_{m \in M_j} \Phi_m \quad \text{for } j = 1, ..., r. \]

As there are no edges between different components, \((3.6)\) gives for the resultants

\[ |(R(f_i, f_j)| = 1 \quad \text{for } i \neq j, \]

\[ |R(f_1, \prod_{j \geq 2} f_j)| = 1, \ |R(f_2, \prod_{j \geq 3} f_j)| = 1, ..., \ |R(f_{r-1}, f_r)| = 1. \]

One applies \(r - 1\) times lemma 6.1 and obtains

\((H_M, h_M) \cong (H_{M_1}, h_{M_1}) \times ... \times (H_{M_r}, h_{M_r})\).
As all eigenspaces are one-dimensional and $S$ is $h_M$-invariant, it is clear that $S$ and the automorphisms decompose accordingly,

$$(H_M, h_M, S) \cong (H_{M_1}, h_{M_1}, S_1) \times \ldots \times (H_{M_r}, h_{M_r}, S_r),$$

$\text{Aut}(H_M, h_M, S) \cong \text{Aut}(H_{M_1}, h_{M_1}, S_1) \times \ldots \times \text{Aut}(H_{M_r}, h_{M_r}, S_r).$

Recall

$$\text{Aut}(H_M, h_M, S) = \{ \pm h_M^k \mid k \in \mathbb{Z} \} \text{ by hypothesis,}$$

$$\text{Aut}(H_{M_j}, h_{M_j}, S_j) \supset \{ \pm h_{M_j}^k \mid k \in \mathbb{Z} \},$$

$$|\{ \pm h_{M_j}^k \mid k \in \mathbb{Z} \}| = \begin{cases} \text{lcm}(M_j) & \text{if } (*) \text{ holds,} \\ 2\text{lcm}(M_j) & \text{else,} \end{cases}$$

$$(*) \quad \iff \exists l_j \in \mathbb{Z}_{\geq 1} \text{ with } \forall m \in M_j \ l(m, 2) = l_j,$$

$$\iff M_j \text{ is a 2-plane with } l(M_j, 2) \geq 1.$$

The last equivalence holds because $M_j$ is a connected subgraph of $G(M)$.

**First case,** $\exists l \in \mathbb{Z}_{\geq 1}$ with $\forall m \in M \ l(m, 2) = l$: Then all $M_j$ are 2-planes with $l(M_j, 2) = l \geq 1$, so $(*)$ holds. Thus

$$|\text{Aut}(H_M, h_M, S)| = \text{lcm}(M) = \text{lcm}(\text{lcm}(M_1), \ldots, \text{lcm}(M_r)),$$

$$|\text{Aut}(H_{M_j}, h_{M_j}, S_j)| \geq |\{ \pm h_{M_j}^k \mid k \in \mathbb{Z} \}| = \text{lcm}(M_j),$$

$$\text{lcm}(\text{lcm}(M_1), \ldots, \text{lcm}(M_r)) \geq \prod_{j=1}^r \text{lcm}(M_j).$$

But $2|\text{lcm}(M_j)$ for all $j$. This is a contradiction. The first case is impossible.

**Second case,** $\not\exists l \in \mathbb{Z}_{\geq 1}$ with $\forall m \in M \ l(m, 2) = l$: Then

$$|\text{Aut}(H_M, h_M, S)| = 2\text{lcm}(M)$$

$$= 2\text{lcm}(\text{lcm}(M_1), \ldots, \text{lcm}(M_r)),$$

$$|\text{Aut}(H_{M_j}, h_{M_j}, S_j)| \geq \begin{cases} \text{lcm}(M_j) & \text{if } (*) \text{ holds,} \\ 2\text{lcm}(M_j) & \text{else,} \end{cases}$$

$$2\text{lcm}(\text{lcm}(M_1), \ldots, \text{lcm}(M_r)) \geq \prod_{j=1}^r \begin{cases} \text{lcm}(M_j) & \text{if } (*) \text{ holds} \\ 2\text{lcm}(M_j) & \text{else} \end{cases}.$$
In case (ii) \( \gcd(\text{lcm}(M_i), \text{lcm}(M_j)) = 1 \) for all pairs \((i, j)\) with \(i < j\) except for one pair which may satisfy \( \gcd(\text{lcm}(M_i), \text{lcm}(M_j)) = 2 \). This also implies \( r = 2 \). \( M_1 \) and \( M_2 \) are 2-planes with \( \ell(M_1, 2) \geq 1 \) and \( \gcd(\text{lcm}(M_i), \text{lcm}(M_j)) = 2 \). As we are in the second case, \( \ell(M_1, 2) \neq \ell(M_2, 2) \). We can suppose \( \ell(M_1, 2) > \ell(M_2, 2) = 1 \).

In case (i) as well as in case (ii), the inequalities above are equalities, and thus

\[
|\text{Aut}(H_M, h_M, S)| = |\{ \pm h_M^k \mid k \in \mathbb{Z} \}|
\]

and thus \( \text{Aut}(H_M, h_M, S) = \{ \pm h_M^k \mid k \in \mathbb{Z} \} \). Case (I) in theorem 1.2 says that the graphs \( \mathcal{G}(M_1) \) and \( \mathcal{G}(M_2) \) satisfy \((T_p)\) for any prime number \( p \geq 3 \). This completes the proof of the necessity of the conditions in case (II) in theorem 1.2.

**Sufficiency of the conditions in case (II) in theorem 1.2.** Let \( M \subset \mathbb{Z}_{\geq 1} \) be a finite set of positive integers, and let \((H_M, h_M, S)\) be a triple as in section 1 such that \( M \) is the set of orders of the eigenvalues of \( h_M \). Suppose that \( \mathcal{G}(M) \) has two components \( M_1 \) and \( M_2 \) whose graphs are 2-planes and satisfy \((T_p)\) for any prime number \( p \geq 3 \). Suppose also (1.7) and (1.8), which are

\[
\gcd(\text{lcm}(M_1), \text{lcm}(M_2)) \in \{1; 2\},
\]

\[
\ell(M_1, 2) > \ell(M_2, 2) \in \{0; 1\}.
\]

We want to show \( \text{Aut}(H_M, h_M, S) = \{ \pm h_M^k \mid k \in \mathbb{Z} \} \).

As there are no edges between \( M_1 \) and \( M_2 \) in the graph \( \mathcal{G}(M) \),

\[
|R(\prod_{m \in M_1} \Phi_m, \prod_{m \in M_2} \Phi_m)| = 1.
\]

Lemma 6.1 applies and says

\[
(H_M, h_M) \cong (H_{M_1}, h_{M_1}) \times (H_{M_2}, h_{M_2}).
\]

As all eigenspaces are one-dimensional and \( S \) is \( h_M \)-invariant, \( S \) and the automorphisms decompose accordingly,

\[
(H_M, h_M, S) \cong (H_{M_1}, h_{M_1}, S_1) \times (H_{M_2}, h_{M_2}, S_2),
\]

\[
\text{Aut}(H_M, h_M, S) \cong \text{Aut}(H_{M_1}, h_{M_1}, S_1) \times \text{Aut}(H_{M_2}, h_{M_2}, S_2).
\]

As \( \mathcal{G}(M_1) \) and \( \mathcal{G}(M_2) \) satisfy \((T_p)\) for any prime number \( p \geq 3 \), case (I) of theorem 1.2 applies and gives

\[
\text{Aut}(H_{M_i}, h_{M_i}, S_i) = \{ \pm h_{M_i}^k \mid k \in \mathbb{Z} \} \quad \text{for} \ i = 1, 2.
\]
$M_1$ and $M_2$ are 2-planes with $l(M_1, 2) \geq 1$ and $l(M_2, 2) \in \{0; 1\}$, thus

$$|\text{Aut}(H_{M_1}, h_{M_1}, S_1)| = \text{lcm}(M_1),$$

$$|\text{Aut}(H_{M_2}, h_{M_2}, S_2)| = \begin{cases} 
\text{lcm}(M_1) & \text{if } l(M_2, 2) = 1, \\
2\text{lcm}(M_1) & \text{if } l(M_2, 2) = 0.
\end{cases}$$

Therefore

$$|\text{Aut}(H_{M}, h_{M}, S)| = |\text{Aut}(H_{M_1}, h_{M_1}, S_1)| \cdot |\text{Aut}(H_{M_2}, h_{M_2}, S_2)|$$

$$= \begin{cases} 
\text{lcm}(M_1) \cdot \text{lcm}(M_2) & \text{if } l(M_2, 2) = 1, \\
\text{lcm}(M_1) \cdot 2\text{lcm}(M_2) & \text{if } l(M_2, 2) = 0,
\end{cases}$$

$$= 2 \cdot \text{lcm}(M) = |\{\pm h_M^k | k \in \mathbb{Z}\}|,$$

thus

$$\text{Aut}(H_{M}, h_{M}, S) = \{\pm h_M^k | k \in \mathbb{Z}\}.$$

\[\square\]

References

[Ap70] T. Apostol: Resultants of cyclotomic polynomials. Proc. A.M.S. 24 (1970), 457–462.
[GH16] F. Gauß, C. Hertling: $\mu$-constant monodromy groups and Torelli results for marked singularities, for the unimodal and some bimodal singularities. In: Singularities and Computer Algebra, Festschrift for Gert-Martin Greuel on the Occasion of his 70th Birthday (W. Decker, G. Pfister, M. Schulze, eds.). Springer International Publishing 2017, 109-146.
[GH17] F. Gauß, C. Hertling: $\mu$-constant monodromy groups and Torelli results for the quadrangle singularities and the bimodal series. arXiv:1710.03507v1, 125 pages, 10.10.2017.
[He98] C. Hertling: Brieskorn lattices and Torelli type theorems for cubics in $\mathbb{P}^3$ and for Brieskorn-Pham singularities with coprime exponents. In: Singularities, the Brieskorn anniversary volume. Progress in Mathematics 162. Birkhäuser Verlag, Basel-Boston-Berlin 1998, pp. 167–194.
[He11] C. Hertling: $\mu$-constant monodromy groups and marked singularities. Ann. Inst. Fourier, Grenoble 61.7 (2011), 2643–2680.
[HZ18] C. Hertling, Ph. Zilke: Seven combinatorial problems around quasihomogeneous singularities. Manuskript, January 2018, 36 pages.
[Or72] P. Orlik: On the homology of weighted homogeneous polynomials. In: Lecture Notes in Math. 298, Springer, Berlin, 1972.
[vW71] B.L. van der Waerden: Algebra I, Springer, Berlin, Heidelberg, New York, 8. Auflage, 1971.
[Wa82] L.C. Washington: Introduction to cyclotomic fields. Springer, New York, 1982.

Claus Hertling, Universität Mannheim, Lehrstuhl für Mathematik VI, Seminargebäude A 5, 6, 68131 Mannheim, Germany
E-mail address: hertling@math.uni-mannheim.de