การแยกตัวประกอบของนัยทั่วไปของพหุนามชี้กำลังบางประเภท

นางสาวเอื้อมพร ฟักสุวรรณ

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาคณิตศาสตร์ ภาควิชาคณิตศาสตร์
คณะวิทยาศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2545

ISBN 974-17-2238-9

FACTORIZATIONS OF SOME GENERALIZED EXPONENTIAL POLYNOMIALS

Miss Ouamporn Phuksuwan

A Thesis Submitted in Partial Fulfillment of the Requirements

for the Degree of Master of Science in Mathematics

Department of Mathematics

Faculty of Science

Chulalongkorn University

Academic Year 2002

ISBN 974-17-2238-9

Thesis Title	Factorizations of some generalized exponential polynomials
By	Miss Ouamporn Phuksuwan
Field of study	Mathematics
Thesis Advisor	Assistant Professor Patanee Udomkavanich, Ph.D.
Thesis Co-advisor	Associate Professor Vichian Laohakosol, Ph.D.

Accepted by the Faculty of Science, Chulalongkorn University in Partial Fulfillment of the Requirements for the Master's Degree

……………………………………………………Dean of Faculty of Science

(Associate Professor Wanchai Phothiphichitr, Ph.D.)

Thesis Committee

……………………………………………………Chairman

(Assistant Professor Ajchara Harnchoowong, Ph.D.)

……………………………………………………Thesis Advisor

(Assistant Professor Patanee Udomkavanich, Ph.D.)

……………………………………………………Thesis Co-advisor

(Associate Professor Vichian Laohakosol, Ph.D.)

……………………………………………………Member

(Nataphan Kitisin, Ph.D.)

……………………………………………………Member

(Phichet Chaoha, Ph.D.)

เอื้อมพร ฟักสุวรรณ : การแยกตัวประกอบของนัยทั่วไปของพหุนามชี้กำลังบางประเภท
(FACTORIZATIONS OF SOME GENERALIZED EXPONENTIAL POLYNOMIALS)
อ. ที่ปรึกษา : ผศ.ดร. พัฒนี อุดมกะวานิช อ. ที่ปรึกษาร่วม : รศ.ดร. วิเชียร เลาหโกศล,
33 หน้า ISBN 974-17-2238-9

ในปี ค.ศ. 1927 Ritt ได้พิสูจน์ว่าผลบวกชี้กำลังเชิงซ้อนสามารถแยกตัวประกอบเป็นผลคูณของส่วนที่ลดทอนไม่ได้และส่วนที่เป็นเชิงเดียวได้เพียงแบบเดียวเท่านั้น ส่วนแรกของวิทยานิพนธ์นี้เป็นการขยายเซตสามเซตซึ่งเกี่ยวข้องในทฤษฎีบทแยกตัวประกอบของ Ritt กล่าวคือสัมประสิทธิ์ ตัวชี้กำลังและฟังก์ชันชี้กำลัง ทั้งนี้โดยการวิเคราะห์บทพิสูจน์ดั้งเดิมของ Ritt

ทฤษฎีบทของ Skolem-Mahler-Lech กล่าวไว้ว่า ถ้าพหุนามชี้กำลังมีรากจำนวนเต็มเป็นจำนวนอนันต์ แล้วรากเหล่านั้นเกือบทั้งหมดยกเว้นเพียงจำกัดตัว จัดได้ในรูปผลผนวกจำกัดของการก้าวหน้าเลขคณิต ในปี ค.ศ. 1959 Shapiro ได้ใช้ผลอันนี้ในการแยกตัวประกอบของพหุนามชี้กำลังดังกล่าว เมื่อให้ตัวชี้กำลังของพหุนามชี้กำลังเป็นพหุนามที่มีสัมประสิทธ์เป็นจำนวนเต็ม ทฤษฎีบทของ Skolem-Mahler-Lech ยังเป็นจริงสำหรับคลาสย่อยบางคลาสของเซตนี้ ในส่วนที่สองของวิทยานิพนธ์นี้เป็นการพิสูจน์ทฤษฎีบทการแยกตัวประกอบของสมาชิกในคลาสย่อยนี้โดยนัยเดียวกับผลของ Shapiro

ภาควิชา **คณิตศาสตร์** ลายมือชื่อนิสิต...
สาขาวิชา **คณิตศาสตร์** ลายมือชื่ออาจารย์ที่ปรึกษา......................................
ปีการศึกษา 2545 ลายมือชื่ออาจารย์ที่ปรึกษาร่วม…………………………

4472514623 : MAJOR MATHEMATICS

KEY WORDS : EXPONENTIAL SUMS, EXPONENTIAL POLYNOMIALS, FACTORIZATION

OUAMPORN PHUKSUWAN : FACTORIZATIONS OF SOME GENERALIZED EXPONENTIAL POLYNOMIALS THESIS ADVISOR : ASSISTANT PROFESSOR PATANEE UDOMKAVANICH, Ph.D. THESIS CO-ADVISOR : ASSOCIATE PROFESSOR VICHIAN LAOHAKOSOL, Ph.D. , 33 pp. ISBN 974-17-2238-9

In 1927, Ritt proved that a complex exponential sum can be uniquely factored as a product of irreducible and simple parts. The first part of this thesis deals with the problem of enlarging the three possible sets of elements involved in Ritt's factorization theorem, namely, coefficients, exponents and exponential function. This is done by analyzing Ritt's original proof.

The Skolem-Mahler-Lech Theorem states that if an exponential polynomial has infinitely many integer zeros, then all but finitely many such zeros form a finite union of arithmetic progressions. Based on this result, Shapiro in 1959, established a factorization theorem for such exponential polynomials. Allowing the exponents in the exponential polynomial to be integer polynomials, the Skolem-Mahler-Lech Theorem still holds for a certain subclass of this set. In the second part of this thesis, a factorization theorem, in the spirit of Shapiro's result, is proved for some elements of this subclass.

Department **Mathematics**	Student's signature......................................
Field of study **Mathematics**	Advisor's signature......................................
Academic year **2002**	Co-advisor's signature………………………..

ACKNOWLEDGEMENTS

A large number of people have assisted in preparing and writing of this thesis either directly or indirectly. First, I am deeply indebted to Assistant Professor Patanee Udomkavanich and Associate Professor Vichian Laohakosol, my thesis advisors for their advice and encouragement. I would also like to thank Assistant Professor Ajchara Harnchoowong, Dr. Nataphan Kitisin and Dr. Phichet Chaoha, my thesis committee for their valuable comments.

I also thank all teachers who have taught me all along. Finally, I would like to express my gratitude towards my family and friends for their continual support.

CONTENTS

CHAPTER I

Ritt's factorization theorem

A (complex) exponential sum is an expression of the form

$$a_0e^{\alpha_0 z} + a_1e^{\alpha_1 z} + ... + a_ne^{\alpha_n z}, \quad a_i, \alpha_i \in \mathbb{C}.$$

Equip a lexicographical ordering ,<, to $\mathbb{C}$. In order to factor such exponential sum, it suffices to factor a normalized exponential sum, i.e an expression of the shape

$$1 + a_1e^{\alpha_1 z} + ... + a_ne^{\alpha_n z},$$

where the exponents are so arranged that $0 < \alpha_1 < ... < \alpha_n$. A (normalized) exponential sum is said to be simple if each α_i is a multiple of some fixed complex number, termed index. Clearly, a simple exponential sum can be factored in infinitely many ways, and for factorization purposes, it is enough to group them into parts with different irrational index ratios. Ritt's factorization theorem of 1927 essentially states that any normalized exponential sum can be uniquely written as a product of simple and irreducible exponential sums, where the simple exponential sums have pairwise irrational index ratio, and the irreducible ones are non-simple and not capable of being decomposed further.

In this chapter, the coefficients, exponents and exponential function involved in Ritt's factorization are studied in order to determine enlarged structures validating Ritt's theorem.

1.1 Definitions

Definition 1.1.1. A **Ritt space** $(\mathcal{R}, \theta_r)$, or simply $\mathcal{R}$, is an $\mathbb{R}$-vector space with a countable basis $\{\theta_r\} = \{\theta_1, \theta_2, ...\}$, and a lexicographical order defined by $\alpha = r_1\theta_1 + ... + r_t\theta_t < \beta = s_1\theta_1 + ... + s_t\theta_t$ $(r_i, s_j \in \mathbb{R})$ if and only if there is a positive integer $n \leq t$ such that $r_1 = s_1, ..., r_{n-1} = s_{n-1}$ but $r_n < s_n$.
Define $\overline{0} = 0\theta_1 + 0\theta_2 + ... + 0\theta_n \in \mathcal{R}$ for all n. Clearly, $\overline{0}$ is the zero element of the Ritt space $\mathcal{R}$.

Proposition 1.1.2. Let $\mathcal{R}$ be a Ritt space. Then

(i) For $\alpha \in \mathcal{R}$ and $r \in \mathbb{R}$, if $\alpha > \overline{0}$ and $r > 0$, then $r \cdot \alpha > \overline{0}$.

(ii) For $\alpha, \beta, \gamma, \delta \in \mathcal{R}$, if $\alpha < \beta$ and $\gamma < \delta$, then $\alpha + \gamma < \beta + \delta$.

(iii) For $\alpha, \beta \in \mathcal{R}$, if $\alpha > \overline{0}$ and $\beta > \overline{0}$, then $\alpha + \beta > \overline{0}$.

Proof. Clear. □

Let $\mathcal{R}$ be a Ritt space. Denote by f a function whose domain is the set $\mathcal{R}x = \{\alpha x \mid \alpha \in \mathcal{R}\}$, where x is an indeterminate, satisfying $f(\alpha_1 x)f(\alpha_2 x) = f((\alpha_1 + \alpha_2)x)$.

Definition 1.1.3. Let $\mathbb{F}$ be an algebraically closed field with characteristic zero and $\mathcal{R}$ a Ritt space. A **Ritt exponential sum**, abbreviated by RES, is an expression of the shape

$$a_0 f(\alpha_0 x) + a_1 f(\alpha_1 x) + ... + a_n f(\alpha_n x),$$

where $a_i \in \mathbb{F}$, $\alpha_i \in \mathcal{R}$ and $\alpha_0 < \alpha_1 < ... < \alpha_n$. The α_i's will be referred to as **RE-coefficients**.

Over the set of RES's, we impose

(i) an equality relation by the condition that
$\sum_{i=0}^{n} a_i f(\alpha_i x) = \sum_{i=0}^{n} b_i f(\beta_i x)$ if and only if $a_i = b_i$ and $\alpha_i = \beta_i$ for all i and

(ii) an algebraic independence condition stating that $f(\alpha_1 x), ..., f(\alpha_n x)$ are algebraically independent over $\mathbb{F}$ whenever $\alpha_1, ..., \alpha_n \in \mathcal{R}$ are linearly independent over $\mathbb{Q}$.

Denote the set of RES's imposed with such conditions by $\mathcal{E}$.

Define addition and multiplication on $\mathcal{E}$ as follows :

For any $E_1(x) = \sum_{i=0}^{n} a_i f(\alpha_i x)$ and $E_2(x) = \sum_{i=0}^{n} b_i f(\alpha_i x)$,

$$E_1(x) + E_2(x) = \sum_{i=0}^{n} (a_i + b_i) f(\alpha_i x), \text{ and}$$

$$E_1(x) \cdot E_2(x) = \sum_{i=0}^{n} \sum_{j=0}^{n} a_i b_j f((\alpha_i + \alpha_j)x).$$

It is easy to verify that, under the operations defined above, $\mathcal{E}$ is a ring with multiplicative identity $f(\bar{0}x)$, indeed $\mathcal{E}$ is an integral domain. The multiplicative inverse of $f(\alpha x)$ is $f(-\alpha x)$, while the additive inverse is $-f(\alpha x)$. Any RES of the form $a_0 f(\bar{0}x)$ is called a **constant Ritt exponential sum**. The constant RES's add and multiply as in $\mathbb{F}$ and so form a subring of $\mathcal{E}$ isomorphic to $\mathbb{F}$. We then identify $\mathbb{F}$ as the set of constant RES's in $\mathcal{E}$. Sometimes, we refer to $\mathcal{E}$ as a **Ritt domain** with respect to $\mathbb{F}$ and $\mathcal{R}$.

It can be proved by induction that $(f(\alpha x))^n = f(n\alpha x)$ for all $n \in \mathbb{N}$ and it follows that $(f(\alpha x))^q = f(q\alpha x)$ for all $q \in \mathbb{Q}_0^+$.

Definition 1.1.4. A nonconstant element $E(x) = \sum_{i=0}^{n} a_i f(\alpha_i x)$ of a Ritt domain $\mathcal{E}$ with respect to $\mathbb{F}$ and $\mathcal{R}$ is said to be **simple** if there exists $\lambda \in \mathcal{R}$ such that for all i, $\alpha_i = k_i \lambda$ where $k_i \in \mathbb{Z}$, equivalently, a simple RES is an RES of the form $E(x) = \sum_{i=0}^{n} a_i f(k_i \lambda x)$ where $k_i \in \mathbb{Z}$. We refer to λ as an **s-index** of the simple RES $E(x)$.

Definition 1.1.5. A nonconstant element $E(x)$ of a Ritt domain $\mathcal{E}$ with respect to $\mathbb{F}$ and $\mathcal{R}$ is said to be **irreducible** if it can not be factored as a product of other RES except 1 and itself.

Remarks.

(i) It follows immediately from the definition that in any Ritt domain $\mathcal{E}$ with respect to $\mathbb{F}$ and $\mathcal{R}$, the RES $a + bf(\beta x)$ is simple for all $a, b \in \mathbb{F}$ and $\beta \in \mathcal{R}$.

(ii) In any Ritt domain $\mathcal{E}$, the class of simple RES's and the class of irreducible RES's are disjoint.

1.2 Finding base

Throughout this section, let $\mathcal{E}$ be a Ritt domain with respect to an algebraically closed field $\mathbb{F}$ and a Ritt space $(\mathcal{R}, \theta_r)$. We will factor RES of the form $1 + a_1 f(\alpha_1 x) + ... + a_n f(\alpha_n x)$ with $\overline{0} < \alpha_1 < ... < \alpha_n$. As the proof is long and complicated, we will first prove those lemmas needed.

A subset $\{m_1, ..., m_p\}$ of $\mathcal{R}$ is said to be **$\mathbb{Q}$-linearly independent** if whenever $\sum_{i=1}^{p} q_i m_i = 0$ for rational numbers $q_1, ..., q_p$, then $q_1 = ... = q_p = 0$. A **$\mathbb{Q}$-base** for $\{\alpha_1, ..., \alpha_n\} \subseteq \mathcal{R}$ is a $\mathbb{Q}$-linearly independent subset of $\mathcal{R}$ which spans $\{\alpha_1, ..., \alpha_n\}$. A $\mathbb{Q}$-linearly independent subset $\{\mu_1, ..., \mu_p\}$ of $\mathcal{R}$ is called a **$\mathbb{Q}^+$-base** for $\{\alpha_1, ..., \alpha_n\}$ if each α_i can be written as a $\mathbb{Q}^+$-linearly combination of μ_i's, i.e. $\alpha_i = \sum_{j=1}^{p} q_{ij} \mu_j$, where $q_{ij} \in \mathbb{Q}^+$.

Definition 1.2.1. An $\alpha = r_1\theta_1 + ... + r_n\theta_n \in \mathcal{R}$ is said to be **strictly positive** if $r_1 > 0$.

The next lemma gives a sufficient condition when a subset $\{\alpha_1, ..., \alpha_n\}$ of $\mathcal{R}$ has a $\mathbb{Q}^+$-base.

Lemma 1.2.2. Let $\{\alpha_1, ..., \alpha_n\} \subseteq \mathcal{R}$. If $\overline{0} < \alpha_1 < ... < \alpha_n$ and α_1 is strictly positive, then there exists a $\mathbb{Q}^+$-base $\{\mu_1, ..., \mu_p\}$ for $\{\alpha_1, ..., \alpha_n\}$.

Proof. Let $\{m_1, ..., m_p\}$ be the largest $\mathbb{Q}$-linearly independent subset of $\{\alpha_1, ..., \alpha_n\}$. For each i, let $\alpha_i = \sum_{k=1}^{p} q_{ik} m_k$, where $q_{ik} \in \mathbb{Q}$. We can also write

$m_j = \sum_k r_{jk}\theta_k$, where $r_{jk} \in \mathbb{R}$. Define a linear map $\varphi : \mathbb{R}^p \to \mathbb{R}^n$ by $\varphi(X) = QX$ for all $X \in \mathbb{R}^p$, where Q is the matrix $(q_{ij})_{n\times p}$. Since α_1 is strictly positive, all entries of $\varphi((r_{11}, ..., r_{p1}))$ are positive. By the continuity of φ and the denseness of $\mathbb{Q}$ in $\mathbb{R}$, for each $i = 1, ..., p$, there is $(t_{1i}, ..., t_{pi}) \in \mathbb{Q}^p$ such that all entries of $\varphi((t_{1i}, ..., t_{pi}))$ are positive and the matrix $(t_{ij})_{p\times p}$ has a nonzero determinant. Hence the system of linear equations

$$\begin{aligned} m_1 &= t_{11}x_1 + t_{12}x_2 + ... + t_{1p}x_p \\ m_2 &= t_{21}x_1 + t_{22}x_2 + ... + t_{2p}x_p \\ &\vdots \\ m_p &= t_{p1}x_1 + t_{p2}x_2 + ... + t_{pp}x_p \end{aligned}$$

has a unique solution, say $\mu_1, ..., \mu_p$. Consequently, each α_i is a $\mathbb{Q}^+$-linear combination of the μ_i's as desired.

It remains to show that $\{\mu_1, ..., \mu_p\}$ is $\mathbb{Q}$-linearly independent. Suppose on the contrary that there exist rational numbers $s_1, ..., s_p$, not all zero, such that

$$s_1\mu_1 + s_2\mu_2 + ... + s_p\mu_p = \overline{0}. \tag{1}$$

The system

$$\begin{aligned} t_{11}x_1 + t_{21}x_2 + ... + t_{p1}x_p &= s_1 \\ t_{12}x_1 + t_{22}x_2 + ... + t_{p2}x_p &= s_2 \\ &\vdots \\ t_{1p}x_1 + t_{2p}x_2 + ... + t_{pp}x_p &= s_p, \end{aligned}$$

then has a nontrivial solution, say $v_1, ..., v_p$. Substituting $s_i = t_{1i}v_1 + t_{2i}v_2 + ... + t_{pi}v_p$ in (1), it follows that $\sum_i v_i m_i = 0$, which contradicts the $\mathbb{Q}$-independence of $\{m_1, ..., m_p\}$. Consequently, $\{\mu_1, ..., \mu_p\}$ is $\mathbb{Q}$-linearly independent. $\square$

Remark. In Ritt's original construction of $\mathbb{Q}^+$-base $\{\mu_1, ..., \mu_p\}$ the real part of each complex α_i was made positive by multiplying with a fixed complex constant.

Our Ritt space, $(\mathcal{R}, \theta_r)$ does not enjoy this characteristic property of $\mathbb{C}$, which forces us to impose the strictly positive condition.

Definition 1.2.3. Let $E_1(x), E_2(x) \in \mathcal{E}$. We say that $E_2(x) \mid E_1(x)$ when there is $E_3(x) \in \mathcal{E}$ such that $E_2(x)E_3(x) = E_1(x)$.

Lemma 1.2.4. Let $E_1(x) = 1 + \sum_{i=1}^{n} a_i f(\alpha_i x)$ and $E_2(x) = 1 + \sum_{i=1}^{r} b_i f(\beta_i x)$. If $E_2(x) \mid E_1(x)$, then each β_j is a $\mathbb{Q}$-linear combination of the α_i's.

Proof. Let

$$1 + \sum_{i=1}^{n} a_i f(\alpha_i x) = (1 + \sum_{i=1}^{r} b_i f(\beta_i x))(1 + \sum_{i=1}^{s} c_i f(\gamma_i x)). \tag{2}$$

Let $\{m_1, ..., m_p\}$ be the largest $\mathbb{Q}$-linearly independent subset of $\{\alpha_1, ..., \alpha_n\}$. Suppose that there is a β_{j_0} which is not a $\mathbb{Q}$-linear combination of α_i's. Taking $m_0 = \beta_{j_0}$, it follows that $\{m_0, m_1, ..., m_p\}$ is also $\mathbb{Q}$-linearly independent. Adjoin $m_{p+1}, ..., m_t$ to this set in such a way that $\{m_0, m_1, ..., m_t\}$ is a $\mathbb{Q}$-linearly independent set and each $\alpha_i, \beta_i, \gamma_i$ is a $\mathbb{Q}$-linear combination of m_i's. Then each β_i has a representation of the form $\sum_k q_{ik} m_k$, where $q_{ik} \in \mathbb{Q}$. Let u_0 be the maximum q_{i0} in the representation of β_i's. Note here that since $\beta_{j_0} = m_0$, $u_0 \geq 1$. Then among those β_i's whose q_{i0} is u_0, let u_1 be the maximum q_{i1}. Continuing this process for all q_{ij}'s, we obtain rational numbers $u_0, u_1, ..., u_t$. Let $\beta = u_0 m_0 + u_1 m_1 + ... + u_t m_t$. Then $\beta = \beta_k$ for some $k = 1, ..., r$. We adjoin $\gamma_0 = 0$ to $\{\gamma_1, ..., \gamma_s\}$ and consider the representation of all γ_i's in the form $\sum_k p_{ik} m_k$, where $p_{ik} \in \mathbb{Q}$. Let v_0 be the maximum p_{i0} in the representation of γ_i's. Since $\gamma_0 = 0$, it follows that $v_0 \geq 0$. Then among those γ_i's whose p_{i0} is v_0, let v_1 be the maximum p_{i1}. Continuing this method for all p_{ij}'s, we get rational numbers $v_0, v_1, ..., v_t$. Let $\gamma = v_0 m_0 + v_1 m_1 + ... + v_t m_t$. Then $\gamma = \gamma_l$ for some $l = 1, ..., s$. Multiplying out the factors on the right hand side of (2), we obtain the unique term $d \cdot f((\beta + \gamma)x)$ in the resulting product for some $d \in \mathbb{F}$. By the choice of β and γ, we have that $\beta + \gamma = \alpha_m$ for some $m = 1, ..., n$. Hence

$\alpha_m = (u_0+v_0)m_0 + (u_1+v_1)m_1 + ... + (u_t+v_t)m_t$ with $u_0+v_0 \geq 1+0 = 1$. This contradicts the fact that $\{m_1, ..., m_p\}$ is a $\mathbb{Q}$-base for $\{\alpha_1, ..., \alpha_n\}$. □

Corollary 1.2.5. Let $E_1(x), E_2(x)$ be RES's. If $E_2(x) \mid E_1(x)$ and $E_1(x)$ is simple, then $E_2(x)$ is also simple.

Proof. Immediate from Lemma 1.2.4. □

Corollary 1.2.6. Assume that $1 + \sum_{i=1}^{n} a_i f(\alpha_i x) = (1 + \sum_{i=1}^{r} b_i f(\beta_i x))(1 + \sum_{i=1}^{s} c_i f(\gamma_i x))$. If α_1 is strictly positive, then each β_i, γ_i can be written as $\mathbb{Q}_0^+$-linear combination with respect to the $\mathbb{Q}^+$-base $\{\mu_1, ..., \mu_p\}$ for $\{\alpha_1, ..., \alpha_n\}$ so obtained in Lemma 1.2.2. In particular,

$$1 + \sum_{i=1}^{n} a_i \prod_{j=1}^{p} f(q_{ij}\mu_j x) = (1 + \sum_{i=1}^{r} b_i \prod_{j=1}^{p} f(q'_{ij}\mu_j x))(1 + \sum_{i=1}^{s} c_i \prod_{j=1}^{p} f(q''_{ij}\mu_j x)), \quad (3)$$

for some positive rational numbers q_{ij}'s and some nonnegative rational numbers q'_{ij}'s and q''_{ij}'s.

Proof. From Lemmas 1.2.2 and 1.2.4, each β_i is a $\mathbb{Q}$-linear combination of μ_i's, say $\beta_i = \sum_k g_{ik}\mu_k$ where $g_{ik} \in \mathbb{Q}$. Suppose on the contrary that there were some β involves, without loss of generality, μ_1 with negative coefficient. Let u_1 be the minimum g_{i1} in the representation of β_i's. Then among those β_i's whose g_{i1} is u_1, let u_2 be the minimum g_{i2}. Continuing this process for all g_{ij}'s, we obtain rational numbers $u_1, ..., u_t$. Let $\beta = u_1\mu_1 + u_2\mu_2 + ... + u_t\mu_t$. Then $\beta = \beta_k$ for some $k = 1, ..., r$, and $u_1 < 0$. We adjoin $\gamma_0 = 0$ to $\{\gamma_1, ..., \gamma_s\}$ and consider the representation of all γ_i's in the form $\sum_k p_{ik}\mu_k$ where $p_{ik} \in \mathbb{Q}$. Let v_1 be the minimum p_{i1} in the representation of γ_i's. Then among those γ_i's whose p_{i1} is v_1, let v_2 be the minimum p_{i2}. Continuing this method for all p_{ij}'s, we obtain rational numbers $v_1, ..., v_t$. Let $\gamma = v_1\mu_1 + v_2\mu_2 + ... + v_t\mu_t$. Then $\gamma = \gamma_l$ for some $l = 1, ..., s$, and $v_1 \leq 0$ because $\gamma_0 = 0$. Multiplying out the factors on the right hand side of (3), we obtain $d \cdot f((\beta+\gamma)x)$ as a unique term for some $d \in \mathbb{F}$. By the choice of β and γ, $\beta+\gamma = \alpha_m$ for some $m = 1, ..., n$. Thus $\alpha_m = (u_1+v_1)\mu_1 + (u_2+v_2)\mu_2 + ... + (u_t+v_t)\mu_t$ where $u_1+v_1 < 0$, i.e. α_m is a $\mathbb{Q}$-linear combination of μ_i's with the coefficient of μ_1 being negative. By assumption, α_m is a $\mathbb{Q}$-linear combination of μ_i's with the coefficient of μ_1 being positive, which is a contradiction. □

1.3 Transforming to polynomials

Let $E(x) = 1 + a_1 f(\alpha_1 x) + ... + a_n f(\alpha_n x) \in \mathcal{E}$ with α_1 strictly positive. Let $\{\mu_1, ..., \mu_p\}$ be a $\mathbb{Q}^+$-base for $\{\alpha_1, ..., \alpha_n\}$. Then

$$\begin{aligned} E(x) &= 1 + a_1 f((\sum_{j=1}^{p} q_{1j}\mu_j)x) + ... + a_n f((\sum_{j=1}^{p} q_{nj}\mu_j)x) \\ &= 1 + a_1 f(q_{11}\mu_1 x)\cdots f(q_{1p}\mu_p x) + ... + a_n f(q_{n1}\mu_1 x)\cdots f(q_{np}\mu_p x), \end{aligned}$$

where q_{ij}'s are positive rational numbers.

Let $l_j \in \mathbb{N}$ $(j = 1, ..., p)$ be the least common multiple of the denominators of q_{ij}, $i = 1, ..., n$. Now

$$\begin{aligned} E(x) &= 1 + a_1 f(q_{11}l_1\frac{\mu_1}{l_1}x)\cdots f(q_{1p}l_p\frac{\mu_p}{l_p}x) + ... + a_n f(q_{n1}l_1\frac{\mu_1}{l_1}x)\cdots f(q_{np}l_p\frac{\mu_p}{l_p}x) \\ &= 1 + a_1 f(k_{11}\frac{\mu_1}{l_1}x)\cdots f(k_{1p}\frac{\mu_p}{l_p}x) + ... + a_n f(k_{n1}\frac{\mu_1}{l_1}x)\cdots f(k_{np}\frac{\mu_p}{l_p}x) \\ &= 1 + a_1(f(\frac{\mu_1}{l_1}x))^{k_{11}}\cdots(f(\frac{\mu_p}{l_p}x))^{k_{1p}} + ... + a_n(f(\frac{\mu_1}{l_1}x))^{k_{n1}}\cdots(f(\frac{\mu_p}{l_p}x))^{k_{np}}, \end{aligned}$$

where $k_{ij} = q_{ij}l_j \in \mathbb{N}$. Invoking on the algebraic independence, replacing $f(\frac{\mu_j}{l_j}x)$ by y_j, the outcome can be considered as a polynomial in $\mathbb{F}[y_1, ..., y_p]$. This polynomial is called the **polynomial corresponding to** $E(x)$ and will be denoted by $Q_E(y_1, ..., y_p)$.

Conversely, for any $P(y_1, ..., y_t) \in \mathbb{F}[y_1, ..., y_t]$, if each y_j is replaced by $f(\alpha_j x)$

where $\{\alpha_1, ..., \alpha_t\}$ is a $\mathbb{Q}$-linearly independent set in $\mathcal{R}$, then we obtain an RES in $\mathcal{E}$, referred to as the **RES corresponding to** $P(y_1, ..., y_t)$ and denoted by $E_P(f(\alpha_1 x), ..., f(\alpha_t x))$.

Remark. $E_{Q_E}(f(\frac{\mu_1}{l_1}x), ..., f(\frac{\mu_p}{l_p}x)) = E(x)$.

Lemma 1.3.1. Let $E(x) = 1 + a_1 f(\alpha_1 x) + ... + a_n f(\alpha_n x)$ with α_1 strictly positive and $Q_E(y_1, ..., y_p)$ be the polynomial corresponding to $E(x)$ with respect to a $\mathbb{Q}^+$-base $\{\mu_1, ..., \mu_p\}$. Then each factorization of $E(x)$ in $\mathcal{E}$ gives rise to a factorization of $Q_E(y_1^{t_1}, ..., y_p^{t_p})$ in $\mathbb{F}[y_1, ..., y_p]$ for some $(t_1, ..., t_p) \in \mathbb{N}^p$ and vice versa.

Proof. ($\Rightarrow$) To simplify notations, we treat only the case when $E(x)$ has two factors. By Corollary 1.2.6,

$$1 + \sum_{i=1}^{n} a_i \prod_{j=1}^{p} f(q_{ij}\mu_j x) = (1 + \sum_{i=1}^{r} b_i \prod_{j=1}^{p} f(q'_{ij}\mu_j x))(1 + \sum_{i=1}^{s} c_i \prod_{j=1}^{p} f(q''_{ij}\mu_j x)),$$

where $q_{ij} = \frac{m_{ij}}{n_{ij}}$, $q'_{ij} = \frac{m'_{ij}}{n'_{ij}}$ and $q''_{ij} = \frac{m''_{ij}}{n''_{ij}}$, $m'_{ij}, m''_{ij} \in \mathbb{N}_0$ and $m_{ij}, n_{ij}, n'_{ij}, n''_{ij} \in \mathbb{N}$. Let $l_j = l.c.m.(n_{1j}, ..., n_{nj})$ and $t_j = l.c.m.(n'_{1j}, ..., n'_{rj}, n''_{1j}, ..., n''_{sj})$. Then

$$1 + \sum_{i=1}^{n} a_i \prod_{j=1}^{p} f(q_{ij}\mu_j x) = 1 + \sum_{i=1}^{n} a_i \prod_{j=1}^{p} (f(\frac{\mu_j}{l_j}x))^{k_{ij}},$$

where $k_{ij} = q_{ij} l_j \in \mathbb{N}$ and

$$1 + \sum_{i=1}^{r} b_i \prod_{j=1}^{p} f(q'_{ij}\mu_j x) = 1 + \sum_{i=1}^{r} b_i \prod_{j=1}^{p} (f(\frac{\mu_j}{l_j}x))^{q'_{ij} l_j},$$

$$1 + \sum_{i=1}^{s} c_i \prod_{j=1}^{p} f(q''_{ij}\mu_j x) = 1 + \sum_{i=1}^{s} c_i \prod_{j=1}^{p} (f(\frac{\mu_j}{l_j}x))^{q''_{ij} l_j}.$$

Thus

$$1 + \sum_{i=1}^{n} a_i \prod_{j=1}^{p} (f(\frac{\mu_j}{l_j}x))^{k_{ij}} = (1 + \sum_{i=1}^{r} b_i \prod_{j=1}^{p} (f(\frac{\mu_j}{l_j}x))^{q'_{ij} l_j})(1 + \sum_{i=1}^{s} c_i \prod_{j=1}^{p} (f(\frac{\mu_j}{l_j}x))^{q''_{ij} l_j}).$$

Substituting $f(\frac{\mu_j}{l_j}x)$ for $y_j^{t_j}$ in the above equation, we get on the left hand side $1 + \sum_{i=1}^{n} a_i \prod_{j=1}^{p} y_j^{k_{ij} t_j}$, which is $Q_E(y_1^{t_1}, ..., y_p^{t_p})$. Since $q'_{ij} l_j t_j$, $q''_{ij} l_j t_j \in \mathbb{N}_0$, we obtain on the right hand side a product of two polynomials in $\mathbb{F}[y_1, ..., y_p]$, $(\sum_{i=1}^{r} b_i \prod_{j=1}^{p} y_j^{q'_{ij} l_j t_j})(\sum_{i=1}^{s} c_i \prod_{j=1}^{p} y_j^{q''_{ij} l_j t_j})$, as required.

($\Leftarrow$) Let

$$Q_E(y_1^{t_1},...,y_p^{t_p}) = R_1(y_1,...,y_p)\cdots R_m(y_1,...,y_p) \tag{5}$$

be a factorization of $Q_E(y_1^{t_1},...,y_p^{t_p})$ in $\mathbb{F}[y_1,...,y_p]$. Replacing y_j by $f(\frac{\mu_j}{l_j}x)$ in (5), we obtain

$$E_{Q_E}((f(\tfrac{\mu_1}{l_1}x))^{t_1},...,(f(\tfrac{\mu_p}{l_p}x))^{t_p}) = E_{R_1}(f(\tfrac{\mu_1}{l_1}x),...,f(\tfrac{\mu_p}{l_p}x))\cdots E_{R_m}(f(\tfrac{\mu_1}{l_1}x),...,f(\tfrac{\mu_p}{l_p}x)).$$

Then

$$\begin{aligned}
E(x) &= E_{Q_E}(f(\frac{\mu_1}{l_1}x),...,f(\frac{\mu_p}{l_p}x)) \\
&= E_{Q_E}((f(\frac{1}{t_1}\frac{\mu_1}{l_1}x))^{t_1},...,(f(\frac{1}{t_p}\frac{\mu_p}{l_p}x))^{t_p}) \\
&= E_{R_1}(f(\frac{1}{t_1}\frac{\mu_1}{l_1}x),...,f(\frac{1}{t_p}\frac{\mu_p}{l_p}x))\cdots E_{R_m}(f(\frac{1}{t_1}\frac{\mu_1}{l_1}x),...,f(\frac{1}{t_p}\frac{\mu_p}{l_p}x))
\end{aligned}$$

is a factorization of $E(x)$ in $\mathcal{E}$ as desired. $\square$

1.4 Polynomials

Having reduced the problem of factorizing RES's to that of factorizing polynomials in several variables, we collect here those results needed to justify the proof of the main theorem.

Let $\varepsilon = (\varepsilon_1,...,\varepsilon_p)$ where ε_i is a primitive k_i-th root of unity. We say that polynomial $P(y_1,...,y_p)$ and $Q(y_1,...,y_p)$ are **ε-related** if $P(y_1,...,y_p) = Q(\varepsilon_1^{n_1}y_1,...,\varepsilon_p^{n_p}y_p)$ for some $(n_1,...,n_p)\in\mathbb{Z}^p$. It can easily be shown that ε-related is an equivalence relation on $\mathbb{F}[y_1,...,y_p]$.

Lemma 1.4.1. Let $Q(y_1,...,y_p)$ be an irreducible polynomial with constant term 1. If there are positive integers t_i's such that

$$Q(y_1^{t_1},...,y_p^{t_p}) = Q_1(y_1,...,y_p)\cdots Q_m(y_1,...,y_p),$$

where $Q_i(y_1,...,y_p)$'s are irreducible polynomials with constant term 1, then every pair $Q_i(y_1,...,y_p)$ and $Q_j(y_1,...,y_p)$ are $(\varepsilon_1,...,\varepsilon_p)$-related where each ε_i is a primitive t_i-th root of unity.

Proof. Since each ε_i is a primitive t_i-th root of unity, it follows that for any $(n_1, ..., n_p) \in \mathbb{Z}^p$, we have

$$\begin{aligned} Q_1(y_1, ..., y_p) \cdots Q_m(y_1, ..., y_p) &= Q(y_1^{t_1}, ..., y_p^{t_p}) \\ &= Q((\varepsilon_1^{n_1} y_1)^{t_1}, ..., (\varepsilon_p^{n_p} y_p)^{t_p}) \\ &= Q_1(\varepsilon_1^{n_1} y_1, ..., \varepsilon_p^{n_p} y_p) \cdots Q_m(\varepsilon_1^{n_1} y_1, ..., \varepsilon_p^{n_p} y_p). \end{aligned}$$

Thus for each $i = 1, ..., m$, $Q_i(\varepsilon_1^{n_1} y_1, ..., \varepsilon_p^{n_p} y_p) = Q_t(y_1, ..., y_p)$ for some $t = 1, ..., m$; that is, each $Q_i(y_1, ..., y_p)$ is ε-related to some $Q_t(y_1, ..., y_p)$. To show that each $Q_i(y_1, ..., y_p)$ is ε-related to all $Q_t(y_1, ..., y_p)$, it suffices to show that $Q_1(y_1, ..., y_p)$ is ε-related to all $Q_t(y_1, ..., y_p)$. Suppose that $Q_1(y_1, ..., y_p)$ is not ε-related to some $Q_t(y_1, ..., y_p)$. Without loss of generality, we may assume that $Q_1(y_1, ..., y_p), ..., Q_j(y_1, ..., y_p)$, $1 \leq j < m$, are in $[Q_1(y_1, ..., y_p)]$, the equivalence class containing $Q_1(y_1, ..., y_p)$, but $Q_{j+1}(y_1, ..., y_p), ..., Q_m(y_1, ..., y_p)$ are not in $[Q_1(y_1, ..., y_p)]$. Thus

$$Q_1(\varepsilon_1^{n_1} y_1, ..., \varepsilon_p^{n_p} y_p) \cdots Q_j(\varepsilon_1^{n_1} y_1, ..., \varepsilon_p^{n_p} y_p) = Q_1(y_1, ..., y_p) \cdots Q_j(y_1, ..., y_p)$$

for all $(n_1, ..., n_p) \in \mathbb{Z}^p$. To show that $Q_1(y_1, ..., y_p) \cdots Q_j(y_1, ..., y_p) := P(y_1, ..., y_p)$ is a polynomial in $y_1^{t_1}, ..., y_p^{t_p}$, suppose not. Then there is y_i such that t_i does not divide an exponent of y_i. Rewrite

$$P(y_1, ..., y_p) = a_0(\overline{y}) + a_1(\overline{y}) y_i + ... + a_n(\overline{y}) {y_i}^n = a_0(\overline{y}) + ... + a_j(\overline{y}) {y_i}^{lt_i + r} + ... ,$$

where $\overline{y} = (y_1, ..., y_{i-1}, y_{i+1}, ..., y_p)$, $a_j(\overline{y}) \neq 0$ and $0 \leq r < t_i$, it follows that

$$\begin{aligned} &a_0(\overline{y}) + ... + a_j(\overline{y}) {y_i}^{lt_i + r} + ... = P(y_1, ..., y_p) = P(\varepsilon_1^{n_1} y_1, ..., \varepsilon_p^{n_p} y_p) \\ &= a_0(\overline{y}) + ... + a_j(\overline{y}) (\varepsilon_i^{n_i} y_i)^{lt_i + r} + ... = a_0(\overline{y}) + ... + a_j(\overline{y}) {y_i}^{lt_i + r} \varepsilon_i^{n_i r} + ... \end{aligned}$$

Thus ${\varepsilon_i}^{n_i r} = 1$, this is not true for all $n_i \in \mathbb{Z}$. Hence $Q_1(y_1, ..., y_p) \cdots Q_j(y_1, ..., y_p)$ $= K(y_1^{t_1}, ..., y_p^{t_p})$ for some $K(y_1, ..., y_p) \in \mathbb{F}[y_1, ..., y_p]$.

Similarly, $Q_{j+1}(y_1, ..., y_p) \cdots Q_m(y_1, ..., y_p) = \overline{K}(y_1^{t_1}, ..., y_p^{t_p})$ for some

$\overline{K}(y_1, ..., y_p) \in \mathbb{F}[y_1, ..., y_p]$. Therefore,

$$\begin{aligned} Q(y_1^{t_1}, ..., y_p^{t_p}) &= Q_1(y_1, ..., y_p) \cdots Q_j(y_1, ..., y_p) Q_{j+1}(y_1, ..., y_p) \cdots Q_m(y_1, ..., y_p) \\ &= K(y_1^{t_1}, ..., y_p^{t_p}) \overline{K}(y_1^{t_1}, ..., y_p^{t_p}). \end{aligned}$$

Then $Q(y_1, ..., y_p) = K(y_1, ..., y_p)\overline{K}(y_1, ..., y_p)$, so $Q(y_1, ..., y_p)$ is reducible, a contradiction. □

Any $P(y_1, ..., y_t) \in \mathbb{F}[y_1, ..., y_t]$ is said to be **primary in** y_i if the greatest common divisor of all exponents of y_i which appear in $P(y_1, ..., y_t)$ is equal to 1 and it is said to be **primary** if it is primary in every y_i.

Lemma 1.4.2. Let $Q(y_1, ..., y_p)$ be a primary irreducible polynomial of degree δ consisting of *more than two terms* and with constant term 1. Suppose that for certain positive integers $t_1, ..., t_p$, the irreducible factors of $Q(y_1^{t_1}, ..., y_p^{t_p})$ are primary. Then there exist a polynomial $T(y_1, ..., y_p)$ and positive integers $\tau_1, ..., \tau_p$ with the following properties :

(a) $T(y_1, ..., y_p)$ is a primary irreducible polynomial with constant term 1.

(b) The degree of $T(y_1, ..., y_p)$ in each variable does not exceed the corresponding degree of $Q(y_1, ..., y_p)$.

(c) For every i, $\tau_i/t_i \geq \delta^{-p}$.

(d) The irreducible factors of $T(y_1^{\tau_1}, ..., y_p^{\tau_p})$ are primary and consist of more than two terms.

(e) The polynomials $T(y_1, y_2^{\tau_2}, ..., y_p^{\tau_p}), T(y_1^{\tau_1}, y_2, y_3^{\tau_3}, ..., y_p^{\tau_p}), ...$ and $T(y_1^{\tau_1}, y_2^{\tau_2}, ..., y_{p-1}^{\tau_{p-1}}, y_p)$ are all irreducible.

Proof. It is enough to consider the case $p = 3$, and replace $y_1, y_2, y_3, t_1, t_2, t_3$ by x, y, z, p, q and r, respectively.

Step 1.((a),(e)) Let

$$Q(x, y^q, z^r) = Q_1(x, y, z) \cdots Q_m(x, y, z), \tag{6}$$

where $Q_i(x, y, z)$'s are irreducible polynomials with constant term 1. By Lemma 1.4.1, Q_1 is related to each Q_i. Thus Q_1 is primary in x, but may not be primary in y and z. Let

$$Q_1(x, y, z) = R(x, y^{q_1}, z^{r_1}),$$

where $R(x, y, z)$ is primary. Then $R(x, y, z)$ is also irreducible. Let a be the degree of x in $Q(x, y, z)$. We will show that $\frac{q}{q_1} \leq a$ and $\frac{r}{r_1} \leq a$.
To see this, from (6), $m \leq a$ and $q_1 | q$. Let $k = \dfrac{q}{q_1}$ and ε_k be a primitive k-th root of unity. Since $R(x, y, z)$ is primary, the k polynomials $R(x, \varepsilon_k^i y^{q_1}, z^{r_1}), i = 1, ..., k$, are all distinct. Since each ε_k^i is a q_1-th power of a q-th root of unity, it follows from Lemma 1.4.1 that $\frac{q}{q_1} = k \leq m \leq a$. Similarly, $\frac{r}{r_1} \leq a$. Denote the degrees of y, z in $Q(x, y, z)$ by b, c, respectively, and the degrees of x, y, z in $R(x, y, z)$ by a_1, b_1, c_1, respectively. By (6), we obtain $a = ma_1$, and so $a_1 \leq a$. Since $mb_1q_1 = bq$ and $q \leq mq_1$, $b_1 \leq b$. Similarly, $c_1 \leq c$.

We replace p by p_1 and let

$$R(x^{p_1}, y, z^{r_1}) = R_1(x, y, z) \cdots R_{m'}(x, y, z),$$

where $R_i(x, y, z)$'s are irreducible polynomials with constant term 1. Then R_1 is primary in y, but may not be primary in x and z. Let

$$R_1(x, y, z) = S(x^{p_2}, y, z^{r_2}),$$

where $S(x, y, z)$ is primary. This implies that $S(x, y, z)$ is irreducible. Then $\frac{p_1}{p_2} \leq b_1$, $\frac{r_1}{r_2} \leq b_1$ and $a_2 \leq a_1, b_2 \leq b_1, c_2 \leq c_1$, where a_2, b_2, c_2 are the degrees of x, y, z in $S(x, y, z)$, respectively.

We substitute q_1 by q_2 and let

$$S(x^{p_2}, y^{q_2}, z) = S_1(x, y, z) \cdots S_{m''}(x, y, z),$$

where $S_i(x, y, z)$'s are irreducible polynomials with constant term 1. Then $S_1(x, y, z)$ is primary in z, but may not be primary in x and y. Let

$$S_1(x,y,z) = T(x^\pi, y^\chi, z),$$

where $T(x,y,z)$ is primary. Then $T(x,y,z)$ is irreducible and $\chi \mid q_2$. Thus $\frac{p_2}{\pi} \le c_2$, $\frac{q_2}{\chi} \le c_2$, $a_3 \le a_2$, $b_3 \le b_2$ and $c_3 \le c_2$, where a_3, b_3, c_3 are the degrees of x, y, z in $T(x,y,z)$, respectively.

We replace r_2 by ρ. We shall show that $T(x, y^\chi, z^\rho)$ is irreducible. Suppose that $T(x, y^\chi, z^\rho)$ is reducible. Let

$$T(x, y^\chi, z^\rho) = A(x,y,z)B(x,y,z),$$

where $A(x,y,z)$ and $B(x,y,z)$ are non-constant polynomials. Then

$$S_1(x,y,z^\rho) = T(x^\pi, y^\chi, z^\rho) = A(x^\pi, y, z)B(x^\pi, y, z).$$

Let $l = \dfrac{q_2}{\chi}$ and ε_l is a primitive l-th root of unity. Since $T(x,y,z)$ is primary, the l polynomials $T(x^\pi, \varepsilon_l^i y^\chi, z^\rho)$, $i = 1, ..., l$, are all distinct. Since each ε_l^i is a χ-th power of a q_2-th root of unity, it follows that each $T(x^\pi, \varepsilon_l^i y^\chi, z^\rho)$ is obtained from $S_1(x,y,z^\rho)$ by replacing y by the product of a q_2-th root of unity and y. Consequently, each $T(x^\pi, \varepsilon_l^i y^\chi, z^\rho)$ is $S_i(x,y,z^\rho)$ and so $l \le m''$. Hence

$$\begin{aligned} S(x^{p_2}, y^{q_2}, z^{r_2}) &= S_1(x,y,z^{r_2}) \cdots S_{m''}(x,y,z^{r_2}) \\ &= S_1(x,y,z^\rho) \cdots S_{m''}(x,y,z^\rho) \\ &= T(x^\pi, y^\chi, z^\rho) T(x^\pi, \varepsilon_l^1 y^\chi, z^\rho) \cdots T(x^\pi, \varepsilon_l^l y^\chi, z^\rho) \cdots \\ &= A(x^\pi, y, z)B(x^\pi, y, z)A(x, \varepsilon_l^1 y^\chi, z)B(x, \varepsilon_l^1 y^\chi, z) \cdots \\ &\quad A(x, \varepsilon_l^l y^\chi, z)B(x, \varepsilon_l^l y^\chi, z) \cdots . \end{aligned}$$

Therefore, $A(x, \varepsilon_l^1 y^\chi, z) \cdots A(x, \varepsilon_l^l y^\chi, z) \mid S(x^{p_2}, y^{q_2}, z^{r_2}) = R(x, y^{q_2}, z)$. Note that when we multiply out $A(x, \varepsilon_l^1 y^\chi, z)...A(x, \varepsilon_l^l y^\chi, z)$ each coefficient of $y^{\chi n}$, $n \in \mathbb{N}$ is a symmetric polynomial in $\varepsilon_l^1, ..., \varepsilon_l^l$ and vanishes unless n is a multiple of l, i.e. $A(x, \varepsilon_l^1 y^\chi, z) \cdots A(x, \varepsilon_l^l y^\chi, z)$ is a polynomial in x, y^{q_2}, z. Thus $R(x,y,z)$ is reducible, which is a contradiction. Hence $T(x, y^\chi, z^\rho)$ is irreducible.

By the same proof as what has just been done, $T(x^\pi, y, z^\rho)$ is irreducible.

Step 2. (d) We have that

(1) $T(x^\pi, y^\chi, z^\rho)$ is a factor of $S(x^{p_2}, y^{q_2}, z^{r_2})$,

(2) $S(x^{p_2}, y^{q_2}, z^{r_2})$ is a factor of $R(x^{p_1}, y^{q_1}, z^{r_1})$ and

(3) $R(x^{p_1}, y^{q_1}, z^{r_1})$ is a factor of $Q(x^p, y^q, z^r)$.

Thus $T(x^\pi, y^\chi, z^\rho)$ is a factor of $Q(x^p, y^q, z^r)$. By assumption, the irreducible factors of $Q(x^p, y^q, z^r)$ are primary. Thus the irreducible factors of $T(x^\pi, y^\chi, z^\rho)$ are primary. Let

$$T(x^\pi, y^\chi, z^\rho) = T_1(x, y, z) \cdots T_t(x, y, z),$$

where $T_i(x, y, z)$'s are primary irreducible polynomials with constant term 1. We must show that each $T_i(x, y, z)$ has more than two terms. Without loss of generality, suppose that $T_1(x, y, z)$ contains only two terms. Let $T_1(x, y, z) = 1 + cx^\alpha y^\beta z^\gamma$. Since $T_1(x, y, z)$ is an irreducible factor of $Q(x^p, y^q, z^r)$, by Lemma 1.4.1, other irreducible factors of $Q(x^p, y^q, z^r)$ are ε-related to $T_1(x, y, z)$. Thus $Q(x^p, y^q, z^r)$ is a polynomial in $x^\alpha y^\beta z^\gamma$. Then the exponents of x, y, z in each term of $Q(x, y, z)$ are respectively multiples of $\frac{\alpha}{p}$, $\frac{\beta}{q}$, $\frac{\gamma}{r}$.

Let A, B, C be the greatest common divisor of all exponents of $x^{\frac{\alpha}{p}}, y^{\frac{\beta}{q}}, z^{\frac{\gamma}{r}}$ which appear in $Q(x, y, z)$, respectively. Let $\mathcal{T} = x^A y^B z^C$. Then $Q(x, y, z)$ is a polynomial in $\mathcal{T}$ which contains more than two terms. Hence $Q(x, y, z)$, considered as polynomial in one variable $\mathcal{T}$ of more than two terms, must then be reducible, which is a contradiction.

Step 3. (b) From above, degree of x in $T(x, y, z) = a_3 \leq a_2 =$ degree of x in $S(x, y, z) \leq a_1 =$ degree of x in $R(x, y, z) \leq a =$ degree of x in $Q(x, y, z)$, and so are the degrees of y, z.

Step 4. (c) We have $\frac{q}{q_1} \leq a$, $\frac{r}{r_1} \leq a$, $\frac{p_1}{p_2} \leq b_1$, $\frac{r_1}{r_2} \leq b_1$, $\frac{p_2}{\pi} \leq c_2$, $\frac{q_2}{\chi} \leq c_2$, $a_2 \leq a_1 \leq a$, $b_2 \leq b_1 \leq b$ and $c_2 \leq c_1 \leq c$. Thus $\frac{\pi}{p} = \frac{\pi}{p_2} \cdot \frac{p_2}{p_1} \cdot \frac{p_1}{p} \geq \frac{1}{c_2} \cdot \frac{1}{b_1} \cdot 1 \geq \frac{1}{ab_1c_2} \geq \frac{1}{abc} \geq \frac{1}{\delta^3}$, $\frac{\chi}{q} = \frac{\chi}{q_2} \cdot \frac{q_2}{q_1} \cdot \frac{q_1}{q} \geq \frac{1}{c_2} \cdot 1 \cdot \frac{1}{a} \geq \frac{1}{ab_1c_2} \geq \frac{1}{abc} \geq \frac{1}{\delta^3}$ and $\frac{\rho}{r} = \frac{\rho}{r_2} \cdot \frac{r_2}{r_1} \cdot \frac{r_1}{r} \geq 1 \cdot \frac{1}{b_1} \cdot \frac{1}{a} \geq \frac{1}{ab_1c_2} \geq$

$\frac{1}{abc} \geq \frac{1}{\delta^3}$, where $\delta \geq max\{a, b, c\}$. □

Lemma 1.4.3. Let $Q(y_1, ..., y_p)$ be a primary irreducible polynomial consisting of more than two terms and having 1 for its constant term. Then there exist only a finite number of sets of positive integers $t_1, ..., t_p$ such that the irreducible factors of $Q(y_1^{t_1}, ..., y_p^{t_p})$ are primary.

Proof. Let $T(y_1, ..., y_p)$ be the polynomial and $\tau_1, ..., \tau_p$ be the integers whose existence were shown in Lemma 1.4.2. Let

$$T(y_1^{\tau_1}, ..., y_p^{\tau_p}) = T_1(y_1, ..., y_p) \cdots T_t(y_1, ..., y_p), \tag{7}$$

where each $T_i(y_1, ..., y_p)$ is a primary irreducible polynomial consisting of more than two terms with constant term 1. We will show that $t = \tau_1 = \tau_2 = ... = \tau_p$. To prove this, let ε be a primitive τ_1-th root of unity. Thus the τ_1 polynomials $T_1(\varepsilon^i y_1, y_2 ..., y_p),\ i = 1, ..., \tau_1$ are all distinct, and each of them is equal to some $T_i(y_1, ..., y_p)$. Then the product of these polynomials is a polynomial in $y_1^{\tau_1}, y_2, ..., y_p$. Since $T_1(\varepsilon^1 y_1, y_2, ..., y_p), ..., T_1(\varepsilon^{\tau_1} y_1, y_2, ..., y_p)$ are irreducible factors of $T(y_1^{\tau_1}, ..., y_p^{\tau_p})$ and they are all distinct, it follows that $\tau_1 \leq t$. Assume that $\tau_1 < t$. Then

$$\begin{aligned} T(y_1^{\tau_1}, ..., y_p^{\tau_p}) &= T_1(\varepsilon^1 y_1, y_2, ..., y_p) \cdots T_1(\varepsilon^{\tau_1} y_1, y_2, ..., y_p) \cdots \\ &= P(y_1^{\tau_1}, y_2, ..., y_p)\overline{P}(y_1^{\tau_1}, y_2, ..., y_p). \end{aligned}$$

Thus $T(y_1, y_2^{\tau_2}, ..., y_p^{\tau_p}) = P(y_1, y_2, ..., y_p)\overline{P}(y_1, y_2, ..., y_p)$. Hence $T(y_1, y_2^{\tau_2}, ..., y_p^{\tau_p})$ is reducible, which contradicts Lemma 1.4.2(e). Therefore, $\tau_1 = t$. Similarly, $\tau_2 = t, ..., \tau_p = t$.

Since $T_1(y_1, ..., y_p)$ is primary, let $ay_1^{\alpha_1} \cdots y_p^{\alpha_p}$ and $by_1^{\beta_1} \cdots y_p^{\beta_p}$ be two terms of $T_1(y_1, ..., y_p)$ with α_1 and α_2 not proportional to β_1 and β_2 ; that is $\alpha_1\beta_2 - \beta_1\alpha_2 \neq 0$. Without loss of generality, we may assume that $\alpha_1\beta_2 - \beta_1\alpha_2 > 0$. Then $\alpha_1 > 0$ and $\beta_2 > 0$. There are t^2 relations transforming y_1 and y_2 in $T_1(y_1, ..., y_p)$ by primitive

t-th roots of unity but there are only t distinct $T_i(y_1, ..., y_p)$'s. Then there must be t ways which leave some $T_j(y_1, ..., y_p)$ invariant. Without loss of generality, we may assume $T_j(y_1, ..., y_p) = T_1(y_1, ..., y_p)$ by taking appropriate composite relations. Let $\varepsilon^u y_1$ and $\varepsilon^v y_2$ be any of the t operations which leave $T_1(y_1, ..., y_p)$ invariant. Thus the congruences

$$\alpha_1 u + \alpha_2 v \equiv 0 \pmod{t}, \quad \beta_1 u + \beta_2 v \equiv 0 \pmod{t}$$

must have at least t solutions (u, v) with $0 \leq u, v < t$. Any solution of the above congruences is also a solution of the congruences

$$(\alpha_1\beta_2 - \beta_1\alpha_2)u \equiv 0 \pmod{t} \tag{8}$$

$$\beta_2 v \equiv -\beta_1 u \pmod{t}. \tag{9}$$

Let h be the greatest common divisor of $(\alpha_1\beta_2 - \beta_1\alpha_2)$ and t. Then (8) has precisely h solutions in u. Let k be the greatest common divisor of β_2 and t. Then for each u satisfying (8), the congruence (9) has at most k solutions in v. Thus $hk \geq t$, so that either $h \geq t^{\frac{1}{2}}$ or $k \geq t^{\frac{1}{2}}$. Finally, we show that for each $i = 1, ..., p$, we have $t_i \leq \delta^{p+4}$ where δ is the degree of $Q(y_1, ..., y_p)$, which will imply that the set of all $(t_1, ..., t_p)$ is finite.

Case 1. $h \geq t^{\frac{1}{2}}$, then $\alpha_1\beta_2 \geq \alpha_1\beta_2 - \beta_1\alpha_2 \geq h \geq t^{\frac{1}{2}}$. Thus $\alpha_1 \geq t^{\frac{1}{4}}$ or $\beta_2 \geq t^{\frac{1}{4}}$.

Case 1.1. $\alpha_1 \geq t^{\frac{1}{4}}$, let a be the degree of y_1 in $T(y_1, ..., y_p)$. Then by (7), $t \cdot a \geq t \cdot \alpha_1 \geq t \cdot t^{\frac{1}{4}}$, and so $a \geq t^{\frac{1}{4}}$. By Lemma 1.4.2(b), $a \leq \delta$ where δ is the degree of $Q(y_1, ..., y_p)$. Thus $t \leq \delta^4$. By Lemma 1.4.2(c), $\frac{t}{t_i} \geq \delta^{-p}$, and so $t_i \leq \delta^{p+4}$ for all $i = 1, ..., p$.

Case 1.2. $\beta_2 \geq t^{\frac{1}{4}}$, by similar argument, $t_i \leq \delta^{p+4}$.

Case 2. $k \geq t^{\frac{1}{2}}$, then $\beta_2 \geq k \geq t^{\frac{1}{2}} \geq t^{\frac{1}{4}}$. Then we are led to Case 1.2. □

1.5 Main theorem

Definition 1.5.1. For any $E_1(x), E_2(x) \in \mathcal{E}$, we say that $E_1(x), E_2(x)$ are **relatively prime** if they have no common divisor in $\mathcal{E}$ except 1.

Lemma 1.5.2. Let $E_1(x) = 1 + \sum_{i=1}^{n} a_i f(\alpha_i x)$, $E_2(x) = 1 + \sum_{i=1}^{r} b_i f(\beta_i x)$ and $E_3(x) = 1 + \sum_{i=1}^{s} c_i f(\gamma_i x)$ be elements in $\mathcal{E}$ with α_1, β_1 and γ_1 strictly positive. If $E_1(x) \mid E_2(x)E_3(x)$ and $E_1(x), E_2(x)$ are relatively prime, then $E_1(x) \mid E_3(x)$

Proof. Assume that $E_2(x)E_3(x) = E_1(x)E_4(x)$ for some $E_4(x) = 1 + \sum_{i=1}^{m} d_i f(\delta_i x)$ in $\mathcal{E}$. Since $\alpha_1, \beta_1, \gamma_1$ are strictly positive, δ_1 is strictly positive. By Lemma 1.2.2, for each $i = 1,...,4$, $E_i(x)$ has a $\mathbb{Q}^+$-base for the RE-coefficients. Let $\{\mu_1, ..., \mu_p\}$ be a largest $\mathbb{Q}^+$-linearly independent subset of the set of elements in $\mathbb{Q}^+$-base of all $E_i(x)$'s. Hence

$$E_1(x) = 1 + \sum_{i=1}^{n} a_i f((\sum_{j=1}^{p} q_{ij}\mu_j)x),$$
$$E_2(x) = 1 + \sum_{i=1}^{r} b_i f((\sum_{j=1}^{p} p_{ij}\mu_j)x),$$
$$E_3(x) = 1 + \sum_{i=1}^{s} c_i f((\sum_{j=1}^{p} k_{ij}\mu_j)x) \quad \text{and}$$
$$E_4(x) = 1 + \sum_{i=1}^{m} d_i f((\sum_{j=1}^{p} l_{ij}\mu_j)x),$$

where q_{ij}'s, p_{ij}'s, k_{ij}'s, l_{ij}'s are nonnegative rational numbers. Let t_j be the least common multiple of the denominators of nonzero q_{ij}, p_{ij}, k_{ij} and l_{ij}. Then

$$E_1(x) = 1 + \sum_{i=1}^{n} a_i f((\sum_{j=1}^{p} q_{ij}t_j\frac{\mu_j}{t_j})x),$$
$$E_2(x) = 1 + \sum_{i=1}^{r} b_i f((\sum_{j=1}^{p} p_{ij}t_j\frac{\mu_j}{t_j})x),$$
$$E_3(x) = 1 + \sum_{i=1}^{s} c_i f((\sum_{j=1}^{p} k_{ij}t_j\frac{\mu_j}{t_j})x) \quad \text{and}$$
$$E_4(x) = 1 + \sum_{i=1}^{m} d_i f((\sum_{j=1}^{p} l_{ij}t_j\frac{\mu_j}{t_j})x).$$

Replacing $f(\frac{\mu_j}{t_j}x)$ by y_j in $E_i(x)$, we obtain a polynomial $Q_i(y_1, ..., y_p)$. Hence

$Q_1Q_4 = Q_2Q_3$; that is, $Q_1 \mid Q_2Q_3$. If there is a nonconstant common factor, $P_{(}y_1, ..., y_p)$, of $Q_1(y_1, ..., y_p)$ and $Q_2(y_1, ..., y_p)$, then $E_P(f(\frac{\mu_1}{t_1}x)), ..., f(\frac{\mu_p}{t_p}x))$, RES corresponding to $P(y_1, ..., y_p)$, is a nonconstant common factor of $E_1(x)$ and $E_2(x)$, which is a contradiction. Thus $Q_1(y_1, ..., y_p), Q_2(y_1, ..., y_p)$ are relatively prime as polynomials, and so $Q_1(y_1, ..., y_p) \mid Q_3(y_1, ..., y_p)$ implying $E_1(x) \mid E_3(x)$. □

We are now ready to prove our main theorem.

Theorem 1.5.3. Every RES of the form

$$1 + a_1 f(\alpha_1 x) + ... + a_n f(\alpha_n x),$$

with $a_1 \neq 0$ and α_1 strictly positive, can be uniquely expressed as a product

$$(S_1 S_2 \cdots S_s)(I_1 I_2 \cdots I_i),$$

where $S_1, ..., S_s$ are simple RES's such that the RE-coefficients in any one of them have irrational ratios to the RE-coefficients in any other, and $I_1, ..., I_i$ are irreducible RES's.

Proof. Let $\{\mu_1, ..., \mu_p\}$ be a $\mathbb{Q}^+$-base for $\{\alpha_1, ..., \alpha_n\}$. Then

$$\begin{aligned} E(x) &= 1 + \sum_{i=1}^{n} a_i f((\sum_{j=1}^{p} q_{ij}\mu_j)x) \\ &= 1 + \sum_{i=1}^{n} a_i f((\sum_{j=1}^{p} q_{ij} l_j \frac{\mu_j}{l_j})x), \end{aligned}$$

where q_{ij}'s are positive rational numbers and l_j is the least common multiple of the denominators of q_{ij}, $i = 1, ..., n$. Replacing $f(\frac{\mu_j}{l_j}x)$ by y_j, we obtain the polynomial corresponding to $E(x)$, $Q_E(y_1, ..., y_p)$. We resolve $Q_E(y_1, ..., y_p)$ into irreducible factors with constant term 1 and separate these factors into two groups. The first group contains irreducible factors consisting of two terms which will be proved in step 1 that they offer the simple factors $S_1, ..., S_s$ and the second group contains the rest which will be proved in step 2 that they provide the irreducible factors $I_1, ..., I_i$.

Step 1. For each irreducible factor consisting of two terms $T(y_1, ..., y_p) = 1 + ay_1^{t_1} \cdots y_p^{t_p}$, replacing y_j in $T(y_1, ...y_p)$ by $f(\frac{\mu_j}{l_j}x)$, we get a simple RES $1 + af((t_1\frac{\mu_1}{l_1} + ... + t_p\frac{\mu_p}{l_p})x)$. Partition the set of these simple RES's into sets such that the RE-coefficients of the RES's of any one set have rational ratios to one another, but have irrational ratios to the RE-coefficients of any other set. Then the product of the simple RES's in each set is also a simple RES. The simple RES's, so obtained, form the required simple RES's $S_1, ..., S_s$.

Step 2. For each irreducible factor consisting of three terms or more $U(y_1, ..., y_r)$; $r \leq p$, we rewrite $U(y_1, ..., y_r)$ as $V(y_1^{m_1}, ..., y_r^{m_r})$, where $V(y_1, ..., y_r)$ is primary. Then $V(y_1, ..., y_r)$ is irreducible. By Lemma 1.4.3, there exist only a finite number of set of positive integers $t_1, ..., t_r$ such that the irreducible factors of $P(y_1^{t_1}, ..., y_r^{t_r})$ are primary for all $P(y_1, ..., y_r) \in \mathbb{F}[y_1, ..., y_r]$. Let $t_1, ..., t_r$ be natural numbers arisen from the factorization of $V(y_1^{t_1}, ..., y_r^{t_r})$ with a maximum number, q, of irreducible and primary factors. Let

$$V(y_1^{t_1}, ..., y_r^{t_r}) = V_1(y_1, ..., y_r) \cdots V_q(y_1, ..., y_r). \tag{10}$$

We claim that the RES's, obtained by replacing each y_j in $V_1(y_1, ..., y_r), ...,$ $V_q(y_1, ..., y_r)$ by $f(\frac{m_j}{t_j}\frac{\mu_j}{l_j}x)$, are all irreducible in $\mathcal{E}$.

Suppose on the contrary that at least one of them is not irreducible, say $V_1(y_1, ..., y_r))$. Let

$$V_1(f(\frac{m_1}{t_1}\frac{\mu_1}{l_1}x), ..., f(\frac{m_r}{t_r}\frac{\mu_r}{l_r}x)) = (1 + \sum_{i=1}^{s_1} c_i f(\gamma_i x))(1 + \sum_{i=1}^{s_2} d_i f(\delta_i x)).$$

By Corollary 1.2.6, γ_i, δ_i are $\mathbb{Q}_0^+$-linear combinations of $\frac{\mu_i}{l_i}$'s. Thus

$$\begin{aligned} V_1(f(\frac{m_1}{t_1}\frac{\mu_1}{l_1}x), ..., f(\frac{m_r}{t_r}\frac{\mu_r}{l_r}x)) &= (1+\sum_{i=1}^{s_1} c_i f(\gamma_i x))(1+\sum_{i=1}^{s_2} d_i f(\delta_i x)) \\ &= (1+\sum_{i=0}^{s_1} c_i f((\sum_{j=0}^{r} q'_{ij}\frac{\mu_j}{l_j})x))\cdot \\ &\quad (1+\sum_{i=0}^{s_2} d_i f((\sum_{j=0}^{r} q''_{ij}\frac{\mu_j}{l_j})x)) \end{aligned}$$

for some $q'_{ij}, q''_{ij} \in \mathbb{Q}_0^+$. Let h_j be the least common multiple of the denominators of $q'_{1j}, ..., q'_{s_1 j}, q''_{1j}, ..., q''_{s_2 j}$. Replacing $f(\frac{\mu_j}{l_j}x)$ by $y_j^{h_j}$, we get

$$V_1(y_1^{\frac{m_1}{t_1}h_1}, ..., y_r^{\frac{m_r}{t_r}h_p}) = (1+\sum_{i=1}^{s_1} c_i \prod_{j=1}^{r} y_j^{q'_{ij}h_j})(1+\sum_{i=1}^{s_2} d_i \prod_{j=1}^{r} y_j^{q''_{ij}h_j}).$$

Thus $\frac{m_1 h_1}{t_1}, ..., \frac{m_r h_r}{t_r}$ are positive integers making $V_1(y_1^{\frac{m_1 h_1}{t_1}}, ..., y_r^{\frac{m_r h_r}{t_r}})$ reducible. From(10), $V(y_1^{t_1 \frac{m_1 h_1}{t_1}}, ..., y_r^{t_r \frac{m_r h_r}{t_r}}) = V_1(y_1^{\frac{m_1 h_1}{t_1}}, ..., y_r^{\frac{m_r h_r}{t_r}}) \cdots V_q(y_1^{\frac{m_1 h_1}{t_1}}, ..., y_r^{\frac{m_r h_r}{t_r}})$ contains more than q primary irreducible factors, which is impossible.

To prove the uniqueness, assume that $(S_1 \cdots S_s)(I_1 \cdots I_i)$ and $(T_1 \cdots T_t)(J_1 \cdots J_j)$ are two factorizations of $E(x)$. Thus $(S_1 \cdots S_s)(I_1 \cdots I_i)$ is divisible by J_1. If $J_1 \mid S_l$ for some l, then J_1 is a simple RES, by Corollary 1.2.5, which is a contradiction. Thus $J_1 \mid (I_1 \cdots I_i)$. If $J_1 \mid I_l$ for some l, then $J_1 = I_l$ which implies that we can cancel out all these identical irreducible factors. Having done so, it follows that $i = j$ and $\{I_1, ..., I_i\}$ is a permutation of $\{J_1, ..., J_j\}$. Since $T_1 \mid S_1 \cdots S_s$, it follows from Lemma 1.5.2 that a factor of T_1 is also a factor of, say S_1. Then we can write

$$T_1 = F_1 T'_1$$
$$S_1 = F_1 S'_1,$$

where F_1 is a common factor of T_1 and S_1 and T'_1 and S'_1 are relatively prime. By Lemma 1.2.4, q_1(s-index of T_1) = (s-index of F_1) = l_1(s-index of S_1) for some $q_1, l_1 \in \mathbb{Q}$. Assume that T'_1 and some S_i, say S_2, have a common factor. Write

$$T_1' = F_2 T_1''$$

$$S_2 = F_2 S_2',$$

where F_2 is a common factor of T_1' and S_2 and T_1'' and S_2' are relatively prime. Thus q_2(s-index of T_1') = (s-index of F_2) = l_2(s-index of S_2) for some $q_2, l_2 \in \mathbb{Q}$. Then $l_1 q_2 q_3$(s-index ofS_1) = $q_2 q_3$(s-index of F_1) = $q_1 q_2 q_3$(s-index of T_1) = $q_1 q_2$(s-index of T_1') = q_1(s-index of F_2) = $l_2 q_1$(s-index of S_2) for some $q_3 \in \mathbb{Q}$. Consequently, s-index of $S_1 = q$(s-index of S_2) for some $q \in \mathbb{Q}$, which is impossible. Thus $T_1 \mid S_1$. Similarly, $S_1 \mid T_1$. Then $S_1 = T_1$. Continuing in this fashion, we have $\{S_1, ..., S_s\}$ is a permutation of $\{T_1, ..., T_t\}$. □

Definition 1.5.4. For any elements $\alpha = r_1\theta_1 + ... + r_m\theta_m$ and $\beta = s_1\theta_1 + ... + s_n\theta_n$ in $\mathcal{R}$, we say that α is **strictly less than** β if $r_1 < s_1$.

Corollary 1.5.5. Let $E(x) = \sum_{i=0}^{n} a_i f(\alpha_i x)$. If α_1 is strictly less than α_0, then $E(x)$ can be uniquely expressed as a product

$$c(S_1 S_2 \cdots S_s)(I_1 I_2 \cdots I_i) \ ,$$

where c is a constant RES, $S_1, ..., S_s$ are simple RES's such that the RE-coefficients in any one of them have irrational ratios to the RE-coefficients in any other, and $I_1, ..., I_i$ are irreducible RES's.

Proof. Let $E(x) = \sum_{i=0}^{n} a_i f(\alpha_i x)$. Then we can write $E(x)$ in the form

$$a_0 f(\alpha_0 x)[1 + \sum_{i=1}^{n} (\frac{a_i}{a_0}) f((\alpha_i - \alpha_0)x)], \quad \alpha_0 < \alpha_1 < ... < \alpha_n.$$

Since α_1 is strictly less than α_0, $\alpha_1 - \alpha_0$ is strictly positive. By Theorem 1.5.3, $1 + \sum_{i=1}^{n} (\frac{a_i}{a_0}) f((\alpha_i - \alpha_0)x)$ can be factored in the form

$$(S_1 \cdots S_s)(I_1 \cdots I_i) \tag{11}$$

where $S_1, ..., S_s$ are simple RES's such that the RE-coefficients in any one of them have irrational ratios to the RE-coefficients in any other, and $I_1, ..., I_i$ are irreducible RES's. If $\alpha_0 = \overline{0}$, then $a_0 f(\alpha_0 x)$ is a constant RES, and we are done. For the case $\alpha_0 \neq \overline{0}$, $a_0 f(\alpha_0 x)$ is a simple RES. If $\alpha_0 = q_0$(s-index of S_{j_0}) for some $j_0 = 1, ..., s$ and $q_0 \in \mathbb{Q}$, then $\overline{S}_{j_0} = a_0 f(\alpha_0 x) S_{j_0}$ is simple, so the factorization obtain by replacing S_{j_0} by $\overline{S}_{j_0}$ in (11) is the factorization needed for $E(x)$. If $\alpha_0 \neq q$(s-index of S_j) for all $j = 1, ..., s$ and $q \in \mathbb{Q}$, then $S_{s+1} = a_0 f(\alpha_0 x)$ is a simple factor of $E(x)$ and $E(x) = (S_1 \cdots S_s S_{s+1})(I_1 \cdots I_i)$ is the required factorization. $\square$

CHAPTER II

Shapiro's factorization theorem

2.1 Backgrounds

Lemma 2.1.1. Let $F(x) = \sum_{i=1}^{n} P_i(x) A_i^{Q(x)}$, where $A_i \in \mathbb{C} \setminus \{0\}$, $P_i(x) \in \mathbb{C}[x] \setminus \{0\}$ and $Q(x) \in \mathbb{Z}[x] \setminus \mathbb{Z}$. If $F(x) = 0$ for all sufficient large integers x, then there exist $i_0, j_0, i_0 \neq j_0$ such that $|\frac{A_{i_0}}{A_{j_0}}| = 1$.

Proof. Suppose that $|\frac{A_i}{A_j}| \neq 1$ for all $i \neq j$. Let $Q(x) = c_m x^m + ... + c_0$, $c_m \neq 0$, and let $Z = \{x \in \mathbb{Z} \mid F(x) = 0\}$. Without loss of generality, arrange the A_i's so that $|A_1| < ... < |A_n|$. Assume that $c_m > 0$. For $x \in Z$,

$$0 = \frac{F(x)}{A_n^{Q(x)}} = P_1(x)(\frac{A_1}{A_n})^{Q(x)} + \ldots + P_{n-1}(x)(\frac{A_{n-1}}{A_n})^{Q(x)} + P_n(x).$$

The limit on the right hand side does not exists, which is a contradiction. The case $c_m < 0$ is similar. □

From Lemma 2.1.1, there exist i, j such that $|\frac{A_i}{A_j}| = 1, i \neq j$. This leads us to consider an expression, called a **pexponential polynomial**, of the form

$$\begin{aligned} F(x) = {} & [P_{01}(x)\rho_{01}^{Q(x)} + P_{02}(x)\rho_{02}^{Q(x)} + ... + P_{0n_0}(x)\rho_{0n_0}^{Q(x)}]A_0^{Q(x)} + \\ & [P_{11}(x)\rho_{11}^{Q(x)} + P_{12}(x)\rho_{12}^{Q(x)} + ... + P_{1n_1}(x)\rho_{1n_1}^{Q(x)}]A_1^{Q(x)} + \\ & [P_{21}(x)\rho_{21}^{Q(x)} + P_{22}(x)\rho_{22}^{Q(x)} + ... + P_{2n_2}(x)\rho_{2n_2}^{Q(x)}]A_2^{Q(x)} + ... + \\ & [P_{k1}(x)\rho_{k1}^{Q(x)} + P_{k2}(x)\rho_{k_2}^{Q(x)} + ... + P_{kn_k}(x)\rho_{kn_k}^{Q(x)}]A_k^{Q(x)}, \end{aligned}$$

where ρ_{ij} is a δ_{ij}-th root of unity, $\rho_{i1} = 1$, $P_{ij}(x) \in \mathbb{C}[x] \setminus \{0\}$, $Q(x) \in \mathbb{Z}[x] \setminus \mathbb{Z}$, $A_i \in \mathbb{C} \setminus \{0\}$, $A_0 = 1$ and $|A_0| < |A_1| < ... < |A_k|$.

Rewrite $F(x)=\sum_{i=0}^{k}F_i(x)$, where $F_i(x)=A_i^{Q(x)}(\sum_{j=1}^{n_i}P_{ij}(x)\rho_{ij}^{Q(x)})$.
Let $S_i=\{\rho_{i1},\rho_{i2},...,\rho_{in_i}\}$ and define the **rank of** $F_i(x)$ to be the least common multiple of the order of the roots of unity in S_i and the **rank of** $F(x)$ to be the least common multiple of the ranks of $F_i(x)$, $i=0,1,...,k$, denoted by $R(F)$.

Let $F(x)=\sum_{i=0}^{k}A_i^{Q(x)}(\sum_{j=1}^{n_i}P_{ij}(x)\rho_{ij}^{Q(x)})$ be a pexponential polynomial. If each $P_{ij}(x)\in\overline{\mathbb{Q}}[x]\setminus\{0\}$, $\log(\rho_{ij}A_i)\in\overline{\mathbb{Q}}\setminus\{0\}$, $Q(0)=0$ and $Q'(0)\neq 0$, then $F(x)$ satisfies the result of the Skolem-Mahler-Lech theorem (Theorem 2.1.2), and will be called an **SML pexponential polynomial** and denoted by SML-pex. This particular shape of SML-pex will be kept standard throughout the rest of this chapter.

Let V denote the set of all nonzero SML-pex $F(x)$ **with infinitely many integer zeros**.

Theorem 2.1.2. If $F(x)\in V$, then there exist an integer Δ and a certain set $\{d_1,...,d_l\}$ of least positive residues modulo Δ such that $F(x)$ vanishes for all integers $x\equiv d_j \pmod{\Delta}$, $j=1,...,l$, and $F(x)$ vanishes only finitely often on other integers.

Proof. This is proved in [1]. □

The integer Δ, which appears in Theorem 2.1.2, is called a **period of** $F(x)$. In fact, any multiple of a period is also a period. We shall call the least positive period the **basic period of** $F(x)$.

For any $F(x)\in V$ with a period Δ, we shall denote by $\mathcal{P}(F,\Delta)$ the set of all least positive residues $d_1,...,d_l$ modulo Δ mentioned in Theorem 2.1.2.

2.2 Lemmas and factorization theorem

Lemma 2.2.1. Let $F(x) \in V$. Then for each $i = 1, 2, ..., k$, $\displaystyle\sum_{j=1}^{n_i} P_{ij}(x)\rho_{ij}^{Q(d)} = 0.$

Proof. Let $\beta \in \mathbb{N}$. Substituting $x = t\beta\Delta + d$, where $t \in \mathbb{Z}$ and $d \in \mathcal{P}(F, \Delta)$, we get $0 = \frac{F(t\beta\Delta+d)}{A_k^{Q(t\beta\Delta+d)}} = \displaystyle\sum_{i=0}^{k} (\frac{A_i}{A_k})^{Q(t\beta\Delta+d)} (\sum_{j=1}^{n_i} P_{ij}(t\beta\Delta + d)\rho_{ij}^{Q(t\beta\Delta+d)})$, $A_0 = 1$. Assuming that the leading coefficient of $Q(x)$ is positive ; the other possibility is treated similarly, then $\displaystyle\sum_{j=1}^{n_k} P_{kj}(t\beta\Delta + d)\rho_{kj}^{Q(t\beta\Delta+d)} \to 0$, as $t \to \infty$. Taking $t = u\delta_k$, where $u \in \mathbb{Z}$, $u \to \infty$

and $\delta_k = l.c.m.(\delta_{k1}, \delta_{k2}, ..., \delta_{kn_k})$, we obtain $\displaystyle\sum_{j=1}^{n_k} P_{kj}(u\delta_k\beta\Delta + d)\rho_{kj}^{Q(d)} \to 0$. The polynomial $\displaystyle\sum_{j=1}^{n_k} P_{kj}(x)\rho_{kj}^{Q(d)}$ tending to 0 as $x \to \infty$ on $\mathbb{Z}$ implies that it must vanish identically, and so

$$\begin{aligned} 0 = F(u\delta_k\beta\Delta + d) &= \sum_{i=0}^{k} A_i^{Q(u\delta_k\beta\Delta+d)} (\sum_{j=1}^{n_i} P_{ij}(u\delta_k\beta\Delta + d)\rho_{ij}^{Q(u\delta_k\beta\Delta+d)}) \\ &= \sum_{i=0}^{k-1} A_i^{Q(u\delta_k\beta\Delta+d)} (\sum_{j=1}^{n_i} P_{ij}(u\delta_k\beta\Delta + d)\rho_{ij}^{Q(u\delta_k\beta\Delta+d)}). \end{aligned}$$

Repeating the above steps again, we have

$$0 = \tfrac{F(u\delta_k\beta\Delta+d)}{A_{k-1}^{Q(u\delta_k\beta\Delta+d)}} = \sum_{i=0}^{k-1} (\frac{A_i}{A_{k-1}})^{Q(u\delta_k\beta\Delta+d)} (\sum_{j=1}^{n_i} P_{ij}(u\delta_k\beta\Delta + d)\rho_{ij}^{Q(u\delta_k\beta\Delta+d)}).$$

Thus $\displaystyle\sum_{j=1}^{n_{k-1}} P_{(k-1)j}(u\delta_k\beta\Delta + d)\rho_{(k-1)j}^{Q(u\delta_k\beta\Delta+d)} \to 0$, as $u \to \infty$.

Taking $u = v\delta_{k-1}$, $v \in \mathbb{Z}, v \to \infty$ and $\delta_{k-1} = l.c.m.(\delta_{(k-1)1}, ..., \delta_{(k-1)n_{k-1}})$, then $\displaystyle\sum_{j=1}^{n_{k-1}} P_{(k-1)j}(v\delta_{k-1}\delta_k\beta\Delta + d)\rho_{(k-1)j}^{Q(d)} \to 0$, as $v \to \infty$, so $\displaystyle\sum_{j=1}^{n_{k-1}} P_{(k-1)j}(x)\rho_{(k-1)j}^{Q(d)} = 0$.

Continuing in this fashion, we get $\displaystyle\sum_{j=1}^{n_i} P_{ij}(x)\rho_{ij}^{Q(d)} = 0$ as required. □

Let $F(x) = \displaystyle\sum_{i=0}^{k} A_i^{Q(x)} (\sum_{j=1}^{n_i} P_{ij}(x)\rho_{ij}^{Q(x)}) \in V$, $d \in \mathcal{P}(F, \Delta)$ and $\beta \in \mathbb{N}$. Define $R_{(\beta,d)}(x) = Q'(d)x + \frac{Q''(d)}{2!}x^2\beta\Delta + ... + \frac{Q^{(m)}(d)}{m!}x^m(\beta\Delta)^{m-1}$, abbreviated by $R(x)$.

By hypothesis (Q, Δ, d, β), we mean :

(1) For $J_{k1}, ..., J_{kl_k}$ with $\rho^{\beta\Delta}_{kJ_{kt}} = \eta_{kJ_{kt}} \neq 1$ $(t = 1, ..., l_k)$, assume that there exist integers $j_{k1}, ..., j_{kl_k}$ such that

$$\begin{vmatrix} 1 & 1 & \dots & 1 \\ 1 & \eta_{kJ_{k1}}^{R(j_{k1})} & \dots & \eta_{kJ_{kl_k}}^{R(j_{k1})} \\ \vdots & \vdots & \vdots & \vdots \\ 1 & \eta_{kJ_{k1}}^{R(j_{kl_k})} & \dots & \eta_{kJ_{kl_k}}^{R(j_{kl_k})} \end{vmatrix} \neq 0$$

(2) For $J_{(k-1)1}, ..., J_{(k-1)l_{k-1}}$ with $\rho^{\beta\Delta}_{(k-1)J_{(k-1)t}} = \eta_{(k-1)J_{(k-1)t}} \neq 1$ $(t = 1, ..., l_{k-1})$, assume that there exist integers $j_{(k-1)1}, ..., j_{(k-1)l_{k-1}}$ such that

$$\begin{vmatrix} 1 & 1 & \dots & 1 \\ 1 & \eta_{(k-1)J_{(k-1)1}}^{R(j_{(k-1)1}\delta_k)} & \dots & \eta_{(k-1)J_{(k-1)l_{k-1}}}^{R(j_{(k-1)1}\delta_k)} \\ \vdots & \vdots & \vdots & \vdots \\ 1 & \eta_{(k-1)J_{(k-1)1}}^{R(j_{(k-1)l_{k-1}}\delta_k)} & \dots & \eta_{(k-1)J_{(k-1)l_{k-1}}}^{R(j_{(k-1)l_{k-1}}\delta_k)} \end{vmatrix} \neq 0,$$

where $\delta_k = l.c.m.(\delta_{k1}, ..., \delta_{kn_k})$.

$\vdots$

(k) For $J_{11}, ..., J_{1l_1}$ with $\rho^{\beta\Delta}_{1J_{1t}} = \eta_{1J_{1t}} \neq 1$ $(t = 1, ..., l_1)$, assume that there exist integers $j_{11}, ..., j_{1l_1}$ such that

$$\begin{vmatrix} 1 & 1 & \dots & 1 \\ 1 & \eta_{1J_{11}}^{R(j_{11}\delta_2\cdots\delta_k)} & \dots & \eta_{1J_{1l_1}}^{R(j_{1l_1}\delta_2\cdots\delta_k)} \\ \vdots & \vdots & \vdots & \vdots \\ 1 & \eta_{1J_{11}}^{R(j_{1l_1}\delta_2\cdots\delta_k)} & \dots & \eta_{1J_{1l_1}}^{R(j_{1l_1}\delta_2\cdots\delta_k)} \end{vmatrix} \neq 0$$

Lemma 2.2.2. If $F(x) \in V$ satisfies the hypothesis (Q, Δ, d, β), then for each $i = 1, ..., k$, we have

$$0 = \sum_{\substack{j \\ \rho_{ij}^{\beta\Delta}=1}} P_\rho(x)\rho_{ij}^{Q(d)} \quad (:= \sum_{j \neq J_{it}} P_{ij}(x)\rho_{ij}^{Q(d)}) \quad \text{and} \quad P_{iJ_{i1}}(x) = ... = P_{iJ_{il_i}}(x) = 0$$

Proof. Substituting $x = t\beta\Delta + d$, where $t \in \mathbb{Z}$, we get

$$0 = \frac{F(t\beta\Delta+d)}{A_k^{Q(t\beta\Delta+d)}} = \sum_{i=0}^{k}(\frac{A_i}{A_k})^{Q(t\beta\Delta+d)}(\sum_{j=1}^{n_i} P_{ij}(t\beta\Delta+d)\rho_{ij}^{Q(t\beta\Delta+d)}).$$

Assuming that the leading coefficient of $Q(x)$ is positive ; the other possibility is treated similarly, then $\sum_{j=1}^{n_k} P_{kj}(t\beta\Delta+d)\rho_{kj}^{Q(t\beta\Delta+d)} \to 0$, as $t \to \infty$. Taking $t = u\delta_k + j_{k1}$, where $u \in \mathbb{Z}$ and $\delta_k = l.c.m.(\delta_{k1}, \delta_{k2}, ..., \delta_{kn_k})$, we get

$$\sum_{j=1}^{n_k} P_{kj}((u\delta_k + j_{k1})\beta\Delta + d)\rho_{kj}^{Q((u\delta_k+j_{k1})\beta\Delta+d)}$$

$$= [\sum_{j\neq J_{kt}} P_{kj}((u\delta_k + j_{k1})\beta\Delta + d)\rho_{kj}^{Q(d)}] + [\sum_{j=J_{kt}} P_{kj}((u\delta_k + j_{k1})\beta\Delta + d)\rho_{kj}^{Q(d)}\eta_{kj}^{R(j_{k1})}]$$

$$\to 0, \quad as\ u \to \infty.$$

Being a polynomial tending to 0 as the variable taking arbitrarily large integral values, we deduce that

$$[\sum_{j\neq J_{kt}} P_{kj}(x)\rho_{kj}^{Q(d)}] + [\sum_{j=J_{kt}} P_{kj}(x)\rho_{kj}^{Q(d)}\eta_{kj}^{R(j_{k1})}] = 0.$$

Continuing in this fashion, we obtain

$$[\sum_{j\neq J_{kt}} P_{kj}(x)\rho_{kj}^{Q(d)}]+[\sum_{j=J_{kt}} P_{kj}(x)\rho_{kj}^{Q(d)}\eta_{kj}^{R(j_{k1})}] = 0 \quad (1)$$

$$[\sum_{j\neq J_{kt}} P_{kj}(x)\rho_{kj}^{Q(d)}]+[\sum_{j=J_{kt}} P_{kj}(x)\rho_{kj}^{Q(d)}\eta_{kj}^{R(j_{k2})}] = 0 \quad (2)$$

$$\vdots$$

$$[\sum_{j\neq J_{kt}} P_{kj}(x)\rho_{kj}^{Q(d)}]+[\sum_{j=J_{kt}} P_{kj}(x)\rho_{kj}^{Q(d)}\eta_{kj}^{R(j_{kl_k})}] = 0. \quad (l_k)$$

By Lemma 2.2.1, we also have

$$[\sum_{j\neq J_{kt}} P_{kj}(x)\rho_{kj}^{Q(d)}]+[\sum_{j=J_{kt}} P_{kj}(x)\rho_{kj}^{Q(d)}] = 0. \quad (l_k+1)$$

Since the determinant

$$\begin{vmatrix} 1 & 1 & \dots & 1 \\ 1 & \eta_{kJ_{k1}}^{R(j_{k1})} & \dots & \eta_{kJ_{kl_k}}^{R(j_{k1})} \\ \vdots & \vdots & \vdots & \vdots \\ 1 & \eta_{kJ_{k1}}^{R(j_{kl_k})} & \dots & \eta_{kJ_{kl_k}}^{R(j_{kl_k})} \end{vmatrix} \neq 0,$$

it follows that $\sum_{j \neq J_{kt}} P_{kj}(x)\rho_{kj}^{Q(d)} = 0$ and $P_{kJ_{kt}}(x)\rho_{kJ_{kt}}^{Q(d)} = 0$, i.e. $P_{kJ_{kt}}(x) = 0$ for all $t = 1, ..., l_k$; that is, the result of the lemma holds for $i = k$. Observe that under the hypothesis (Q, Δ, d, β) what we have done above is to reduce the number of terms in the sum representing $F(x)$ by choosing appropriate integral values of x. We now repeat the steps by taking $x = u\delta_k\beta\Delta + d$, $u \in \mathbb{Z}$. Thus

$$0 = \frac{F(u\delta_k\beta\Delta + d)}{A_{k-1}^{Q(u\delta_k\beta\Delta+d)}} = \sum_{i=0}^{k-1}(\frac{A_i}{A_{k-1}})^{Q(u\delta_k\beta\Delta+d)}(\sum_{j=1}^{n_i} P_{ij}(u\delta_k\beta\Delta + d)\rho_{ij}^{Q(j\delta_k\beta\Delta+d)}).$$

Then $\sum_{j=1}^{n_{k-1}} P_{(k-1)j}(u\delta_k\beta\Delta + d)\rho_{(k-1)j}^{Q(u\delta_k\beta\Delta+d)} \to 0$, as $u \to \infty$.

Taking $u = v\delta_{k-1} + j_{(k-1)1}$, where $v \in \mathbb{Z}$ and $\delta_{k-1} = l.c.m.(\delta_{(k-1)1}, ..., \delta_{(k-1)n_{k-1}})$, we get

$$\begin{aligned}
&\sum_{j=1}^{n_{k-1}} P_{(k-1)j}((v\delta_{k-1} + j_{(k-1)1})\delta_k\beta\Delta + d)\rho_{(k-1)j}^{Q((v\delta_{k-1}+j_{(k-1)1})\delta_k\beta\Delta+d)} \\
&= [\sum_{j \neq J_{(k-1)t}} P_{(k-1)j}((v\delta_{k-1} + j_{(k-1)1})\delta_k\beta\Delta + d)\rho_{(k-1)j}^{Q(d)}] + \\
&\quad [\sum_{j = J_{(k-1)t}} P_{(k-1)j}((v\delta_{k-1} + j_{(k-1)1})\delta_k\beta\Delta + d)\rho_{(k-1)j}^{Q(d)}\eta_{(k-1)j}^{R(j_{(k-1)1}\delta_k)}] \\
&\to 0, \quad as\ v \to \infty.
\end{aligned}$$

As polynomials, we infer as above that

$$[\sum_{j \neq J_{(k-1)t}} P_{(k-1)j}(x)\rho_{(k-1)j}^{Q(d)}] + [\sum_{j = J_{(k-1)t}} P_{(k-1)j}(x)\rho_{(k-1)j}^{Q(d)}\eta_{(k-1)j}^{R(j_{(k-1)1}\delta_k)}] = 0,$$

and so

$$[\sum_{j \neq J_{(k-1)t}} P_{(k-1)j}(x)\rho_{(k-1)j}^{Q(d)}] + [\sum_{j = J_{(k-1)t}} P_{(k-1)j}(x)\rho_{(k-1)j}^{Q(d)}\eta_{(k-1)j}^{R(j_{(k-1)1}\delta_k)}] = 0 \qquad (1)$$

$$[\sum_{j \neq J_{(k-1)t}} P_{(k-1)j}(x)\rho_{(k-1)j}^{Q(d)}] + [\sum_{j = J_{(k-1)t}} P_{(k-1)j}(x)\rho_{(k-1)j}^{Q(d)}\eta_{(k-1)j}^{R(j_{(k-1)2}\delta_k)}] = 0 \qquad (2)$$

$$\vdots$$

$$[\sum_{j \neq J_{(k-1)t}} P_{(k-1)j}(x)\rho_{(k-1)j}^{Q(d)}] + [\sum_{j = J_{(k-1)t}} P_{(k-1)j}(x)\rho_{(k-1)j}^{Q(d)}\eta_{(k-1)j}^{R(j_{(k-1)l_{k-1}}\delta_k)}] = 0. \qquad (l_{k-1})$$

$$[\sum_{j\neq J_{(k-1)t}} P_{(k-1)j}(x)\rho_{(k-1)j}^{Q(d)}]+[\sum_{j=J_{(k-1)t}} P_{(k-1)j}(x)\rho_{(k-1)j}^{Q(d)}]=0. \qquad (l_{k-1}+1)$$

Since the determinant

$$\begin{vmatrix} 1 & 1 & \dots & 1 \\ 1 & \eta_{(k-1)J_{(k-1)1}}^{R(j_{(k-1)1}\delta_k)} & \dots & \eta_{(k-1)J_{(k-1)l_{k-1}}}^{R(j_{(k-1)1}\delta_k)} \\ \vdots & \vdots & \vdots & \vdots \\ 1 & \eta_{(k-1)J_{(k-1)1}}^{R(j_{(k-1)l_{k-1}}\delta_k)} & \dots & \eta_{(k-1)J_{(k-1)l_{k-1}}}^{R(j_{(k-1)l_{k-1}}\delta_k)} \end{vmatrix} \neq 0,$$

it follows that $\sum_{j\neq J_{(k-1)t}} P_{(k-1)j}(x)\rho_{(k-1)j}^{Q(d)}=0$ and $P_{(k-1)J_{(k-1)t}}(x)\rho_{(k-1)J_{(k-1)t}}^{Q(d)}=0$ for all $t=1,...,l_{k-1}$, i.e. the result holds for $i=k-1$.

Continuing in this pattern, we get the desired result. □

Lemma 2.2.3. Let $F(x)\in V$, $d\in\mathcal{P}(F,\Delta)$ and $\beta\in\mathbb{N}$. If $F(x)$ satisfies the hypothesis (Q,Δ,d,β), then $F_i^{\beta}(x)=\sum_{j\neq J_{it}} P_{ij}(x)\rho_{ij}^{Q(x)}\in V$, $i=1,...,k$ with a period $\beta\Delta$.

Proof. By Lemma 2.2.2, $\sum_{j\neq J_t} P_{ij}(x)\rho_{ij}^{Q(d)}=0$. Replacing x by $u\beta\Delta+d$, $u\in\mathbb{Z}$, we obtain, for all i, $0=\sum_{j\neq J_t} P_{ij}(u\beta\Delta+d)\rho_{ij}^{Q(d)}=\sum_{j\neq J_t} P_{ij}(u\beta\Delta+d)\rho_{ij}^{Q(u\beta\Delta+d)}=F_i^{\beta}(u\beta\Delta+d)$. □

Lemma 2.2.4. Let $G(x)=[P_1(x)\rho_1^{Q(x)}+P_2(x)\rho_2^{Q(x)}+...+P_n(x)\rho_n^{Q(x)}]A^{Q(x)}$ be an element in V with order of $\rho_i=\delta_i$, $P_i(x)\neq 0$ $(i=1,...,n)$. If $G(x)$ satisfies the hypothesis $(Q,\Delta,d,1)$, then $l.c.m(\delta_1,...,\delta_m)\mid\Delta$ where m is the number of ρ_i's in $G^1(x):=A^{Q(x)}\sum_{j,\rho_j^{\Delta}=1} P_j(x)\rho_j^{Q(x)}$.

Proof. Since $\rho_i^{\Delta}=1$ for all ρ_i in $G^1(x)$, $\delta_i\mid\Delta$ $(i=1,...,m)$, and so $l.c.m.(\delta_1,...,\delta_m)\mid\Delta$. □

Theorem 2.2.5. Let $F(x)\in V$ with the basic period Δ and rank $r(F)$. If $F(x)$ satisfies the hypothesis $(Q,\Delta,d,1)$, then

$$F(x) = \{ \prod_{d \in \mathcal{P}(F,\Delta)} (\eta^{Q(x)} - \eta^{Q(d)}) \} G(x),$$

where η is a primitive Δ-th root of unity and $G(x)$ is a pexponential polynomial.

Proof. Recall that $F(x) = \sum_{i=0}^{k} F_i(x)$, $F_i(x) = A_i^{Q(x)}(\sum_{j=1}^{n_i} P_{ij}(x)\rho_{ij}^{Q(x)})$, and $F_i^1(x) := A_i^{Q(x)}(\sum_{j,\rho_{ij}^{\Delta}=1} P_{ij}(x)\rho_{ij}^{Q(x)}) = A_i^{Q(x)}(\sum_{j \neq J_{it}} (same))$. By Lemma 2.2.2, $F_i(x) = F_i^1(x)$. By Lemma 2.2.3, $F_i(x) = F_i^1(x) \in V$ with a period Δ, and so Lemma 2.2.4 implies $r(F_i^1) \mid \Delta$, i.e. ρ_{ij} is a Δ-root of unity. Rewriting $F_i^1(x)$ as a polynomial in x with exponential coefficients, we have $F_i^1(x) = A_i^{Q(x)}(\sum_t x^t(p_{1_t}\rho_1^{Q(x)} + ... + p_{i_t}\rho_{i_t}^{Q(x)}))$, and $\rho_j^{\Delta} = 1$ $(j = 1, ..., i_t)$. For each $d \in \mathcal{P}(F,\Delta)$ and $u \in \mathbb{Z}$,

$$\begin{aligned} 0 &= F_i^1(u\Delta + d) \\ &= A_i^{Q(u\Delta+d)}(\sum_t (u\Delta + d)^t(p_{1_t}\rho_1^{Q(u\Delta+d)} + ... + p_{i_t}\rho_{i_t}^{Q(u\Delta+d)})) \\ &= A_i^{Q(u\Delta+d)}(\sum_t (u\Delta + d)^t(p_{1_t}\rho_1^{Q(d)} + ... + p_{i_t}\rho_{i_t}^{Q(d)})). \end{aligned}$$

Thus for each i, $p_{1_t}\rho_1^{Q(d)} + ... + p_{i_t}\rho_{i_t}^{Q(d)} = 0$. Let η be a primitive Δ-th root of unity. Then $\rho_j = \eta^{k_j}$ for some $k_j \in \mathbb{N}$. Hence

$$p_{1_t}\eta^{k_1 Q(d)} + ... + p_{i_t}\eta^{k_{i_t} Q(d)} = 0 \quad ;$$

that is, $\eta^{Q(d)}$ is a root of $H_i(y) = p_{1_t}y^{k_1} + ... + p_{i_t}y^{k_{i_t}}$. Thus

$$H_i(y) = \{ \prod_{d \in \mathcal{P}(F,\Delta)} (y - \eta^{Q(d)}) \} G_i(y),$$

where $G_i(y)$ is a polynomial. Hence

$$\begin{aligned} F_i^1(x) &= A_i^{Q(x)}(\sum_t x^t H_i(\eta^{Q(x)})) \\ &= A_i^{Q(x)}(\{ \prod_{d \in \mathcal{P}(F,\Delta)} (\eta^{Q(x)} - \eta^{Q(d)}) \} \sum_t x^t G_i(\eta^{Q(x)})), \end{aligned}$$

and so $F(x) = \{ \prod_{d \in \mathcal{P}(F,\Delta)} (\eta^{Q(x)} - \eta^{Q(d)}) \} (\sum_i A_i^{Q(x)} \sum_t x^t G_i(\eta^{Q(x)}))$. $\square$

REFERENCES

[1] Bezivin, Jean-Paul and V. Laohakosol. *On the theorem of Skolem-Mahler-Lech*. Expo. Math., 9(1991), 89-96.

[2] Ritt, J.F.. *A factorization theory for exponential function*. Trans. Amer. Math. Soc., 52(1927), 584-596.

[3] Shapiro, H.N.. *On a theorem concerning exponential polynomials*. Comm. Pure and Applied Math., 12(1959), 487-500.

VITA

Miss Ouamporn Phuksuwan was born on July 16, 1979 in Bangkok, Thailand. She graduated with a Bachelor Degree of Science in Mathematics from Chulalongkorn University in 2001. Then she got a scholarship from the Ministry Staff Development Project in 2001 to further her study in Mathematics. For her Master degree, she has studied Mathematics at the Faculty of Science, Chulalongkorn University. According to scholarship requirement, she will be a lecturer at the Faculty of Science, Chulalongkorn University.