การแยกตัวประกอบของพหุนาม

นางสาวอัมริสา จันทนะศิริ

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต

สาขาวิชาคณิตศาสตร์ ภาควิชาคณิตศาสตร์

คณะวิทยาศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

ปีการศึกษา 2546

ISBN 974-17-5545-7

FACTORIZATION OF POLYNOMIALS

Miss Amarisa Chantanasiri

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 2003
ISBN 974-17-5545-7

Thesis Title	Factorization of polynomials
By	Miss Amarisa Chantanasiri
Field of Study	Mathematics
Thesis Advisor	Assistant Professor Ajchara Harnchoowong, 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 the Faculty of Science
(Professor Piamsak Menasveta, Ph.D.)

Thesis Committee

.... Chairman
(Assistant Professor Patanee Udomkavanich, Ph.D.)

.... Thesis Advisor
(Assistant Professor Ajchara Harnchoowong, Ph.D.)

.... Thesis Co-advisor
(Associate Professor Vichian Laohakosol, Ph.D.)

.... Member
(Sajee Pianskool, Ph.D.)

อัมริสา จันทนะศิริ : การแยกตัวประกอบของพหุนาม (FACTORIZATION OF POLYNOMIALS) อ.ที่ปรึกษา : ผศ. ดร. อัจฉรา หาญชูวงศ์, อ.ที่ปรึกษาร่วม : รศ. ดร. วิเชียร เลาหโกศล, 105 หน้า. ISBN 974-17-5545-7.

ในปีค.ศ. 1975 - 1976 ออสทรอฟสกี้ตีพิมพ์ผลงานวิจัยอันลึกซึ้งและกว้างขวางในเรื่องการคูณและการแยกตัวประกอบของพหุนาม โดยมีพื้นฐานจากนัยทั่วไปของความคิดเกี่ยวกับพจน์สูงสุดและพจน์ต่ำสุดของพหุนาม ซึ่งเรียกว่าการส่ง Λ จากพหุนามไปยังกลุ่มก้อนสุดขีด

ส่วนแรกของงานวิจัยของออสทรอฟสกี้ พิจารณาการจัดอันดับ Ω ที่เป็นไปได้ทั้งหมดในเซตของผลคูณของกำลังของตัวแปรอิสระภายใต้สัจพจน์ทั่วไป ซึ่งมีหลักการจัดอันดับของพหุนามเป็นกรณีเฉพาะ จากนั้นเป็นการแสดงการสมนัยหนึ่งต่อหนึ่งระหว่าง Ω และ Λ และใช้ความรู้เรื่องฟังก์ชันน้ำหนัก และทรงหลายหน้าแบริกของพหุนามหาการจัดอันดับ Ω ที่เป็นไปได้ทั้งหมด

ส่วนที่สองของงานวิจัยของออสทรอฟสกี้ เป็นการประยุกต์ผลที่ได้จากส่วนแรกไปสู่ปัญหาว่าด้วยการลดทอนไม่ได้ของพหุนาม โดยเฉพาะอย่างยิ่งในกรณีของพหุนามที่มี 2 และ 3 พจน์ ปัญหาว่าด้วยการลดทอนไม่ได้ตอบได้โดยสมบูรณ์ ส่วนกรณีของพหุนามที่มี 4 พจน์ เฉพาะกรณีที่รูปหลายเหลี่ยมแบริกเป็นรูปสามเหลี่ยมเท่านั้นที่มีคำตอบครบถ้วน

งานวิจัยนี้เป็นการศึกษางานวิจัยของออสทรอฟสกี้อย่างละเอียด โดยวิเคราะห์ ให้รายละเอียดเพิ่มเติม พิสูจน์และให้ตัวอย่างที่เกี่ยวเนื่อง และประยุกต์กับปัญหาว่าด้วยการลดทอนไม่ได้ในกรณีของพหุนามที่มี 4 พจน์ที่รูปหลายเหลี่ยมแบริกเป็นรูปสี่เหลี่ยม โดยได้ผลที่สมบูรณ์ในบางกลุ่มของพหุนามดังกล่าว

ภาควิชา **คณิตศาสตร์** ลายมือชื่อนิสิต......อัมริสา...จันทนะศิริ..........
สาขาวิชา **คณิตศาสตร์** ลายมือชื่ออาจารย์ที่ปรึกษา.........................
ปีการศึกษา 2546 ลายมือชื่ออาจารย์ที่ปรึกษาร่วม.........................

4572588123 : MAJOR MATHEMATICS
KEY WORDS : FACTORIZATION / POLYNOMIALS
AMARISA CHANTANASIRI : FACTORIZATION OF POLYNOMIALS.
THESIS ADVISOR : ASSIST. PROF. AJCHARA HARNCHOOWONG, Ph.D.,
THESIS CO-ADVISOR : ASSOC. PROF. VICHIAN LAOHAKOSOL, Ph.D.,
105 pp. ISBN 974-17-5545-7

In 1975-1976, A. Ostrowski published a deep, general and extensive research on multiplication and factorization of polynomials based principally on the generalized notions of highest and lowest terms of a polynomial, called general mappings, Λ, of a polynomial into an extreme aggregate of its terms.

The first part of Ostrowski's works discusses all possible orderings, Ω, in the set of products of powers of independent variables under a very general set of postulates, which contains the usual lexicographical principle as a special case. A one-to-one correspondence between Ω and Λ is established and all realizations of postulates defining Ω are investigated using the ideas of weight functions and the baric polyhedron of a polynomial.

The second part of Ostrowski's works contains applications of the results in the first part to the problem of irreducibility of polynomials. In particular, the cases of 2 and 3 term polynomials are completely determined, while that of 4 term polynomials a complete discussion is only carried out for the case of the baric polygon being a triangle.

In this thesis, we carry out a comprehensive study on the above-mentioned works of Ostrowski by analyzing, clarifying, proving and supplying relevant examples to all his results. In addition, the irreducibility of 4 term polynomials whose baric polygon is a quadrangle is investigated and complete results for some large classes of polynomials are obtained.

Department **Mathematics**
Field of study **Mathematics**
Academic year **2003**

Student's signature ....Amarisa Chantanasiri....
Advisor's signature ....Ajchara Harnchoowong....
Co-advisor's signature ....Vichian Laohakosol....

ACKNOWLEDGEMENTS

I would like to express my profound gratitude and deep appreciation to Assistant Professor Dr. Ajchara Harnchoowong and Associate Professor Dr. Vichian Laohakosol, my thesis advisor and co-advisor, respectively, for their advice and encouragement. Sincere thanks and deep appreciation are also extended to Assistant Professor Dr. Patanee Udomkavanich, the chairman, and Dr. Sajee Pianskool, the committee member, for their comments and suggestions. Finally, I thank all teachers who have taught me all along and Ms. Angkana Sripayap who helps sending me a number of references from abroad.

In particular, I would like to express my deep gratitude to my family and friends for their encouragement throughout my graduate study.

TABLE OF CONTENTS

TABLE OF CONTENTS (Continued)

GLOSSARY OF TERMS

GLOSSARY OF TERMS (Continued)

GLOSSARY OF TERMS (Continued)

GLOSSARY OF TERMS (Continued)

page

CHAPTER I

INTRODUCTION

The problem of factorizing a given polynomial is generally difficult and has been a subject of a great deal of investigations. Yet, till now, there is no particular method capable of identifying whether a given polynomial is reducible.

In 1975-1976, Ostrowski conducted a comprehensive study on multiplication and factorization of polynomials, based on the generalized notion of ordering embracing the Lexicographic Principle for polynomials. Ostrowski also applied his results to the problem of irreducibility of polynomials. This work of Ostrowski is general, deep and noteworthy.

This thesis represents an elaborate study of Ostrowski's work by analyzing, clarifying, proving and providing relevant examples to all above-mentioned results of Ostrowski. In addition, complete determination of the irreducibility of some classes of 4 term polynomials whose baric polygon is a quadrangle, which was not resolved by Ostrowski, is given.

In Chapter II, we define of products of powers, their orderings and discuss all possible orderings Ω of products of powers satisfying a simple set of postulates. Next we introduce a weight function and establish an ordering in the set of products of powers of independent variables by the Lexicographic Principle using a sequence of weight functions. Then we use the concepts of the highest and lowest terms of a polynomial to define of a general mapping, Λ, of a polynomial into an extreme aggregate of its terms. The classical definition of the highest terms is usually given using the Lexicographic Principle. A one-to-one correspondence between all orderings of the type Ω and all mappings of the type Λ is established. However, the same aggregates of extreme terms can be obtained for infinitely many choices of weight functions. In order to obtain a complete picture of all possibilities we introduce the baric polyhedron of a polynomial, which is uniquely determined by this polynomial.

In Chapter III, we apply the concepts and methods developped in Chapter II to the problem of irreducibility of polynomials. In the cases of 2 and 3 term polynomials, the problem can be solved completely. For 4 term polynomials a complete discussion is given only if the baric polygon is a triangle. If the baric polygon is a quadrangle, after simplifying the problem, the irreducibility of certain classes are determined completely.

CHAPTER II

ORDERINGS AND EXTREME AGGREGATES OF TERMS

2.1 Orderings of products of powers

Let $m \geq 1$ and $x_1, \ldots, x_m$ be independent variables. The **product of powers** (denoted by $\boldsymbol{PP}$) of these variables is an expression of the form

$$P := x_1^{\alpha_1} \ldots x_m^{\alpha_m} \tag{2.1}$$

with $\alpha_\mu \in \mathbb{Z}$ $\big(\mu \in \{1, \ldots, m\}\big)$. Such PP will be called **rational**, and a rational PP with $\alpha_\mu \geq 0$ $\big(\mu \in \{1, \ldots, m\}\big)$ will be called **integer**. If $\alpha_\mu = 0$ where $\mu \in \{1, \ldots, m\}$, we may write $x_1^{\alpha_1} \ldots x_m^{\alpha_m} = x_1^{\alpha_1} \ldots x_{\mu-1}^{\alpha_{\mu-1}} x_{\mu+1}^{\alpha_{\mu+1}} \ldots x_m^{\alpha_m}$. If all α_μ $\big(\mu \in \{1, \ldots, m\}\big)$ are $= 0$, we may write $x_1^{\alpha_1} \ldots x_m^{\alpha_m} = 1$. The sum $\alpha_1 + \cdots + \alpha_m$ is called the **dimension** of the PP. In the following, P, P_1, P_2, P_3, P_4 are arbitrary PP's.

A **regular ordering** of PP's is a set, Ω, of binary relations between PP's, denoted by $\sim$, $>$ and $<$ and satisfying the following postulates:

I. There exists the complete disjunction: either $P_1 \sim P_2$ or $P_1 > P_2$ or $P_1 < P_2$.

II. $P_1 \sim P_1$, $(P_1 \sim P_2) \Rightarrow (P_2 \sim P_1)$, $(P_1 > P_2) \Leftrightarrow (P_2 < P_1)$.

III. $\big((P_1 > P_2) \wedge (P_2 \gtrsim P_3)\big) \Rightarrow (P_1 > P_3)$, $\big((P_1 \sim P_2) \wedge (P_2 > P_3)\big) \Rightarrow (P_1 > P_3)$.

IV. $(P_1 > P_2) \Rightarrow (P_3 P_1 > P_3 P_2)$.

From the definition, we derive a number of elementary properties, as follows:

A. $((P_1 < P_2) \wedge (P_2 \lesssim P_3)) \Rightarrow (P_1 < P_3)$, $((P_1 \sim P_2) \wedge (P_2 < P_3)) \Rightarrow (P_1 < P_3)$.

Proof. These follow easily from II and III. □

B. ($\equiv$ III′.) $$((P_1 \sim P_2) \wedge (P_2 \sim P_3)) \Rightarrow (P_1 \sim P_3).$$

Proof. Suppose $P_1 > P_3$. Since $P_3 \sim P_2$, it follows from III that $P_1 > P_2$ which is a contradiction. Similarly, we can disprove $P_1 < P_3$. □

C. ($\equiv$ IV′.) $\quad (P_1 \sim P_2) \Rightarrow (P_3P_1 \sim P_3P_2)$, $(P_1 < P_2) \Rightarrow (P_3P_1 < P_3P_2)$.

Proof. The last assertion follows from II and IV. To show the first assertion, assume that $P_1 \sim P_2$. If $P_3P_1 > P_3P_2$ or $P_3P_1 < P_3P_2$, then, multiply by $1/P_3$, we have $P_1 > P_2$ or $P_1 < P_2$ which is a contradiction. □

D. $\Big(((P_1 > P_2) \wedge (P_3 > P_4)) \vee ((P_1 \sim P_2) \wedge (P_3 > P_4)) \vee ((P_1 > P_2) \wedge (P_3 \sim P_4))\Big) \Rightarrow (P_1P_3 > P_2P_4)$, $((P_1 \sim P_2) \wedge (P_3 \sim P_4)) \Rightarrow (P_1P_3 \sim P_2P_4)$.

Proof. These follow by repeated applications of IV and IV′. □

E. For $p \in \mathbb{N}$, we have $P_1^p > P_2^p$ or $P_1^p \sim P_2^p$ or $P_1^p < P_2^p$, and $P_1^{-p} < P_2^{-p}$ or $P_1^{-p} \sim P_2^{-p}$ or $P_1^{-p} > P_2^{-p}$.

Proof. Let $p \in \mathbb{N}$. Since

$$P_1 > P_2 \text{ or } P_1 \sim P_2 \text{ or } P_1 < P_2, \tag{2.2}$$

by repeated applications of D, it follows that

$$P_1^p > P_2^p \text{ or } P_1^p \sim P_2^p \text{ or } P_1^p < P_2^p. \tag{2.3}$$

Now, multiplying (2.2) by $1/P_1P_2$, we have

$$1/P_1 < 1/P_2 \text{ or } 1/P_1 \sim 1/P_2 \text{ or } 1/P_1 < 1/P_2.$$

By repeated applications of D, it follows again that

$$1/P_1^p < 1/P_2^p \text{ or } 1/P_1^p \sim 1/P_2^p \text{ or } 1/P_1^p < 1/P_2^p, \tag{2.4}$$

i.e. $P_1^{-p} < P_2^{-p}$ or $P_1^{-p} \sim P_2^{-p}$ or $P_1^{-p} > P_2^{-p}$. □

We could define the ordering directly for the field of integer PP's. We have to add to the postulates I - IV the postulate

$$(P_3P_1 > P_3P_2) \Rightarrow (P_1 > P_2),$$

since the invariance with respect to division is no longer contained in IV. Then, obviously, III′ and IV′ are valid again.

Any rational PP (2.1) with partly negative α_μ, can be written as $P = P_1/P_2$ with integer PP's, P_1 and P_2. For integer PP's P_1, P_2, P_3, P_4, define $P_1/P_2 > P_3/P_4$ or $P_1/P_2 \sim P_3/P_4$ or $P_1/P_2 < P_3/P_4$, according as $P_1P_4 > P_2P_3$ or $P_1P_4 \sim P_2P_3$ or $P_1P_4 < P_2P_3$. This definition does not depend on the special choice of P_1, P_2, P_3, P_4. To see this, let $P_1, P_2, P_3, P_4, Q_1, Q_2, Q_3, Q_4$ be integer PP's such that $P_1/P_2 = Q_1/Q_2$ and $P_3/P_4 = Q_3/Q_4$. Then $P_1Q_2 = P_2Q_1$ and $P_3Q_4 = P_4Q_3$. By the above definition and the postulates IV and IV′, we have

$$P_1/P_2 > P_3/P_4 \text{ or } P_1/P_2 \sim P_3/P_4 \text{ or } P_1/P_2 < P_3/P_4$$

$$\Leftrightarrow P_1P_4 > P_2P_3 \text{ or } P_1P_4 \sim P_2P_3 \text{ or } P_1P_4 < P_2P_3$$

$$\Leftrightarrow Q_1Q_4P_1P_4 > Q_1Q_4P_2P_3 \text{ or } Q_1Q_4P_1P_4 \sim Q_1Q_4P_2P_3 \text{ or } Q_1Q_4P_1P_4 < Q_1Q_4P_2P_3$$

$$\Leftrightarrow Q_1Q_4P_1P_4 > Q_2Q_3P_1P_4 \text{ or } Q_1Q_4P_1P_4 \sim Q_2Q_3P_1P_4 \text{ or } Q_1Q_4P_1P_4 < Q_2Q_3P_1P_4$$

$$\Leftrightarrow Q_1Q_4 > Q_2Q_3 \text{ or } Q_1Q_4 \sim Q_2Q_3 \text{ or } Q_1Q_4 < Q_2Q_3$$
$$\Leftrightarrow Q_1/Q_2 > Q_3/Q_4 \text{ or } Q_1/Q_2 \sim Q_3/Q_4 \text{ or } Q_1/Q_2 < Q_3/Q_4.$$

We see now easily that all postulates I - IV, III′, IV′ remain valid in the field of rational PP's. Thus once we have the ordering for the field of integer PP's, we can define the ordering for the field of rational PP's.

We consider now the PP (2.1) with $\alpha_\mu \in \mathbb{Q}$ $\big(\mu \in \{1, \ldots, m\}\big)$. Such PP will be called **algebraic**. The set of these PP's will be denoted by $[x_1, \ldots, x_m]$.

In order to define our relations for the algebraic PP's,

$$P_1 := x_1^{\alpha_1} \ldots x_m^{\alpha_m},\ P_2 := x_1^{\beta_1} \ldots x_m^{\beta_m},$$

let M be the smallest common denominator of all α_μ and β_μ. If P_1 and P_2 are rational PP's, we take M as 1. Then we define $P_1 > P_2$ or $P_1 \sim P_2$ or $P_1 < P_2$, according as $P_1^M > P_2^M$ or $P_1^M \sim P_2^M$ or $P_1^M < P_2^M$.

Let $N \in \mathbb{N}$ be such that both P_1^N and P_2^N are rational PP's. Then $N = pM$ for some $p \in \mathbb{N}$. By E, it follows that $P_1^N > P_2^N$ or $P_1^N \sim P_2^N$ or $P_1^N < P_2^N$, according as $P_1^M > P_2^M$ or $P_1^M \sim P_2^M$ or $P_1^M < P_2^M$. Thus by the above definition, we have that from any of the relations between P_1 and P_2 follows the corresponding relation between P_1^N and P_2^N.

We see now easily that all postulates I - IV are satisfied for our ordering in the field of algebraic PP's. Moreover, for any $p \in \mathbb{Q}^+$, from any of the relations (2.2) between algebraic PP's, P_1 and P_2, follow the corresponding relations in (2.3) and (2.4).

From now on, we will consider generally the algebraic PP's unless otherwise specified. Further, all exponents which will occur in the following,

will be assumed to be rational numbers, unless otherwise specified.

Any ordering of algebraic PP's satisfying the postulates I - IV will be called a **regular ordering**.

Now, we will apply a **multiplicative reversible transformation** (m-r-transformation) with $a_{\mu\nu} \in \mathbb{Q}$ $\big(\mu, \nu \in \{1, \ldots, m\}\big)$ such that $\det[a_{\mu\nu}] \neq 0$:

$$x_\mu = y_1^{a_{\mu 1}} \ldots y_m^{a_{\mu m}} \quad \big(\mu \in \{1, \ldots, m\}\big).$$

Then each PP (2.1) becomes

$$y_1^{\beta_1} \ldots y_m^{\beta_m},$$

where $\beta_\nu = a_{1\nu}\alpha_1 + \cdots + a_{m\nu}\alpha_m \in \mathbb{Q}$ $\big(\nu \in \{1, \ldots, m\}\big)$, which is an algebraic PP from $[y_1, \ldots, y_m]$. For $\mu \in \{1, \ldots, m\}$, since $x_\mu = y_1^{a_{\mu 1}} \ldots y_m^{a_{\mu m}}$, $\log x_\mu = a_{\mu 1} \log y_1 + \cdots + a_{\mu m} \log y_m$, then

$$\begin{bmatrix} \log x_1 \\ \vdots \\ \log x_m \end{bmatrix} = [a_{\mu\nu}] \begin{bmatrix} \log y_1 \\ \vdots \\ \log y_m \end{bmatrix}.$$

Let $[b_{\mu\nu}] := [a_{\mu\nu}]^{-1}$. Then

$$\begin{bmatrix} \log y_1 \\ \vdots \\ \log y_m \end{bmatrix} = [b_{\mu\nu}] \begin{bmatrix} \log x_1 \\ \vdots \\ \log x_m \end{bmatrix}.$$

For $\mu \in \{1, \ldots, m\}$, $\log y_\mu = b_{\mu 1} \log x_1 + \cdots + b_{\mu m} \log x_m$, so $y_\mu = x_1^{b_{\mu 1}} \ldots x_m^{b_{\mu m}}$ which is an algebraic PP from $[x_1, \ldots, x_m]$.

Let $P_1 := x_1^{\alpha_1} \ldots x_m^{\alpha_m}$ and $P_2 := x_1^{\beta_1} \ldots x_m^{\beta_m}$ be any algebraic PP's from $[x_1, \ldots, x_m]$.

After applying the above m-r-transformation, we have

$P_1 = y_1^{a_{11}\alpha_1+\cdots+a_{m1}\alpha_m} \dots y_m^{a_{1m}\alpha_1+\cdots+a_{mm}\alpha_m}$, $P_2 = y_1^{a_{11}\beta_1+\cdots+a_{m1}\beta_m} \dots y_m^{a_{1m}\beta_1+\cdots+a_{mm}\beta_m}$. Observe that any of the relations between P_1 and P_2 is invariant as P_1 and P_2 are considered to be algebraic PP's from $[y_1, \dots, y_m]$. Let M be the smallest common denominator of all $a_{1\nu}\alpha_1 + \cdots + a_{m\nu}\alpha_m$ and $a_{1\nu}\beta_1 + \cdots + a_{m\nu}\beta_m$. By E, $P_1^M > P_2^M$ or $P_1^M \sim P_2^M$ or $P_1^M < P_2^M$, according as $P_1 > P_2$ or $P_1 \sim P_2$ or $P_1 < P_2$.

2.2 Weight functions

A function $W : [x_1, \dots, x_m] \to \mathbb{R}$ is called a **weight function** if for P_1 and P_2 from $[x_1, \dots, x_m]$,

$$W(P_1P_2) = W(P_1) + W(P_2).$$

It follows that $W(1) = 0$ and for any PP P and $\alpha \in \mathbb{Q}$, we have $W(P^\alpha) = \alpha W(P)$. If we put $w_\mu := W(x_\mu)$ $\big(\mu \in \{1, \dots, m\}\big)$, we obtain

$$\begin{aligned} W(x_1^{\alpha_1} \dots x_m^{\alpha_m}) &= W(x_1^{\alpha_1}) + \cdots + W(x_m^{\alpha_m}) \\ &= \alpha_1 W(x_1) + \cdots + \alpha_m W(x_m) \\ &= w_1\alpha_1 + \cdots + w_m\alpha_m. \end{aligned} \tag{2.5}$$

This shows that we can define any weight function by (2.5) choosing $w_1, \dots, w_m$ as arbitrary real numbers. If $w_\mu \in \mathbb{Q}$ $\big(\mu \in \{1, \dots, m\}\big)$, $W(P)$ is called a **rational weight function**.

Example 2.2.1. 1) The weight function given by the **dimension**:

$$w_1 = \cdots = w_m = 1.$$

2) The weight function given by the **degree in x_1**:

$$w_1 = 1,\ w_2 = \cdots = w_m = 0.$$

3) The weight function given by the **classical weight in the theory of symmetric functions**:

$$w_1 = 1,\ w_2 = 2, \ldots,\ w_m = m.$$

Proposition 2.2.2. If r is the maximal number of the w_μ in (2.5) which are linearly independent with respect to $\mathbb{Q}$, then $W(P)$ in (2.5) can be represented in the form

$$W(P) = \sum_{\rho=1}^{r} w^{(\rho)} W^{(\rho)}(P) \tag{2.6}$$

where $w^{(\rho)}$ $\big(\rho \in \{1, \ldots, r\}\big)$ are linearly independent real numbers chosen from $w_1, \ldots, w_m$ and $W^{(\rho)}(P)$ $\big(\rho \in \{1, \ldots, r\}\big)$ are r rational weight functions which are linearly independent as linear forms in $\alpha_1, \ldots, \alpha_m$. The number r will be called the **rank** of the weight function $W(P)$.

Proof. From the assumption, we have $w^{(1)}, \ldots, w^{(r)}$ are linearly independent with respect to $\mathbb{Q}$ and there are $k_{ij} \in \mathbb{Q}$ $\big(i \in \{1, \ldots, m-r\},\ j \in \{1, \ldots, r\}\big)$, not all zero, such that

$$\begin{aligned} w^{(r+1)} &= k_{11} w^{(1)} + \cdots + k_{1r} w^{(r)}, \\ &\vdots \\ w^{(m)} &= k_{(m-r)1} w^{(1)} + \cdots + k_{(m-r)r} w^{(r)}. \end{aligned}$$

It follows that

$$\begin{aligned}W(P) &= w^{(1)}\alpha^{(1)} + \cdots + w^{(m)}\alpha^{(m)} \\ &= w^{(1)}\alpha^{(1)} + \cdots + w^{(r)}\alpha^{(r)} + (k_{11}w^{(1)} + \cdots + k_{1r}w^{(r)})\alpha^{(r+1)} \\ &\quad + \cdots + (k_{(m-r)1}w^{(1)} + \cdots + k_{(m-r)r}w^{(r)})\alpha^{(m)} \\ &= w^{(1)}(\alpha^{(1)} + k_{11}\alpha^{(r+1)} + \cdots + k_{(m-r)1}\alpha^{(m)}) \\ &\quad + \cdots + w^{(r)}(\alpha^{(r)} + k_{1r}\alpha^{(r+1)} + \cdots + k_{(m-r)r}\alpha^{(m)}),\end{aligned}$$

where $\{\alpha^{(1)}, \ldots, \alpha^{(m)}\}$ is the same set of $\{\alpha_1, \ldots, \alpha_m\}$ but ordered appropriately.
Define

$$\left.\begin{aligned}W^{(1)}(P) &:= \alpha^{(1)} + k_{11}\alpha^{(r+1)} + \cdots + k_{(m-r)1}\alpha^{(m)}, \\ &\ \vdots \\ W^{(r)}(P) &:= \alpha^{(r)} + k_{1r}\alpha^{(r+1)} + \cdots + k_{(m-r)r}\alpha^{(m)}.\end{aligned}\right\} \tag{2.7}$$

We see that $W^{(\rho)}(P)$ $\left(\rho \in \{1, \ldots, r\}\right)$ are rational weight functions and $W(P) = \sum_{\rho=1}^{r} w^{(\rho)}W^{(\rho)}(P)$. Finally, we show that $W^{(\rho)}(P)$ $\left(\rho \in \{1, \ldots, r\}\right)$ are linearly independent as linear forms in $\alpha_1, \ldots, \alpha_m$. Suppose there exist $a_1, \ldots, a_r \in \mathbb{Q}$ such that $a_1W^{(1)}(P) + \cdots + a_rW^{(r)}(P) = 0$. Then $a_1\alpha^{(1)} + \cdots + a_r\alpha^{(r)} + (a_1k_{11} + \cdots + a_rk_{1r})\alpha^{(r+1)} + \cdots + (a_1k_{(m-r)1} + \cdots + a_rk_{(m-r)r})\alpha^{(m)} = 0$. As $\alpha_1, \ldots, \alpha_m$ are indeterminates, we get $a_1 = \cdots = a_r = 0$. Thus $W^{(\rho)}(P)$ $\left(\rho \in \{1, \ldots, r\}\right)$ are linearly independent as linear forms in $\alpha_1, \ldots, \alpha_m$. □

From Proposition 2.2.2, for any PP P, if $W(P) = 0$, since $w^{(1)}, \ldots, w^{(r)}$ are linearly independent with respect to $\mathbb{Q}$ and $W^{(\rho)}(P)$ $\left(\rho \in \{1, \ldots, r\}\right)$ are rational weight functions, it follows that $W^{(\rho)}(P) = 0$ $\left(\rho \in \{1, \ldots, r\}\right)$.

Proposition 2.2.3. Let r be as in Proposition 2.2.2. Then there exist $m - r$ PP's, $P^{(1)}, \ldots, P^{(m-r)}$ such that for any PP P with $W(P) = 0$, $P = P^{(1)u_1} \ldots P^{(m-r)u_{m-r}}$, where $u_1, \dots, u_{m-r} \in \mathbb{Q}$ and $W(P^{(1)}) = \cdots = W(P^{(m-r)}) = 0$.

Proof. For $\rho \in \{1, \dots, r\}$, let $x^{(\rho)}$ be the independent variable corresponding to the $w^{(\rho)}$ as stated in Proposition 2.2.2.

Choose

$$\begin{aligned} P^{(1)} &:= x^{(1)(-k_{11})} \dots x^{(r)(-k_{1r})} x^{(r+1)}, \\ &\vdots \\ P^{(m-r)} &:= x^{(1)(-k_{(m-r)1})} \dots x^{(r)(-k_{(m-r)r})} x^{(m)}, \end{aligned}$$

where k_{ij} $\big(i \in \{1, \dots, m-r\},\ j \in \{1, \dots, r\}\big)$ are as in Proposition 2.2.2.

Let $P := x_1^{\alpha_1} \dots x_m^{\alpha_m}$ be a PP such that $W(P) = 0$. Then $W^{(\rho)}(P) = 0$ $\big(\rho \in \{1, \dots, r\}\big)$. By (2.7), we have

$$\begin{aligned} \alpha^{(1)} &= -k_{11}\alpha^{(r+1)} - \cdots - k_{(m-r)1}\alpha^{(m)}, \\ &\vdots \\ \alpha^{(r)} &= -k_{1r}\alpha^{(r+1)} - \cdots - k_{(m-r)r}\alpha^{(m)}. \end{aligned}$$

Thus

$$\begin{aligned} P &= x_1^{\alpha_1} \dots x_m^{\alpha_m} = x^{(1)\alpha^{(1)}} \dots x^{(m)\alpha^{(m)}} \\ &= x^{(1)(-k_{11}\alpha^{(r+1)} - \cdots - k_{(m-r)1}\alpha^{(m)})} \dots x^{(r)(-k_{1r}\alpha^{(r+1)} - \cdots - k_{(m-r)r}\alpha^{(m)})} x^{(r+1)\alpha^{(r+1)}} \dots x^{(m)\alpha^{(m)}} \\ &= \big(x^{(1)(-k_{11})} \dots x^{(r)(-k_{1r})} x^{(r+1)}\big)^{\alpha^{(r+1)}} \dots \big(x^{(1)(-k_{(m-r)1})} \dots x^{(r)(-k_{(m-r)r})} x^{(m)}\big)^{\alpha^{(m)}}. \end{aligned}$$

Let $u_1 := \alpha^{(r+1)}, \dots, u_{(m-r)} := \alpha^{(m)}$. Then $P = P^{(1)u_1} \dots P^{(m-r)u_{m-r}}$.

By (2.7), it follows that

$$W^{(1)}(P^{(1)}) = W^{(1)}(x^{(1)(-k_{11})} \dots x^{(r)(-k_{1r})} x^{(r+1)}) = -k_{11} + k_{11} = 0,$$

$$\vdots$$

$$W^{(r)}(P^{(1)}) = W^{(r)}(x^{(1)(-k_{11})} \dots x^{(r)(-k_{1r})} x^{(r+1)}) = -k_{1r} + k_{1r} = 0.$$

By (2.6), we have that $W(P^{(1)}) = \sum_{\rho=1}^{r} w^{(\rho)} W^{(\rho)}(P^{(1)}) = 0$. Similarly, we have also that $W(P^{(2)}) = \cdots = W(P^{(m-r)}) = 0$. □

Proposition 2.2.4. Let $W^*(P)$ be a rational weight function which has the property that for any PP P, if $W(P) = 0$, then $W^*(P) = 0$. Then $W^*(P)$ is a $\mathbb{Q}$-linear combination of $W^{(1)}(P), \dots, W^{(r)}(P)$.

Proof. Let r and k_{ij} $\big(i \in \{1, \dots, m-r\},\ j \in \{1, \dots, r\}\big)$ be as in Proposition 2.2.2. Put $a_1 := W^*(x^{(1)}), \dots, a_r := W^*(x^{(r)})$ and $b_1 := -k_{11}W^*(x^{(1)}) - \cdots - k_{1r}W^*(x^{(r)}) + W^*(x^{(r+1)}), \dots, b_{m-r} := -k_{(m-r)1}W^*(x^{(1)}) - \cdots - k_{(m-r)r}W^*(x^{(r)}) + W^*(x^{(m)})$. Note that $a_j, b_i \in \mathbb{Q}$ $\big(i \in \{1, \dots, m-r\},\ j \in \{1, \dots, r\}\big)$ since $W^*(P)$ is a rational weight function. For $P := x_1^{\alpha_1} \dots x_m^{\alpha_m} = x^{(1)\alpha^{(1)}} \dots x^{(m)\alpha^{(m)}}$, by (2.7), we have

$$\begin{aligned}
W^*(P) &= \alpha^{(1)}W^*(x^{(1)}) + \cdots + \alpha^{(r)}W^*(x^{(r)}) + \alpha^{(r+1)}W^*(x^{(r+1)}) \\
&\quad + \cdots + \alpha^{(m)}W^*(x^{(m)}) \\
&= \big(W^{(1)}(P) - k_{11}\alpha^{(r+1)} - \cdots - k_{(m-r)1}\alpha^{(m)}\big)W^*(x^{(1)}) \\
&\quad + \cdots + \big(W^{(r)}(P) - k_{1r}\alpha^{(r+1)} - \cdots - k_{(m-r)r}\alpha^{(m)}\big)W^*(x^{(r)}) \\
&\quad + \alpha^{(r+1)}W^*(x^{(r+1)}) + \cdots + \alpha^{(m)}W^*(x^{(m)}) \\
&= W^*(x^{(1)})W^{(1)}(P) + \cdots + W^*(x^{(r)})W^{(r)}(P) \\
&\quad + \big(-k_{11}W^*(x^{(1)}) - \cdots - k_{1r}W^*(x^{(r)}) + W^*(x^{(r+1)})\big)\alpha^{(r+1)} \\
&\quad + \cdots + \big(-k_{(m-r)1}W^*(x^{(1)}) - \cdots - k_{(m-r)r}W^*(x^{(r)}) + W^*(x^{(m)})\big)\alpha^{(m)} \\
&= a_1W^{(1)}(P) + \cdots + a_rW^{(r)}(P) + b_1\alpha^{(r+1)} + \cdots + b_{m-r}\alpha^{(m)}.
\end{aligned}$$

From Proposition 2.2.3, $W(P^{(1)}) = \cdots = W(P^{(m-r)}) = 0$. It follows from Proposition 2.2.2 that $W^{(\rho)}(P^{(1)}) = \cdots = W^{(\rho)}(P^{(m-r)}) = 0$ $\big(\rho \in \{1, \dots, r\}\big)$ and by the hypothesis that $W^*(P^{(1)}) = \cdots = W^*(P^{(m-r)}) = 0$. Then

$$0 = W^*(P^{(1)}) = W^*(x^{(1)(-k_{11})} \dots x^{(r)(-k_{1r})} x^{(r+1)}) = b_1,$$
$$\vdots$$
$$0 = W^*(P^{(m-r)}) = W^*(x^{(1)(-k_{(m-r)1})} \dots x^{(r)(-k_{(m-r)r})} x^{(m)}) = b_{m-r}.$$

Thus $W^*(P) = a_1 W^{(1)}(P) + \cdots + a_r W^{(r)}(P)$. □

The rational weight function $W^*(P)$ which has the property that for any *PP* P, if $W(P) = 0$, then $W^*(P) = 0$ will be called **belonging to *W(P)***. From Proposition 2.2.4, it follows that the set of all rational weight functions belonging to $W(P)$ is identical with the set of all $\mathbb{Q}$-linear combinations of $W^{(1)}(P), \dots, W^{(r)}(P)$. Thus the set of all rational weight functions belonging to $W(P)$ is uniquely determined by $W(P)$.

Consider now an ordered sequence of weight functions

$$W_\kappa(x_1^{\alpha_1} \dots x_m^{\alpha_m}) := \sum_{\mu=1}^{m} w_\mu^{(\kappa)} \alpha_\mu \quad \big(\kappa \in \{1, \dots, k\}\big). \tag{2.8}$$

Using the sequence (2.8), a regular ordering Ω of *PP*'s can he **induced by** the **Principle of Lexicographic Ordering**, postulating that $P_1 \sim P_2$ if $W_\kappa(P_1) = W_\kappa(P_2)\big(\kappa \in \{1, \dots, k\}\big)$, and that $P_1 > P_2$ if there exists $k_0 \in \{1, \dots, k\}$ such that $W_\kappa(P_1) = W_\kappa(P_2)$ $(\kappa < k_0)$ and $W_{k_0}(P_1) > W_{k_0}(P_2)$. Then $P_1 < P_2$ if there exists $k_0 \in \{1, \dots, k\}$ such that $W_\kappa(P_1) = W_\kappa(P_2)$ $(\kappa < k_0)$ and $W_{k_0}(P_1) < W_{k_0}(P_2)$. Properties I, II, III follow immediately. To show property IV, let P_1, P_2, P_3 be arbitrary *PP*'s. Assume that $P_1 > P_2$. Then there exists $k_0 \in \{1, \dots, k\}$ such that

$W_\kappa(P_1) = W_\kappa(P_2)$ ($\kappa < k_0$) and $W_{k_0}(P_1) > W_{k_0}(P_2)$. Note that for $\kappa \in \{1, \ldots, k\}$, $W_\kappa(P_3P_1) - W_\kappa(P_3P_2) = \big(W_\kappa(P_3) + W_\kappa(P_1)\big) - \big(W_\kappa(P_3) + W_\kappa(P_2)\big) = W_\kappa(P_1) - W_\kappa(P_2)$. It follows that $W_\kappa(P_3P_1) - W_\kappa(P_3P_2) = W_\kappa(P_1) - W_\kappa(P_2) = 0$ ($\kappa < k_0$), i.e. $W_\kappa(P_3P_1) = W_\kappa(P_3P_2)$ ($\kappa < k_0$), and $W_{k_0}(P_3P_1) - W_{k_0}(P_3P_2) = W_{k_0}(P_1) - W_{k_0}(P_2) > 0$, i.e. $W_{k_0}(P_3P_1) > W_{k_0}(P_3P_2)$. Thus $P_3P_1 > P_3P_2$.

We see that the weight functions and the ordering defined above by means of weight functions are invariant if we apply an m-r-transformation of coordinates.

For the case $m = 1$, by (2.5), we have that any weight function is of the form $W(x_1^{\alpha_1}) = w_1\alpha_1$ where $w_1 \in \mathbb{R}$. Assume that $w_1 \neq 0$. Then for any $\alpha_1, \beta_1 \in \mathbb{Q}$, $W(x_1^{\alpha_1}) = W(x_1^{\beta_1}) \Leftrightarrow w_1\alpha_1 = w_1\beta_1 \Leftrightarrow \alpha_1 = \beta_1$. Thus any sequence of weight functions $W_1(P), \ldots, W_k(P)$ which induces a regular ordering of $[x_1]$ could be replaced by the sequence $W_{k_0}(P)$ where $k_0 = \min\{\kappa \in \{1, \ldots, k\} \mid W_\kappa(P) \not\equiv 0\}$ if there exists $\kappa \in \{1, \ldots, k\}$ such that $W_\kappa(P) \not\equiv 0$. Let Ω be the regular ordering of $[x_1]$ induced by the weight function $W(x_1^{\alpha_1}) := w_1\alpha_1$ where $w_1 \in \mathbb{R}$. For $w_1 = 0$, we have $W(x_1^{\alpha_1}) \equiv 0$. Then there is no ordering at all. We may assume that $w_1 \neq 0$. So $x_1^{\alpha_1} \sim x_1^{\beta_1} \Leftrightarrow W(x_1^{\alpha_1}) = W(x_1^{\beta_1}) \Leftrightarrow w_1\alpha_1 = w_1\beta_1 \Leftrightarrow \alpha_1 = \beta_1 \Leftrightarrow x_1^{\alpha_1} = x_1^{\beta_1}$. If $w_1 > 0$, then $x_1^{\alpha_1} > x_1^{\beta_1} \Leftrightarrow W(x_1^{\alpha_1}) > W(x_1^{\beta_1}) \Leftrightarrow w_1\alpha_1 > w_1\beta_1 \Leftrightarrow \alpha_1 > \beta_1$, and dually, $x_1^{\alpha_1} < x_1^{\beta_1} \Leftrightarrow \alpha_1 < \beta_1$. Similarly, if $w_1 < 0$, then $x_1^{\alpha_1} > x_1^{\beta_1} \Leftrightarrow W(x_1^{\alpha_1}) > W(x_1^{\beta_1}) \Leftrightarrow w_1\alpha_1 > w_1\beta_1 \Leftrightarrow \alpha_1 < \beta_1$, and dually, $x_1^{\alpha_1} < x_1^{\beta_1} \Leftrightarrow \alpha_1 > \beta_1$. Hence there are two possible regular orderings of $[x_1]$.

Proposition 2.2.5. The sequence (2.8) of weight functions allows the following transformations which do not change the ordering Ω.

A. Any weight function in (2.8) can be multiplied by any positive constant.

B. Any weight function $W_{\kappa'}(P)$ in (2.8) can be replaced with

$$\bar{W}_{\kappa'}(P) := W_{\kappa'}(P) + \sum_{\kappa<\kappa'} c_\kappa W^*_\kappa(P),$$

with arbitrary c_κ where each $W^*_\kappa(P)$ is a rational weight function belonging to $W_\kappa(P)$.

C. A weight function which is $\equiv 0$ can be dropped from the sequence (2.8), if we do not change the order of the remaining elements of (2.8).

Proof. A and C are clear. To show B, let P_1, P_2 be arbitrary PP's and $\kappa' \in \{1, \ldots, k\}$. Replace $W_{\kappa'}(P)$ in (2.8) with $\bar{W}_{\kappa'}(P)$. Then (2.8) becomes

$$W_1(P), \ldots, W_{\kappa'-1}(P), \bar{W}_{\kappa'}(P), W_{\kappa'+1}(P), \ldots, W_k(P). \tag{2.9}$$

If $P_1 \sim P_2$ with respect to (2.8), then $W_\kappa(P_1) = W_\kappa(P_2)$ $\big(\kappa \in \{1, \ldots, k\}\big)$, so $W_\kappa(P_1 P_2^{-1}) = W_\kappa(P_1) - W_\kappa(P_2) = 0$ $\big(\kappa \in \{1, \ldots, k\}\big)$. Since each $W^*_\kappa(P)$ is belonging to $W_\kappa(P)$, $W^*_\kappa(P_1 P_2^{-1}) = 0$ $(\kappa < \kappa')$, yielding $W^*_\kappa(P_1) = W^*_\kappa(P_2)$ $(\kappa < \kappa')$. Then $\bar{W}_{\kappa'}(P_1) = W_{\kappa'}(P_1) + \sum_{\kappa<\kappa'} c_\kappa W^*_\kappa(P_1) = W_{\kappa'}(P_2) + \sum_{\kappa<\kappa'} c_\kappa W^*_\kappa(P_2) = \bar{W}_{\kappa'}(P_2)$. Thus $P_1 \sim P_2$ with respect to (2.9). Next, if $P_1 > P_2$ with respect to (2.8), then there exists $k_0 \in \{1, \ldots, k\}$ such that $W_\kappa(P_1) = W_\kappa(P_2)$ $(\kappa < k_0)$ and $W_{k_0}(P_1) > W_{k_0}(P_2)$, so $W_\kappa(P_1 P_2^{-1}) = W_\kappa(P_1) - W_\kappa(P_2) = 0$ $(\kappa < k_0)$. Since each $W^*_\kappa(P)$ is belonging to $W_\kappa(P)$, $W^*_\kappa(P_1 P_2^{-1}) = 0$ $(\kappa < k_0)$, yielding $W^*_\kappa(P_1) = W^*_\kappa(P_2)$ $(\kappa < k_0)$. If $\kappa' > k_0$, it follows immediately from $W_{k_0}(P_1) > W_{k_0}(P_2)$ that $P_1 > P_2$ with respect to (2.9). If $\kappa' < k_0$, then $W_{\kappa'}(P_1) = W_{\kappa'}(P_2)$ and $\sum_{\kappa<\kappa'} c_\kappa W^*_\kappa(P_1) = \sum_{\kappa<\kappa'} c_\kappa W^*_\kappa(P_2)$, implying $\bar{W}_{\kappa'}(P_1) = \bar{W}_{\kappa'}(P_2)$. This together with $W_{k_0}(P_1) > W_{k_0}(P_2)$ show that $P_1 > P_2$ with respect to (2.9). If $\kappa' = k_0$, then $W_{\kappa'}(P_1) > W_{\kappa'}(P_2)$ and $\sum_{\kappa<\kappa'} c_\kappa W^*_\kappa(P_1) = \sum_{\kappa<\kappa'} c_\kappa W^*_\kappa(P_2)$, implying $\bar{W}_{\kappa'}(P_1) > \bar{W}_{\kappa'}(P_2)$. Thus $P_1 > P_2$ with respect to (2.9). The proof is similar for $P_1 < P_2$. □

Now we reduce the sequence (2.8) by using Proposition 2.2.5. By Proposition 2.2.5 C, we can assume that any weight function in (2.8) is $\not\equiv 0$. By Proposition 2.2.2, we have rational weight functions

$$W_1^{(1)}(P), \ldots, W_1^{(r_1)}(P) \tag{2.10}$$

belonging to $W_1(P)$ which are linearly independent as linear forms in $\alpha_1, \ldots, \alpha_m$ and $W_1(P) = \sum_{\rho=1}^{r_1} w_1^{(\rho)} W_1^{(\rho)}(P)$. If $r_1 < m$, by Proposition 2.2.2, we have again rational weight functions $W_2^{(1)}(P), \ldots, W_2^{(r_2)}(P)$ belonging to $W_2(P)$ which are linearly independent as linear forms in $\alpha_1, \ldots, \alpha_m$ and $W_2(P) = \sum_{\rho=1}^{r_2} w_2^{(\rho)} W_2^{(\rho)}(P)$. Then add to the sequence (2.10), $W_2^{(\rho)}(P)$, such that each time when we add, rational weight functions in the obtained sequence are still linearly independent as linear forms in $\alpha_1, \ldots, \alpha_m$. Assume that we add s_2 rational weight functions to (2.10). If $r_1 + s_2 < m$, then continue this process by considering $W_3(P), \ldots, W_k(P)$ until the number of rational weight functions in the obtained sequence is m or we have considered all cases. Suppose that we obtain the sequence:

$$W_1^{(1)}(P), \ldots, W_1^{(r_1)}(P), W_2^{(\rho_{21})}(P), \ldots, W_2^{(\rho_{2s_2})}(P), \ldots, W_l^{(\rho_{l1})}(P), \ldots, W_l^{(\rho_{ls_l})}(P).$$

Define

$$\bar{W}_1(P) := W_1(P) = \sum_{\rho=1}^{r_1} w_1^{(\rho)} W_1^{(\rho)}(P),$$

$$\bar{W}_2(P) := w_2^{(\rho_{21})} W_2^{(\rho_{21})}(P) + \cdots + w_2^{(\rho_{2s_2})} W_2^{(\rho_{2s_2})}(P),$$

$$\vdots$$

$$\bar{W}_l(P) := w_l^{(\rho_{l1})} W_l^{(\rho_{l1})}(P) + \cdots + w_l^{(\rho_{ls_l})} W_l^{(\rho_{ls_l})}(P).$$

We can write $\bar{W}_2(P)$ in the form $W_2(P) + \sum_{\rho=1}^{r_1} c_2^{(\rho)} W_1^{(\rho)}(P)$ where $c_2^{(\rho)} \in \mathbb{R}$ $\big(\rho \in \{1,\ldots,r_1\}\big)$. For $\kappa' \in \{3,\ldots,l\}$, we can write $\bar{W}_{\kappa'}(P)$ in the form $W_{\kappa'}(P) + \sum_{\kappa<\kappa'} c_\kappa^{(\kappa')} W_\kappa^{(\kappa')}(P)$, where $c_\kappa^{(\kappa')} \in \mathbb{R}$ and each $W_\kappa^{(\kappa')}(P)$ is a rational weight function belonging to $W_\kappa(P)$. By Proposition 2.2.5 B, the sequence (2.8) can be replaced by

$$\bar{W}_1(P), \bar{W}_2(P), \ldots, \bar{W}_l(P). \tag{2.11}$$

The sequence (2.11) is called **regular**. Note that the sum of the ranks of all weight functions in (2.11) is $= r_1 + s_2 + \cdots + s_l \leq m$. We will show that this sum is $= m$ if and only if the only PP which is ~ 1 is 1. First, assume that the sum of the ranks of $\bar{W}_1(P), \bar{W}_2(P), \ldots, \bar{W}_l(P)$ is $= m$. Let $P := x_1^{\alpha_1} \ldots x_m^{\alpha_m}$ be a PP such that $P \sim 1$. Then $\bar{W}_\kappa(P) = \bar{W}_\kappa(1) = 0$ $\big(\kappa \in \{1,\ldots,l\}\big)$, so $W_1^{(1)}(P) = \cdots = W_1^{(r_1)}(P) = W_2^{(\rho_{21})}(P) = \cdots = W_2^{(\rho_{2s_2})}(P) = \cdots = W_l^{(\rho_{l1})}(P) = \cdots = W_l^{(\rho_{ls_l})}(P) = 0$. This leads to $r_1 + s_2 + \cdots + s_l = m$ linearly independent equations with m unknowns $(\alpha_1, \ldots, \alpha_m)$, since $W_1^{(1)}(P), \ldots, W_1^{(r_1)}(P), W_2^{(\rho_{21})}(P), \ldots, W_2^{(\rho_{2s_2})}(P), \ldots, W_l^{(\rho_{l1})}(P), \ldots, W_l^{(\rho_{ls_l})}(P)$ are linearly independent as linear forms in $\alpha_1, \ldots, \alpha_m$. Thus $\alpha_1 = \cdots = \alpha_m = 0$, so $P = 1$. Conversely, suppose that the sum of the ranks of $\bar{W}_1(P), \bar{W}_2(P), \ldots, \bar{W}_l(P)$ is $< m$. If we take $W_1^{(1)}(P) = \cdots = W_1^{(r_1)}(P) = W_2^{(\rho_{21})}(P) = \cdots = W_2^{(\rho_{2s_2})}(P) = \cdots = W_l^{(\rho_{l1})}(P) = \cdots = W_l^{(\rho_{ls_l})}(P) = 0$ and introduce the expression of P in the variables $x_1, \ldots, x_m$, then this leads to $r_1 + s_2 + \cdots + s_l < m$ equations with m unknowns $(\alpha_1, \ldots, \alpha_m)$. Thus there is a nontrivial solution, so there exists a PP $P \neq 1$ such that $\bar{W}_\kappa(P) = 0 = \bar{W}_\kappa(1)$ $\big(\kappa \in \{1,\ldots,l\}\big)$, i.e. $P \sim 1$. The sum of the ranks of all weight functions in (2.11) is called the **rank** of the sequence (2.11). Note also that for a regular sequence (2.11), $l \leq m$. The number l is the **length** of (2.11).

Example 2.2.6. 1) For $m = 3$ and $P := x_1^{\alpha_1} x_2^{\alpha_2} x_3^{\alpha_3}$,

define $W_1(P) := 1 \cdot \alpha_1 + \sqrt{2} \cdot \alpha_2 + \pi \cdot \alpha_3$, $W_2(P) := (1 + \sqrt{2}) \cdot \alpha_1 + \pi \cdot \alpha_2 + 0 \cdot \alpha_3$.

Write $W_1(P), W_2(P)$ in the form (2.6),

$W_1(P) = w_1^{(1)}W_1^{(1)}(P) + w_1^{(2)}W_1^{(2)}(P) + w_1^{(3)}W_1^{(3)}(P)$,

where $w_1^{(1)} = 1,\ w_1^{(2)} = \sqrt{2},\ w_1^{(3)} = \pi,\ W_1^{(1)}(P) = \alpha_1,\ W_1^{(2)}(P) = \alpha_2,\ W_1^{(3)}(P) = \alpha_3$,

$W_2(P) = w_2^{(1)}W_2^{(1)}(P) + w_2^{(2)}W_2^{(2)}(P)$,

where $w_2^{(1)} = 1 + \sqrt{2},\ w_2^{(2)} = \pi,\ W_2^{(1)}(P) = \alpha_1,\ W_2^{(2)}(P) = \alpha_2$.

By the above procedure, we can replace the sequence $W_1(P), W_2(P)$ by a regular sequence

$\bar{W}_1(P) := W_1(P) = w_1^{(1)}W_1^{(1)}(P) + w_1^{(2)}W_1^{(2)}(P) + w_1^{(3)}W_1^{(3)}(P)$.

Note that the rank of this sequence is = the rank of $W_1(P)$ = 3, and the length of this sequence is = 1.

2) For $m = 4$ and $P := x_1^{\alpha_1}x_2^{\alpha_2}x_3^{\alpha_3}x_4^{\alpha_4}$,

define $W_1(P) := \pi \cdot \alpha_1 + \sqrt{2} \cdot \alpha_2 + (2\sqrt{2} + 3\pi) \cdot \alpha_3 + (-\sqrt{2} + 7\pi) \cdot \alpha_4$,

$W_2(P) := \sqrt{3} \cdot \alpha_1 + \pi \cdot \alpha_2 + 1 \cdot \alpha_3 + (2 + \pi) \cdot \alpha_4$.

Write $W_1(P), W_2(P)$ in the form (2.6),

$W_1(P) = w_1^{(1)}W_1^{(1)}(P) + w_1^{(2)}W_1^{(2)}(P)$,

where $w_1^{(1)} = \pi,\ w_1^{(2)} = \sqrt{2},\ W_1^{(1)}(P) = \alpha_1 + 3\alpha_3 + 7\alpha_4,\ W_1^{(2)}(P) = \alpha_2 + 2\alpha_3 - \alpha_4$,

$W_2(P) = w_2^{(1)}W_2^{(1)}(P) + w_2^{(2)}W_2^{(2)}(P) + w_2^{(3)}W_2^{(3)}(P)$,

where $w_2^{(1)} = \sqrt{3},\ w_2^{(2)} = \pi,\ w_2^{(3)} = 1,\ W_2^{(1)}(P) = \alpha_1,\ W_2^{(2)}(P) = \alpha_2 + \alpha_4$,

$W_2^{(3)}(P) = \alpha_3 + 2\alpha_4$.

By the above procedure, we can replace the sequence $W_1(P), W_2(P)$ by a regular sequence

$\bar{W}_1(P) := W_1(P) = w_1^{(1)}W_1^{(1)}(P) + w_1^{(2)}W_1^{(2)}(P)$,

$\bar{W}_2(P) := w_2^{(1)}W_2^{(1)}(P) + w_2^{(2)}W_2^{(2)}(P)$.

Note that the rank of this sequence is = the rank of $\bar{W}_1(P)$ + the rank of $\bar{W}_2(P)$ = 2+2 = 4, and the length of this sequence is = 2.

2.3 Comparability of ordered PP's

We say that P_1 is **comparable with** P_2 (denoted by $P_1 \; c \; P_2$) if there exist $\epsilon = \pm 1$ and $\lambda, \mu \in \mathbb{Q}^+$ such that

$$P_1 \lesssim P_2^{\epsilon\lambda}, \; P_1 \gtrsim P_2^{\epsilon\mu}. \tag{2.12}$$

From this definition, we derive the following simple properties:

A. $P \; c \; P$ (reflexivity).

B. $(P_1 \; c \; P_2) \Rightarrow (P_2 \; c \; P_1)$ (symmetry).

C. $(P_1 \; c \; P_2) \Rightarrow (P_1 \; c \; P_2^{-1})$.

D. $(P_1 \; c \; P_2) \Rightarrow (P_1^{-1} \; c \; P_2)$.

E. $(P_1 \; c \; P_2) \wedge (P_2 \sim 1) \Rightarrow (P_1 \sim 1)$.

F. If $(P_1 \; c \; P_2)$ and both P_1, P_2 are $\gtrsim 1$, then ϵ in (2.12) can be chosen as 1.

G. $(P_1 \; c \; P_2) \wedge (P_2 \; c \; P_3) \Rightarrow (P_1 \; c \; P_3)$ (transitive).

H. For $\alpha \in \mathbb{Q} \setminus \{0\}, \; P \; c \; P^\alpha$.

I. $(P_1 \sim P_2) \Rightarrow (P_1 \; c \; P_2)$.

J. $(P \; c \; 1) \Leftrightarrow (P \sim 1)$.

K. If $P_2^{-\alpha} < P_1 < P_2^{\alpha}$ for all $\alpha \in \mathbb{Q}^+$, then P_1 and P_2 are not comparable.

Proof. A - J are obvious. We will prove K. Suppose $P_1 \; c \; P_2$. Then there exist $\epsilon = \pm 1$ and $\lambda, \mu \in \mathbb{Q}^+$ such that $P_1 \lesssim P_2^{\epsilon\lambda}, \; P_1 \gtrsim P_2^{\epsilon\mu}$. If $\epsilon = 1$, we have $P_1 \gtrsim P_2^{\mu}$, which is a contradiction. If $\epsilon = -1$, we have $P_1 \lesssim P_2^{-\lambda}$, which is also a contradiction. □

Example 2.3.1. For $m = 3$ and $P := x_1^{\alpha_1} x_2^{\alpha_2} x_3^{\alpha_3}$, define $W(P) := 1 \cdot \alpha_1 + 2 \cdot \alpha_2 + 3 \cdot \alpha_3$. We could define a regular ordering Ω by using $W(P)$.

Let $P_1 := x_1 x_2^2 x_3^3, \; P_2 := x_1^3 x_2 x_3$. We will show that $P_1 \; c \; P_2$ but $P_1 \nsim P_2$.

Note that $W(P_1) = 1 \cdot 1 + 2 \cdot 2 + 3 \cdot 3 = 14, \; W(P_2) = 1 \cdot 3 + 2 \cdot 1 + 3 \cdot 1 = 8$.

Since $W(P_1) \neq W(P_2)$, $P_1 \nsim P_2$. Choose $\epsilon = \mu = 1, \; \lambda = 2$.

Then $W(P_2^{\epsilon\lambda}) = W(P_2^2) = 2 \cdot W(P_2) = 16, W(P_2^{\epsilon\mu}) = W(P_2) = 8$.
Since $W(P_1) < W(P_2^{\epsilon\lambda})$ and $W(P_1) > W(P_2^{\epsilon\mu})$, $P_1 < P_2^{\epsilon\lambda}$ and $P_1 > P_2^{\epsilon\mu}$, respectively. Thus $P_1 \; c \; P_2$. This shows that the converse of property I is not true.

By properties A, B and G, we have that c is an equivalent relation. Then the set of all PP's is now decomposed into **comparability classes**, where all PP's in the same comparability class are comparable, but the PP's from two different comparability classes are not comparable.

In particular, the **comparability class containing 1 will be denoted by U**. By property J, U consists of all PP's which are equivalent to 1. If U contains only 1, it is called **trivial**. Otherwise, it is called **nontrivial**.

For the case $m = 1$, by property H, we have that every PP which is $\neq 1$ are comparable. Then if U is nontrivial, there is only one comparability class and if U is trivial, there are two comparability classes.

Lemma 2.3.2. Assume that C_1 and C_2 are two different comparability classes which are $\neq U$. Let P_1, Q_1 be two PP's from C_1 which are both > 1 and P_2, Q_2 be two PP's from C_2 which are both > 1. Then if $Q_1 > Q_2$, we have that for any $\delta \in \mathbb{Q}^+$, $P_1^\delta > P_2$. Especially, $P_1 > P_2$.

Proof. Since $P_2 \; c \; Q_2$ and both P_2, Q_2 are $\gtrsim 1$, by property F, $P_2 \lesssim Q_2^\lambda$ for some $\lambda \in \mathbb{Q}^+$. Since $Q_2^{\lambda'} < Q_1^\lambda$, $P_2 < Q_1^\lambda$. By property H, $Q_1 \; c \; Q_1^\lambda$, then Q_1^λ is in the class C_1. Since $Q_1^\lambda \; c \; P_1$ and both Q_1^λ, P_1 are $\gtrsim 1$, by property F, $Q_1^\lambda \lesssim P_1^\mu$ for some $\mu \in \mathbb{Q}^+$. Since $P_2 < Q_1^\lambda$ and $Q_1^\lambda \lesssim P_1^\mu$, $P_2 < P_1^\mu$. If $P_2 \gtrsim P_1^\delta$, then it follows that $P_1 \; c \; P_2$ which is a contradiction. Thus $P_2 < P_1^\delta$. $\square$

We will say that the class C_1 is **higher than** the class C_2 (denoted by $C_1 > C_2$) if for any PP P_1 from C_1 and PP P_2 from C_2 such that $P_1 > 1$ and $P_2 \gtrsim 1$, we have $P_1 > P_2$. Obviously, this relationship is transitive. Note that if there exists a comparability class $C \neq U$, then C must contain a PP P which is $\not\approx 1$; by property H, we can assume that $P > 1$. Thus we have always $C > U$.

Lemma 2.3.3. Assume that $k \geq 1$ and $C_0, C_1, \ldots, C_k$ are $k+1$ comparability classes such that $C_0 < C_1 < \cdots < C_k$. Choose an arbitrary P_κ from each C_κ $\left(\kappa \in \{0, 1, \ldots, k\}\right)$. Let $P^* := P_0^{\beta_0} P_1^{\beta_1} \ldots P_k^{\beta_k}$, with $\beta_\kappa \in \mathbb{Q}$ $\left(\kappa \in \{0, 1, \ldots, k\}\right)$. If $\beta_k \neq 0$, we have $P^* \in C_k$ and $P^* > 1$ or $P^* < 1$ according as $P_k^{\beta_k} > 1$ or $P_k^{\beta_k} < 1$.

Proof. Without loss of generality, we can assume that

1) $P_\kappa > 1$ $\left(\kappa \in \{0, 1, \ldots, k\}\right)$ since we can replace P_κ by P_κ^{-1},

2) $\beta_k > 0$ since we can replace P^* by P^{*-1},

3) $\beta_\kappa \neq 0$ $\left(\kappa \in \{0, 1, \ldots, k\}\right)$ since we can leave out those C_κ for which $\beta_\kappa = 0$.

Let $\beta := \sum_{\kappa=0}^{k} |\beta_\kappa|$ and $\epsilon := \dfrac{\beta_k}{2\beta}$. For $\kappa \in \{0, 1, \ldots, k-1\}$, since $C_\kappa < C_k$, $P_\kappa < P_k^\epsilon$. And since $P_k > 1$, $P_k^{-\epsilon} < 1$. But $1 < P_\kappa$, so $P_k^{-\epsilon} < P_\kappa$. Then $P_k^{-\epsilon} < P_\kappa < P_k^\epsilon$. If $\beta_\kappa > 0$, $P_k^{-\epsilon\beta_\kappa} < P_\kappa^{\beta_\kappa} < P_k^{\epsilon\beta_\kappa}$. If $\beta_\kappa < 0$, $P_k^{\epsilon\beta_\kappa} < P_\kappa^{\beta_\kappa} < P_k^{-\epsilon\beta_\kappa}$. Thus $P_k^{-\epsilon|\beta_\kappa|} < P_\kappa^{\beta_\kappa} < P_k^{\epsilon|\beta_\kappa|}$. Then $P_k^{-\epsilon|\beta_0|} P_k^{-\epsilon|\beta_1|} \ldots P_k^{-\epsilon|\beta_{k-1}|} < P_0^{\beta_0} P_1^{\beta_1} \ldots P_{k-1}^{\beta_{k-1}} < P_k^{\epsilon|\beta_0|} P_k^{\epsilon|\beta_1|} \ldots P_k^{\epsilon|\beta_{k-1}|}$, i.e. $P_k^{\epsilon(\beta_k - \beta)} < \dfrac{P^*}{P_k^{\beta_k}} < P_k^{\epsilon(\beta - \beta_k)}$, so $P_k^{\epsilon(\beta_k-\beta)+\beta_k} < P^* < P_k^{\epsilon(\beta-\beta_k)+\beta_k}$. Note that $\epsilon(\beta_k - \beta) + \beta_k = \epsilon\beta_k + \dfrac{\beta_k}{2}$ and $\epsilon(\beta - \beta_k) + \beta_k = \dfrac{3\beta_k}{2} - \epsilon\beta_k$. Since $P_k > 1$ and $\epsilon, \beta_k > 0$, it follows that $P_k^{\epsilon\beta_k} > 1$ and $P_k^{-\epsilon\beta_k} < 1$. Then $P_k^{\beta_k/2} < P_k^{\epsilon\beta_k + \beta_k/2} = P_k^{\epsilon(\beta_k-\beta)+\beta_k} < P^* < P_k^{\epsilon(\beta-\beta_k)+\beta_k} = P_k^{3\beta_k/2 - \epsilon\beta_k} < P_k^{3\beta_k/2}$. Thus $P^* \in C_k$. Finally, if $P_k^{\beta_k} > 1$, then $P_k^{\beta_k/2} > 1$. But $P^* > P_k^{\beta_k/2}$, so $P^* > 1$. And if $P_k^{\beta_k} < 1$, then $P_k^{3\beta_k/2} < 1$. But $P^* < P_k^{3\beta_k/2}$, so $P^* < 1$. □

Proposition 2.3.4. Assume that $k \geq 1$ and $C_0, C_1, \ldots, C_k$ are $k+1$ comparability classes such that $C_0 < C_1 < \cdots < C_k$. If U is nontrivial, take $C_0 = U$; otherwise, assume $C_0 > U$. Choose an element $P_\kappa \neq 1$ from each C_κ $\left(\kappa \in \{0, 1, \ldots, k\}\right)$. Then for any $\beta_\kappa \in \mathbb{Q}$ $\left(\kappa \in \{0, 1, \ldots, k\}\right)$, not all zero, we have that the relation

$$P_0^{\beta_0} P_1^{\beta_1} \dots P_k^{\beta_k} = 1 \tag{2.13}$$

is impossible.

Proof. Without loss of generality, we can assume that $\beta_k \neq 0$. Otherwise, we can leave out C_k. Suppose that $P_0^{\beta_0} P_1^{\beta_1} \dots P_k^{\beta_k} = 1$. Then $P_k^{\beta_k} = P_0^{-\beta_0} P_1^{-\beta_1} \dots P_{k-1}^{-\beta_{k-1}}$. By Lemma 2.3.3, it follows that $P_k^{\beta_k} = P_0^{-\beta_0} P_1^{-\beta_1} \dots P_{k-1}^{-\beta_{k-1}}$ is an element of U or C_κ for some $\kappa \in \{0, 1, \dots, k-1\}$. And by property H, we obtain that $P_k^{\beta_k}$ is an element of C_k, which is a contradiction. □

Note that the relation (2.13) is always possible for $k \geq m$. To see this, suppose that $P_0^{\beta_0} P_1^{\beta_1} \dots P_k^{\beta_k} = 1$. Introducing the expressions of $P_0, P_1, \dots, P_k$ in the variables $x_1, \dots, x_m$ leads to m equations with $k+1 > m$ unknowns. Then there is a nontrivial solution $\beta_\kappa \in \mathbb{Q}$ $\big(\kappa \in \{0, 1, \dots, k\}\big)$, not all zero, such that $P_0^{\beta_0} P_1^{\beta_1} \dots P_k^{\beta_k} = 1$. It follows that the number k in Proposition 2.3.4 must be $\leq m - 1$. Thus we have that the total number of the comparability classes is $\leq m + 1$, and even $\leq m$ if U is nontrivial.

Theorem 2.3.5. Any regular ordering of algebraic PP's can be obtained by the lexicographic principle from a regular ordered sequence of weight functions.

Proof. First, we will prove in the special case that U is trivial and that, besides U, there is only one comparability class C. Then all x_μ $\big(\mu \in \{1, \dots, m\}\big)$ are comparable. We can assume that $x_\mu > 1$ $\big(\mu \in \{1, \dots, m\}\big)$ since we can replace each x_μ with x_μ^{-1} by an m-r-transformation. If $m = 1$, define $W(P) := \alpha_1$. Since $x_1 > 1$, it follows that for any $\alpha > 0$, $x_1^\alpha > 1$ and $x_1^{-\alpha} < 1$. Then we have that for any $\alpha, \beta \in \mathbb{Q}$, $x_1^\alpha > x_1^\beta \Leftrightarrow x_1^{\alpha-\beta} > 1 \Leftrightarrow \alpha - \beta > 0 \Leftrightarrow \alpha > \beta \Leftrightarrow W(x_1^\alpha) > W(x_1^\beta)$. Dually, $x_1^\alpha < x_1^\beta \Leftrightarrow W(x_1^\alpha) < W(x_1^\beta)$. And $x_1^\alpha \sim x_1^\beta \Leftrightarrow x_1^{\alpha-\beta} \sim 1 \Leftrightarrow \alpha - \beta = 0 \Leftrightarrow \alpha = \beta \Leftrightarrow W(x_1^\alpha) = W(x_1^\beta)$. Thus $W(P)$ satisfies the requirements of Theorem 2.3.5. So we can assume that $m > 1$. For $\kappa \in \{2, \dots, m\}$, we claim that there is no $\sigma \in \mathbb{Q}$ such that $x_1^\sigma \sim x_\kappa$. To see this, suppose that there exists $\sigma \in \mathbb{Q}$ such that $x_1^\sigma \sim x_\kappa$. Then $x_\kappa x_1^{-\sigma} \sim 1$, so $x_\kappa x_1^{-\sigma}$ is an element of U. Since U is trivial, $x_\kappa x_1^{-\sigma} = 1$. This contradicts the fact that x_1, x_κ are independent.

Since for $\kappa \in \{2, \dots, m\}$, $x_\kappa \; c \; x_1$, there exist $\lambda, \mu \in \mathbb{Q}^+$ such that $x_1^\lambda < x_\kappa < x_1^\mu$. Then $x_1^{\lambda-\mu} < 1$. Since $x_1 > 1$, it follows that $\lambda - \mu < 0$, so $\lambda < \mu$. Let $\gamma_\kappa \in \mathbb{R}$ be the least upper bound of the set $\{\sigma \in \mathbb{Q} \mid x_1^\sigma < x_\kappa\}$. For $\sigma \in \mathbb{Q}$, if $\gamma_\kappa < \sigma$, then $x_\kappa < x_1^\sigma$. We show that if $\sigma < \gamma_\kappa$, then $x_1^\sigma < x_\kappa$. Put $\delta := \gamma_\kappa - \sigma > 0$. Thus there exists $\sigma' \in \mathbb{Q}$ such that $\gamma_\kappa - \dfrac{\delta}{2} < \sigma'$ and $x_1^{\sigma'} < x_\kappa$. Since $\sigma = \gamma_\kappa - \delta < \gamma_\kappa - \dfrac{\delta}{2} < \sigma'$ and $x_1 > 1$, $x_1^\sigma < x_1^{\sigma'} < x_\kappa$. For $\kappa = 1$, we set $\gamma_1 := 1$. It is convenient to establish next the following result.

Lemma 2.3.6. Assume that U is trivial and that, besides U, there is only one comparability class C. Moreover, assume that $x_\mu > 1$ $\big(\mu \in \{1, \dots, m\}\big)$ and $m > 1$. For $\kappa \in \{1, \dots, m\}$, let γ_κ be the constant defined above and $\alpha_\kappa \in \mathbb{Q}$ be such that $\sum_{\kappa=1}^{m} |\alpha_\kappa| > 0$. For $P := x_1^{\alpha_1} \dots x_m^{\alpha_m}$, put $L(P) := \sum_{\kappa=1}^{m} \alpha_\kappa \gamma_\kappa$. Let $u, v \in \mathbb{Q}$ be such that $u < L(P) < v$. Then $x_1^u < P < x_1^v$.

Proof of Lemma 2.3.6. If $\sum_{\kappa=2}^{m} |\alpha_\kappa| = 0$, then $\alpha_\kappa = 0$ for all $\kappa \in \{2, \dots, m\}$, so $P = x_1^{\alpha_1}$ and $L(P) = \alpha_1$. From $u < \alpha_1 < v$ and $x_1 > 1$, it follows that $x_1^u < x_1^{\alpha_1} < x_1^v$. So we can assume that $\sum_{\kappa=2}^{m} |\alpha_\kappa| > 0$. Set $A := \sum_{\kappa=1}^{m} |\alpha_\kappa|$. Let $\epsilon \in \mathbb{Q}$ be such that $0 < \epsilon < \dfrac{L(P) - u}{A}$, $\sigma_1 := 1$ and for $\kappa \in \{2, \dots, m\}$, let $\sigma_\kappa \in \mathbb{Q}$ be such that $\gamma_\kappa - \epsilon < \sigma_\kappa < \gamma_\kappa$, if $\alpha_\kappa > 0$, $\gamma_\kappa < \sigma_\kappa < \gamma_\kappa + \epsilon$ if $\alpha_\kappa < 0$, $\sigma_\kappa = 0$ if $\alpha_\kappa = 0$. Put $u_1 := \sum_{\kappa=1}^{m} \alpha_\kappa \sigma_\kappa$. For $\kappa \in \{2, \dots, m\}$, we have $\alpha_\kappa \sigma_\kappa < \alpha_\kappa \gamma_\kappa$ if $\alpha_\kappa \neq 0$, and so $u_1 < L(P)$. And $L(P) - u_1 = \sum_{\alpha_\kappa > 0} \alpha_\kappa(\gamma_\kappa - \sigma_\kappa) - \sum_{\alpha_\kappa < 0} \alpha_\kappa(\sigma_\kappa - \gamma_\kappa) < \sum_{\alpha_\kappa > 0} |\alpha_\kappa|\epsilon + \sum_{\alpha_\kappa < 0} |\alpha_\kappa|\epsilon = A\epsilon < L(P) - u$, so $u < u_1$. For $\kappa \in \{2, \dots, m\}$, if $\alpha_\kappa > 0$, then $\sigma_\kappa < \gamma_\kappa$, and so $x_1^{\sigma_\kappa} < x_\kappa$. Then $x_1^{\alpha_\kappa \sigma_\kappa} < x_\kappa^{\alpha_\kappa}$. If $\alpha_\kappa < 0$, then $\gamma_\kappa < \sigma_\kappa$, and so $x_\kappa < x_1^{\sigma_\kappa}$. Then

$x_1^{\alpha_\kappa\sigma_\kappa} < x_\kappa^{\alpha_\kappa}$. Thus $x_1^{u_1} = x_1^{\alpha_1\sigma_1+\cdots+\alpha_m\sigma_m} < x_1^{\alpha_1}\ldots x_m^{\alpha_m} = P$. Since $u < u_1$ and $x_1 > 1$, $x_1^u < x_1^{u_1}$. Therefore $x_1^u < P$. To show that $P < x_1^v$, consider $P^{-1} = x_1^{-\alpha_1}\ldots x_m^{-\alpha_m}$. Then we have $L(P^{-1}) = \sum_{\kappa=1}^{m}(-\alpha_\kappa)\gamma_\kappa = -\sum_{\kappa=1}^{m}\alpha_\kappa\gamma_\kappa = -L(P)$. Since $L(P) < v$, $-v < -L(P) = L(P^{-1})$. By the first inequality, substituting P by P^{-1} and u by $-v$, we get $x_1^{-v} < P^{-1}$. Therefore $P < x_1^v$. ☐

We now show that $\gamma_1,\ldots,\gamma_m$ are $\mathbb{Q}$-linearly independent. Suppose that there exist $\beta_\kappa \in \mathbb{Z}$ $(\kappa \in \{1,\ldots,m\})$, not all zero, such that $\sum_{\kappa=1}^{m}\beta_\kappa\gamma_\kappa = 0$. Let $P^* := x_1^{\beta_1}\ldots x_m^{\beta_m}$. Then $L(P^*) = 0$. For any $p \in \mathbb{Q}^+$, since $-p < L(P^*) < p$, by Lemma 2.3.6, it follows that $x_1^{-p} < P^* < x_1^p$. By property K, we have P^* and x_1 are not comparable. Thus P^* must belong to U. Since U is trivial, $P^* = 1$. So $\beta_\kappa = 0$ $(\kappa \in \{1,\ldots,m\})$, which is a contradiction.

Observe that if $L(P) > 0$, by choosing $p \in \mathbb{Q}$, $0 < p < L(P)$, then by Lemma 2.3.6, $P > x_1^p > 1$. Similarly, if $L(P) < 0$, then $P < 1$. We prove that for any PP's P_1, P_2, we have $P_1 > P_2$ if $L(P_1) > L(P_2)$, $P_1 < P_2$ if $L(P_1) < L(P_2)$, $P_1 \sim P_2$ if $L(P_1) = L(P_2)$. Let $P_1 := x_1^{\alpha_1}\ldots x_m^{\alpha_m}, P_2 := x_1^{\beta_1}\ldots x_m^{\beta_m}$. Then $P_1P_2^{-1} = x_1^{\alpha_1-\beta_1}\ldots x_m^{\alpha_m-\beta_m}$. Note that $L(P_1) - L(P_2) = \sum_{\kappa=1}^{m}\alpha_\kappa\gamma_\kappa - \sum_{\kappa=1}^{m}\beta_\kappa\gamma_\kappa = \sum_{\kappa=1}^{m}(\alpha_\kappa - \beta_\kappa)\gamma_\kappa = L(P_1P_2^{-1})$. Thus $L(P_1) > L(P_2) \Rightarrow L(P_1) - L(P_2) > 0 \Rightarrow L(P_1P_2^{-1}) > 0 \Rightarrow P_1P_2^{-1} > 1 \Rightarrow P_1 > P_2$. And dually, $L(P_1) < L(P_2) \Rightarrow P_1 < P_2$. Assume that $L(P_1) = L(P_2)$. Then $\sum_{\kappa=1}^{m}\alpha_\kappa\gamma_\kappa = \sum_{\kappa=1}^{m}\beta_\kappa\gamma_\kappa$. Since $\gamma_1,\ldots,\gamma_m$ are $\mathbb{Q}$-linearly independent, it follows that $\alpha_\kappa = \beta_\kappa$ $(\kappa \in \{1,\ldots,m\})$. Thus $P_1 = P_2$, so $P_1 \sim P_2$. We see that the requirements of Theorem 2.3.5 are satisfied if we define $W(P) := L(P)$. Then Theorem 2.3.5 is proved in the special case.

Now, we consider the general case. For $m = 1$, if U is trivial, this is a special case which has been already proved above. Otherwise, if U is nontrivial, then every $P = x_1^{\alpha_1}$ belongs to U and there is no ordering at all. We can choose here $W(P) := 0$.

We will prove the remaining case of Theorem 2.3.5 by induction. Assume that Theorem 2.3.5 has already been proved for all $m' < m$.

Let $C_0 < C_1 < \cdots < C_s$ be the ordered sequence of all comparability classes. If U is nontrivial, take $C_0 = U$. Otherwise, assume $C_0 > U$. If $s < 1$, this is a special case which has been already proved. Then we assume that $s \geq 1$.

We will show that if P_1, P_2 belong to C_0, then $P_1P_2 = 1$ or P_1P_2 belongs to C_0. This is clear if $P_1 = 1$ or $P_2 = 1$. So we assume that $P_1 \neq 1$ and $P_2 \neq 1$. Let P be an element of C_1 such that $P > 1$ and $p \in \mathbb{Q}^+$. Then $P^p > 1$ and $P^{-p} < 1$. If $P_1 > 1$, from $C_0 < C_1$, $P_1 < P^p$. Since $P^{-p} < 1$, $P^{-p} < P_1$. So we have $P^{-p} < P_1 < P^p$. If $P_1 < 1$, then $P_1^{-1} > 1$. From $C_0 < C_1$, $P_1^{-1} < P^p$, so $P^{-p} < P_1$. Since $P_1 < 1 < P^p$, we also have $P^{-p} < P_1 < P^p$. Similarly, $P^{-p} < P_2 < P^p$. Thus $P^{-2p} < P_1P_2 < P^{2p}$. Then for any $\alpha \in \mathbb{Q}^+$, $P^{-\alpha} = P^{-2(\alpha/2)} < P_1P_2 < P^{2(\alpha/2)} < P^{\alpha}$. By property K, P_1P_2 and P are not comparable, so P_1P_2 does not belong to C_1. But $P_1P_2 < P^{\alpha}$ for any $\alpha \in \mathbb{Q}^+$, then P_1P_2 belongs to a class $< C_1$. Thus if $P_1P_2 \neq 1$, we have that P_1P_2 belongs to C_0.

For $P := x_1^{\alpha_1} \dots x_m^{\alpha_m}$, we introduce the set of linear forms

$$S(u) := \alpha_1 u_1 + \cdots + \alpha_m u_m$$

with indeterminates $u_1, \dots, u_m$. We will called P and $S(u)$ **associated**. Obviously, the product of two PP's is associated to the sum of their associated linear forms.

Let T be the set of all linear forms associated with elements of C_0 and $L_1, \dots, L_t$ be the maximal number of linearly independent forms from T chosen in an arbitrary way. Note that $t \leq m$. Then any form $L \in T$ can be written as $L = \sum_{\tau=1}^{t} \rho_\tau L_\tau$ where $\rho_\tau \in \mathbb{Q}$.

For $\tau \in \{1,\ldots,t\}$, denote the PP associated with L_τ by P_τ. For $\beta_\tau \in \mathbb{Z}$ $\big(\tau \in \{1,\ldots,t\}\big)$ such that $P_1^{\beta_1}\ldots P_t^{\beta_t}=1$, we have $\beta_1 L_1+\cdots+\beta_t L_t=0$. This leads to t linearly independent equations with t unknowns $(\beta_1,\ldots,\beta_t)$, since $L_1,\ldots,L_t$ are the maximal number of linearly independent forms from T. Thus $\beta_1=\cdots=\beta_t=0$. Let P be an element of C_0 and L its associated linear form. Since $L=\rho_1 L_1+\cdots+\rho_t L_t=0$ where $\rho_\tau \in \mathbb{Q}$ $\big(\tau \in \{1,\ldots,t\}\big)$, $P=P_1^{\rho_1}\ldots P_t^{\rho_t}$.

By an m-r-transformation, we can transform $P_1,\ldots,P_t$ into $x_1,\ldots,x_t$, respectively. Then we can assume that $C_0 \equiv [x_1,\ldots,x_t] \setminus \{1\}$, if U is trivial and $C_0 \equiv [x_1,\ldots,x_t]$, if U is nontrivial. For $P:=x_1^{\alpha_1}\ldots x_m^{\alpha_m}$, we can write $P=\bar{P}'\bar{P}$ where $\bar{P}'=x_1^{\alpha_1}\ldots x_t^{\alpha_t}\in[x_1,\ldots,x_t]$ and $\bar{P}=x_{t+1}^{\alpha_{t+1}}\ldots x_m^{\alpha_m}\in[x_{t+1},\ldots,x_m]$. We see that $\bar{P}'=1$ or $\bar{P}'$ is an element of C_0. We show that $\bar{P}=1$ or $\bar{P}$ belongs to the same comparability class $C>C_0$ as P. Suppose that $\bar{P}\neq 1$. Then $\alpha_\mu \neq 0$ for some $\mu\in\{t+1,\ldots,m\}$, so $\bar{P}$ does not belong to C_0. Obviously, $\bar{P}$ does not belong to U, if U is trivial. Thus $\bar{P}$ belongs to some comparability class $C>C_0$. If $\bar{P}'=1$, then $P=\bar{P}$, so P belongs to C. If $\bar{P}'$ is an element of C_0, by Lemma 2.3.3, P belongs to C and it follows also that $P>1$ or $P<1$ according as $\bar{P}>1$ or $\bar{P}<1$. Note that for any PP's P_1,P_2, $\overline{P_1/P_2}=\bar{P}_1/\bar{P}_2$. Then we have that $P_1>P_2$ or $P_1<P_2$ according as $\bar{P}_1>\bar{P}_2$ or $\bar{P}_1<\bar{P}_2$. Let $\bar{\Omega}$ be the ordering of $[x_{t+1},\ldots,x_m]$ given by Ω and $\bar{W}(\bar{P}')$ the weight function which generates the ordering in $[x_1,\ldots,x_t]$ if U is trivial and $\bar{W}(\bar{P}'):=0$ if U is nontrivial. Observe that if U is trivial, the existence of $\bar{W}(\bar{P}')$ has been proved as the special case of Theorem 2.3.5. By the induction hypothesis, $\bar{\Omega}$ can be generated by a regular sequence of weight functions, $\bar{W}_1(\bar{P}),\bar{W}_2(P),\ldots,\bar{W}_k(\bar{P})$. Put $W_\kappa(P):=\bar{W}_\kappa(\bar{P})$ $\big(\kappa\in\{1,\ldots,k\}\big)$ and $W_{k+1}(P):=\bar{W}(\bar{P}')$.

We now claim that Ω is generated by the sequence

$$W_1(P),\ldots,W_{k+1}(P). \tag{2.14}$$

Let P_1, P_2 be any PP's,

Case 1. $W_\kappa(P_1) = W_\kappa(P_2)$ $\big(\kappa \in \{1,\ldots,k+1\}\big)$. Then $\bar{W}_\kappa(\bar{P}_1) = \bar{W}_\kappa(\bar{P}_2)$ $\big(\kappa \in \{1,\ldots,k\}\big)$ and $\bar{W}(\bar{P}_1{}') = \bar{W}(\bar{P}_2{}')$. Thus $\bar{P}_1 \sim \bar{P}_2$ and $\bar{P}_1{}' \sim \bar{P}_2{}'$, so $P_1 = \bar{P}_1{}'\bar{P}_1 \sim \bar{P}_2{}'\bar{P}_2 = P_2$.

Case 2. $W_\kappa(P_1) \neq W_\kappa(P_2)$ for some $\kappa \in \{1,\ldots,k+1\}$. Let $k_0 := \min\{\kappa \in \{1,\ldots,k+1\} \mid W_\kappa(P_1) \neq W_\kappa(P_2)\}$. Then $W_\kappa(P_1) = W_\kappa(P_2)$ $(\kappa < k_0)$.

Case 2.1. $W_{k_0}(P_1) > W_{k_0}(P_2)$. If $k_0 \in \{1,\ldots,k\}$, then $\bar{W}_\kappa(\bar{P}_1) = \bar{W}_\kappa(\bar{P}_2)$ $(\kappa < k_0)$ and $\bar{W}_{k_0}(\bar{P}_1) > \bar{W}_{k_0}(\bar{P}_2)$. Thus $\bar{P}_1 > \bar{P}_2$, so $P_1 > P_2$. If $k_0 = k+1$, then $W_\kappa(P_1) = W_\kappa(P_2)$ $\big(\kappa \in \{1,\ldots,k\}\big)$ and $W_{k+1}(P_1) > W_{k+1}(P_2)$, i.e. $\bar{W}_\kappa(\bar{P}_1) = \bar{W}_\kappa(\bar{P}_2)$ $\big(\kappa \in \{1,\ldots,k\}\big)$ and $\bar{W}(\bar{P}_1{}') > \bar{W}(\bar{P}_2{}')$. Thus $\bar{P}_1 \sim \bar{P}_2$ and $\bar{P}_1{}' > \bar{P}_2{}'$, so $P_1 = \bar{P}_1{}'\bar{P}_1 > \bar{P}_2{}'\bar{P}_2 = P_2$.

Case 2.2. $W_{k_0}(P_1) < W_{k_0}(P_2)$. Similar arguments as in Case 2.1 show that $P_1 < P_2$.

Cases 1 and 2 prove the claim.

Note that the rational weight functions belonging to $W_{k+1}(P)$ depend only on $\alpha_1,\ldots,\alpha_t$. But the rational weight functions belonging to $W_\kappa(P)$ $\big(\kappa \in \{1,\ldots,k\}\big)$ depend on $\alpha_{t+1},\ldots,\alpha_m$, so they are independent of $\alpha_1,\ldots,\alpha_t$. Thus (2.14) is regular, and Theorem 2.3.5 is proved. □

2.4 Structure of sequences of weight functions

We assume now that the ordering Ω in $[x_1,\ldots,x_m]$ is generated by the sequence of the rank r,

$$W_1(P),\ldots,W_k(P). \tag{2.15}$$

We assume that (2.15) is **irreducible**, i.e. none of $W_\kappa(P)$ $\big(\kappa \in \{1,\ldots,k\}\big)$ is a linear combination of the rational weight functions belonging to $W_1(P),\ldots,W_{\kappa-1}(P)$.

We claim that there exists a sequence of r rational weight functions

$$R_1(P), \dots, R_r(P) \tag{2.16}$$

and a sequence of positive integers $r_1 < \cdots < r_k = r$ such that

$$W_\kappa(P) = \sum_{\tau=1}^{r_\kappa} w_\kappa^{(\tau)} R_\tau(P) \quad \big(\kappa \in \{1, \dots, k\}\big), \tag{2.17}$$

where the set of linear forms (2.16) is linearly independent and each of the sets, $\{w_1^{(1)}, \dots, w_1^{(r_1)}\}$, $\{w_2^{(r_1+1)}, \dots, w_2^{(r_2)}\}, \dots,$ $\{w_k^{(r_{k-1}+1)}, \dots, w_k^{(r_k)}\}$ are linearly independent with respect to $\mathbb{Q}$.

In order to prove the claim, we begin by writing $W_1(P)$ in the form (2.6) as in Proposition 2.2.2, i.e. $W_1(P) = \sum_{\tau=1}^{r_1} w_1^{(\tau)} R_\tau(P)$, where $w_1^{(1)}, \dots, w_1^{(r_1)}$ are linearly independent real numbers. By Proposition 2.2.2 and Proposition 2.2.4, $R_1(P), \dots, R_{r_1}(P)$ form a basis of the set of all rational weight functions belonging to $W_1(P)$. Consider the set of all rational weight functions belonging to $W_1(P)$ or to $W_2(P)$ and construct a basis for this set by adding new basis elements to $R_1(P), \dots, R_{r_1}(P)$. In this way, we obtain additional basis elements $R_{r_1+1}(P), \dots, R_{r_2}(P)$. Since (2.15) is irreducible, it follows that $r_2 > r_1$. Then we can write

$$W_2(P) = \sum_{\tau=1}^{r_2} w_2^{(\tau)} R_\tau(P), \tag{2.18}$$

where $w_2^{(\tau)} \in \mathbb{R}$ $\big(\tau \in \{1, \dots, r_2\}\big)$. We next show that $w_2^{(r_1+1)}, \dots, w_2^{(r_2)}$ are linearly independent. Suppose that they are not linearly independent. So we can eliminate one of them in (2.18), obtaining the corresponding representation of $W_2(P)$ with at most $r_2 - r_1 - 1$ additional basis elements. But, by our construction, r_2 is the rank of the set of all rational weight functions belonging to $W_1(P)$ or to $W_2(P)$. This is a contradiction. The proof for other $\{w_3^{(r_2+1)}, \ldots, w_3^{(r_3)}\}, \ldots, \{w_k^{(r_{k-1}+1)}, \ldots, w_k^{(r_k)}\}$ is similar.

If we assume that the sequence (2.15) is not only irreducible but even regular, then, with $r_0 := 0$, (2.17) becomes

$$W_\kappa(P) = \sum_{\tau=r_{\kappa-1}+1}^{r_\kappa} w_\kappa^{(\tau)} R_\tau(P) \quad \big(\kappa \in \{1, \ldots, k\}\big).$$

Write $R_\tau(P)$ $\big(\tau \in \{1, \ldots, r\}\big)$ in (2.16) as linear form in $\alpha_1, \ldots, \alpha_m$, $R_\tau(P) = \sum_{\mu=1}^{m} c_{\tau\mu}\alpha_\mu$ $\big(\tau \in \{1, \ldots, r\}\big)$ where $c_{\tau\mu} \in \mathbb{Q}$ $\big(\tau \in \{1, \ldots, r\},\ \mu \in \{1, \ldots, m\}\big)$. If $r < m$, since $R_1(P), \ldots, R_\tau(P)$ are linearly independent, we can introduce $m - r$ linear forms $R_\nu(P) = \sum_{\mu=1}^{m} c_{\nu\mu}\alpha_\mu$ $\big(\nu \in \{r+1, \ldots, m\}\big)$ where $c_{\nu\mu} \in \mathbb{Q}$ $\big(\nu \in \{r+1, \ldots, m\},\ \mu \in \{1, \ldots, m\}\big)$ such that $\det[c_{\nu\mu}] \neq 0$. If we now apply the m-r-transformation, $x_\mu := y_1^{c_{1\mu}} \ldots y_m^{c_{m\mu}}$ $\big(\mu \in \{1, \ldots, m\}\big)$, then PP (2.1) becomes $x_1^{\alpha_1} \ldots x_m^{\alpha_m} = y_1^{\beta_1} \ldots y_m^{\beta_m}$ where $\beta_\nu = \sum_{\mu=1}^{m} c_{\nu\mu}\alpha_\mu$ $\big(\nu \in \{1, \ldots, m\}\big)$. We see that $R_\nu(P)$ $\big(\nu \in \{1, \ldots, m\}\big)$ become simple linear forms in $\beta_1, \ldots, \beta_m$, i.e. $R_\nu(P) = \beta_\nu$ $\big(\nu \in \{1, \ldots, m\}\big)$. Assume that we have applied the above transformation and the new variables are denoted again by $x_1, \ldots, x_m$. Then $R_\tau(P) = \alpha_\tau$ $\big(\tau \in \{1, \ldots, r\}\big)$. Thus for the case that the sequence (2.15) is irreducible, we have $W_\kappa(P) = \sum_{\tau=1}^{r_\kappa} w_\kappa^{(\tau)}\alpha_\tau$ $\big(\kappa \in \{1, \ldots, k\}\big)$, and for the case that the sequence (2.15) is regular and indeed also irreducible, we have $W_\kappa(P) = \sum_{\tau=r_{\kappa-1}+1}^{r_\kappa} w_\kappa^{(\tau)}\alpha_\tau$ $\big(\kappa \in \{1, \ldots, k\}\big)$, with $r_0 := 0$.

Example 2.4.1. Let $m = 3$ and $P := x_1^{\alpha_1} x_2^{\alpha_2} x_3^{\alpha_3}$.

1) Define $W(P) := 1 \cdot \alpha_1 + 2 \cdot \alpha_2 + 3 \cdot \alpha_3$. Assume that the ordering Ω in $[x_1, x_2, x_3]$ is generated by the sequence $W(P)$. It is clear that this sequence is regular.

Write $W(P)$ in the form (2.6),

$W(P) = w_1^{(1)} R_1^{(1)}(P)$, where $w_1^{(1)} = 1,\ R_1^{(1)}(P) = 1 \cdot \alpha_1 + 2 \cdot \alpha_2 + 3 \cdot \alpha_3$.

Define $R_2(P) := 0 \cdot \alpha_1 + 1 \cdot \alpha_2 + 0 \cdot \alpha_3$, $R_3(P) := 0 \cdot \alpha_1 + 0 \cdot \alpha_2 + 1 \cdot \alpha_3$.

Note that $\det \begin{bmatrix} 1 & 2 & 3 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = 1 \neq 0$. Now, we apply the above m-r-transformation, let $x_1 := y_1^1 y_2^0 y_3^0 = y_1,\ x_2 := y_1^2 y_2^1 y_3^0 = y_1^2 y_2,\ x_3 := y_1^3 y_2^0 y_3^1 = y_1^3 y_3$. So $PP\,(2.1)$ becomes $x_1^{\alpha_1} x_2^{\alpha_2} x_3^{\alpha_3} = y_1^{\alpha_1}(y_1^2 y_2)^{\alpha_2}(y_1^3 y_3)^{\alpha_3} = y_1^{\alpha_1+2\alpha_2+3\alpha_3} y_2^{\alpha_2} y_3^{\alpha_3}$. If we denote y_1, y_2, y_3 again by x_1, x_2, x_3, respectively, then by the above procedure, we have $W(P) = \alpha_1$.

2) Define $W_1(P) := 1 \cdot \alpha_1 + 2 \cdot \alpha_2 + 3 \cdot \alpha_3$, $W_2(P) := 1 \cdot \alpha_1 + \sqrt{2} \cdot \alpha_2 + \pi \cdot \alpha_3$.

Assume that the ordering Ω in $[x_1, x_2, x_3]$ is generated by the sequence $W_1(P), W_2(P)$.

Write $W_1(P)$ in the form (2.6),

$W_1(P) = w_1^{(1)} R_1(P)$, where $w_1^{(1)} = 1,\ R_1(P) = 1 \cdot \alpha_1 + 2 \cdot \alpha_2 + 3 \cdot \alpha_3$.

Then we can write $W_2(P) = w_2^{(1)} R_1(P) + w_2^{(2)} R_2(P) + w_2^{(3)} R_3(P)$,

where $w_2^{(1)} = \dfrac{\pi}{3},\ w_2^{(2)} = 1 - \dfrac{\pi}{3},\ w_2^{(3)} = \sqrt{2} - \dfrac{2\pi}{3},\ R_2(P) = \alpha_1,\ R_3(P) = \alpha_2$.

We see that $w_2^{(2)}, w_2^{(3)}$ are linearly independent with respect to $\mathbb{Q}$ and $R_1(P), R_2(P)$, $R_3(P)$ are linearly independent as linear forms in $\alpha_1, \alpha_2, \alpha_3$. Thus we can replace the sequence $W_1(P), W_2(P)$ by a regular sequence

$\bar{W}_1(P) := W_1(P) = w_1^{(1)} R_1(P)$,

$\bar{W}_2(P) := w_2^{(2)} R_2(P) + w_2^{(3)} R_3(P)$.

Note that $R_1(P) = 1 \cdot \alpha_1 + 2 \cdot \alpha_2 + 3 \cdot \alpha_3,\ R_2(P) = 1 \cdot \alpha_1 + 0 \cdot \alpha_2 + 0 \cdot \alpha_3,\ R_3(P) = 0 \cdot \alpha_1 + 1 \cdot \alpha_2 + 0 \cdot \alpha_3$. Now, we apply the above m-r-transformation, let $x_1 := y_1^1 y_2^1 y_3^0 = y_1 y_2,\ x_2 := y_1^2 y_2^0 y_3^1 = y_1^2 y_3,\ x_3 := y_1^3 y_2^0 y_3^0 = y_1^3$. So $PP\,(2.1)$ becomes $x_1^{\alpha_1} x_2^{\alpha_2} x_3^{\alpha_3} = (y_1 y_2)^{\alpha_1}(y_1^2 y_3)^{\alpha_2}(y_1^3)^{\alpha_3} = y_1^{\alpha_1+2\alpha_2+3\alpha_3} y_2^{\alpha_1} y_3^{\alpha_2}$. If we denote y_1, y_2, y_3 again by x_1, x_2, x_3, respectively, then by the above procedure, we have $\bar{W}_1(P) = \alpha_1$,

$\bar{W}_2(P) = w_2^{(2)} \alpha_2 + w_2^{(3)} \alpha_3$.

Theorem 2.4.2. Let the ordering Ω in $[x_1, \ldots, x_m]$ be generated by an irreducible sequence of weight functions of the length k and the rank r:

$$W_1(P), \ldots, W_k(P), \tag{2.19}$$

and assume that $s \geq 0$ and $U = C_0 < C_1 < \cdots < C_s$ is the complete sequence of comparability classes corresponding to Ω. Then $k = s$ and

$$C_\sigma = \{P \mid W_\kappa(P) = 0 \ \big(\kappa \in \{1, \ldots, k-\sigma\}\big),\ W_{k-\sigma+1}(P) \neq 0\} \quad \big(\sigma \in \{0, \ldots, s\}\big). \tag{2.20}$$

Proof. In order to prove Theorem 2.4.2, we introduce and discuss certain sets of PP's which are connected with the sequence (2.19). Define $U_\kappa := \{P \mid W_1(P) = \cdots = W_\kappa(P) = 0\}$ $\big(\kappa \in \{1, \ldots, k\}\big)$, $U_o := [x_1, \ldots, x_m]$, $U_{k+1} := \varnothing$ and $D_\kappa := U_{\kappa-1} - U_\kappa$ $\big(\kappa \in \{1, \ldots, k+1\}\big)$. By the definition, $D_\kappa = \{P \mid W_1(P) = \cdots = W_{\kappa-1}(P) = 0,\ W_\kappa(P) \neq 0\}$ $\big(\kappa \in \{1, \ldots, k\}\big)$ and $D_{k+1} = U_k$. Since $W_\kappa(P^{-1}) = -W_\kappa(P)$ $\big(\kappa \in \{1, \ldots, k\}\big)$, it follows that for $\kappa \in \{1, \ldots, k+1\}$, if $P \in D_\kappa$, then also $P^{-1} \in D_\kappa$.

We show that PP's $\in$ the same D_κ $\big(\kappa \in \{1, \ldots, k+1\}\big)$ if and only if they are comparable. Let $\kappa \in \{1, \ldots, k+1\}$ and $P, Q \in D_\kappa$. If $\kappa = k+1$, then $D_{k+1} = U_k$, and so $W_1(P) = \cdots = W_k(P) = W_1(Q) = \cdots = W_k(Q) = 0$. Thus $P \sim 1$ and $Q \sim 1$, so P, Q and 1 are comparable. It follows that $D_{k+1} = U_k = U = C_0$. Hence (2.20) holds for $\sigma = 0$. If $\kappa < k+1$, without loss of generality, we can assume that $P > 1$ and $Q > 1$ since we can replace P, Q by P^{-1}, Q^{-1}, respectively. It follows that $W_1(P) = \cdots = W_{\kappa-1}(P) = W_1(Q) = \cdots = W_{\kappa-1}(Q) = 0,\ W_\kappa(P) > 0,\ W_\kappa(Q) > 0$. We will find $\lambda, \mu \in \mathbb{Q}^+$ such that $P^\lambda < Q < P^\mu$. If $W_\kappa(P) = W_\kappa(Q)$, choose $\lambda = \frac{1}{2}$, $\mu = 2$, then $\lambda W_\kappa(P) < W_\kappa(Q) < \mu W_\kappa(P)$. So $W_\kappa(P^\lambda) < W_\kappa(Q) < W_\kappa(P^\mu)$.

Thus $P^\lambda < Q < P^\mu$. If $W_\kappa(P) < W_\kappa(Q)$, then choosing $\lambda = 1$ gives $P^\lambda = P < Q$. Note that there exists $\mu \in \mathbb{Q}^+$ such that $W_\kappa(Q) < \mu W_\kappa(P) = W_\kappa(P^\mu)$, so $Q < P^\mu$. If $W_\kappa(P) > W_\kappa(Q)$, then choosing $\mu = 1$ gives $Q < P = P^\mu$. Note that there exists $\lambda \in \mathbb{Q}^+$ such that $W_\kappa(P^\lambda) = \lambda W_\kappa(P) < W_\kappa(Q)$, so $P^\lambda < Q$. Thus P and Q are comparable.

Now assume that $1 < P \in D_\kappa$ and $1 < Q \in D_\lambda$ where $1 \leq \lambda < \kappa \leq k$. We see that $W_1(P) = \cdots = W_{\lambda-1}(P) = W_1(Q) = \cdots = W_{\lambda-1}(Q) = 0$ and $W_\lambda(P) = 0 < W_\lambda(Q)$. Let $\delta \in \mathbb{Q}^+$. Since $W_\kappa(Q^\delta) = \delta W_\kappa(Q)$ and $W_\kappa(Q^{-\delta}) = -\delta W_\kappa(Q)$ $\big(\kappa \in \{1, \ldots, k\}\big)$, $W_1(Q^\delta) = \cdots = W_{\lambda-1}(Q^\delta) = W_1(Q^{-\delta}) = \cdots = W_{\lambda-1}(Q^{-\delta}) = 0$, it follows that $W_\lambda(Q^{-\delta}) < 0 = W_\lambda(P)$ and $W_\lambda(P) = 0 < W_\lambda(Q^\delta)$, so $Q^{-\delta} < P < Q^\delta$. By property K, P and Q are not comparable.

Thus each D_κ $\big(\kappa \in \{1, \ldots, k+1\}\big)$ is identical with exactly one of the comparability class C_σ $\big(\sigma \in \{0, \ldots, s\}\big)$. Since $[x_1, \ldots, x_m] = \bigcup_{\kappa=1}^{k+1} D_\kappa$, it follows that for any $\sigma \in \{0, \ldots, s\}$, there exists exactly one $\kappa \in \{1, \ldots, k+1\}$ such that $C_\sigma = D_\kappa$. Thus $k = s$. From the last paragraph, we have that $D_\kappa < D_\lambda$ if $1 \leq \lambda < \kappa \leq k$. Then $U = D_{k+1} < D_k < \cdots < D_1$. Thus $C_\kappa = D_{k-\kappa+1}$ $\big(\kappa \in \{0, \ldots, k\}\big)$. Hence $C_\kappa = \{P \mid W_1(P) = \cdots = W_{k-\kappa}(P) = 0,\ W_{k-\kappa+1}(P) \neq 0\}$ $\big(\kappa \in \{1, \ldots, k\}\big)$, and Theorem 2.4.2 is proved. □

From Theorem 2.4.2, since the rank of (2.19) is r, $U = C_0$ is characterized by r linear homogeneous equations between the exponents $\alpha_1, \ldots, \alpha_m$. Then the dimension of U is $= m-r$. More generally, if we let $r_0 := 0$, $r_{k+1} := m$, then for $\kappa \in \{0, \ldots, k+1\}$, the dimension of each U_κ is $= m - r_\kappa$. Furthermore, for $\kappa \in \{1, \ldots, k+1\}$, the dimension of D_κ is $= (m - r_{\kappa-1}) - (m - r_\kappa) = r_\kappa - r_{\kappa-1}$. Finally, for $\kappa \in \{0, \ldots, k\}$, since $C_\kappa = D_{k-\kappa+1}$, the dimension of C_κ is $= r_{k-\kappa+1} - r_{k-\kappa}$.

2.5 Extreme aggregates of terms

We consider now the set of all polynomials in $x_1, \ldots, x_m$ with coefficients from an arbitrary field K. Define an **algebraic** polynomial as the sum of the terms $F := \sum_{\nu} c_\nu P_\nu$ where $c_\nu \in K \smallsetminus \{0\}$ and P_ν are algebraic PP's. Then we will say that any term $c_\nu P_\nu$ and the corresponding PP, P_ν are **contained in** F and write $c_\nu P_\nu \in F$, $P_\nu \in F$. If we write the polynomial F in the form $\sum c_\nu P_\nu$, then P_ν are assumed to be distinct PP's. In particular, if all PP's in F are rational (integer), we will call F **rational (integer)**. **From now on, by polynomial we mean an algebraic polynomial, unless otherwise specified.**

Let Λ he a mapping of each polynomial F upon a certain aggregate of its terms, $\bar{F}$. Assume that Λ has the following properties:

i. There is no PP, contained both in $\bar{F}$ and $F - \bar{F}$.

ii. If $F \not\equiv 0$, then $\bar{F} \not\equiv 0$.

iii. For any polynomials F_1, F_2, we have $\overline{F_1 F_2} = \bar{F}_1 \bar{F}_2$.

Then $\bar{F}$ will be called an **extreme aggregate** of F.

We easily see that for any PP P and $c \in K$, $\overline{cP} = cP$ and for a monomial polynomial F, $\bar{F} = F$.

A polynomial which is not a monomial, i.e. contains at least two different PP's, will be called a **proper polynomial**.

In the following, P,P_1,P_2,P_3 will denote general algebraic PP's, unless otherwise specified.

Using our mapping Λ we will now define an ordering Ω of PP's **induced by** Λ and prove that Ω is a regular ordering.

If P_1, P_2 are PP's, from the above postulates, it follows that either $\overline{P_1 + P_2} = P_1 + P_2$ or $\overline{P_1 + P_2} = P_1$ or $\overline{P_1 + P_2} = P_2$, and this is a complete disjunction. If

$\overline{P_1 + P_2} = P_1 + P_2$, we will say that P_1 and P_2 are **equivalent** (denoted by $P_1 \sim P_2$, $P_2 \sim P_1$). If $\overline{P_1 + P_2} = P_1$, we will say that P_1 is **higher than** P_2 and P_2 is **lower than** P_1 (denoted by $P_1 > P_2$, $P_2 < P_1$). And similarly if $\overline{P_1 + P_2} = P_2$.

The ordering Ω defined in this way satisfies obviously the postulates I and II of the definition of a regular ordering. To prove that the postulate IV is satisfied, Assume $P_1 > P_2$. Then $\overline{P_1P_3 + P_2P_3} = (\overline{P_1 + P_2})\bar{P_3} = P_1P_3$. Thus $P_1P_3 > P_2P_3$. This is the assertion of the postulate IV. We will prove that the postulate III is also satisfied later.

Proposition 2.5.1. Assume that F contains the term $c_1P_1 + c_2P_2$ where $P_1 \neq P_2$. Let $G := (P_1 + P_2)F$. We see that the term P_1P_2 in G has exactly the coefficient $c_1 + c_2$. Then

A. If $P_1 \sim P_2$ and $c_1P_1 \in \bar{F}$, then $c_2P_2 \in \bar{F}$.

Proof. Suppose that $c_2P_2 \notin \bar{F}$. From $P_1 \sim P_2$, we have $\bar{G} = (\overline{P_1 + P_2})\bar{F} = (P_1+P_2)\bar{F}$. Then $\bar{G}$ contains P_1P_2 with a coefficient c_1. But if P_1P_2 occurs in $\bar{G}$, it must have the same coefficient $c_1 + c_2$ as in G. This is a contradiction. □

B. If $P_1 > P_2$, then $c_2P_2 \notin \bar{F}$. Dually, if $P_1 < P_2$, then $c_1P_1 \notin \bar{F}$.

Proof. Suppose that $c_2P_2 \in \bar{F}$. From $P_1 > P_2$, we have $\bar{G} = (\overline{P_1 + P_2})\bar{F} = P_1\bar{F}$. Then $\bar{G}$ contains P_1P_2 with a coefficient c_2 which is again $\neq c_1 + c_2$. □

C. If $c_1P_1 \in \bar{F}$ and $c_2P_2 \in \bar{F}$, then $P_1 \sim P_2$.

Proof. If $P_1 > P_2$ or $P_1 < P_2$, then by B, $c_2P_2 \notin \bar{F}$ or $c_1P_1 \notin \bar{F}$, respectively. □

D. If $c_1P_1 \in \bar{F}$ but $c_2P_2 \notin \bar{F}$, then $P_1 > P_2$.

Proof. If $P_1 \sim P_2$, this contradicts A. If $P_1 < P_2$, this contradicts B. □

Now we will prove that Ω satisfies the postulate III of the definition of a regular ordering. Let $F := (P_1 + P_2)(P_2 + P_3) = P_1P_2 + P_1P_3 + P_2^2 + P_2P_3$. If $P_1 > P_2$ and $P_2 > P_3$, then $\bar{F} = (\overline{P_1 + P_2})(\overline{P_2 + P_3}) = P_1P_2$. Since $P_1P_2 \in \bar{F}$ but $P_2P_3 \notin \bar{F}$, by Proposition 2.5.1 D, it follows that $P_1P_2 > P_2P_3$. Multiplying by $1/P_2$, we have $P_1 > P_3$ since the postulate IV is satisfied. If $P_1 > P_2$ and $P_2 \sim P_3$, then $\bar{F} = (\overline{P_1 + P_2})(\overline{P_2 + P_3}) = P_1(P_2 + P_3) = P_1P_2 + P_1P_3$. It follows again that $P_1P_2 > P_2P_3$, so $P_1 > P_3$. Finally, if $P_1 \sim P_2$ and $P_2 > P_3$, then $\bar{F} = (\overline{P_1 + P_2})(\overline{P_2 + P_3}) = (P_1 + P_2)P_2 = P_1P_2 + P_2^2$. It follows again that $P_1P_2 > P_2P_3$, so $P_1 > P_3$. Thus III is proved. Moreover, properties A - D in Section 2.1 remain valid because they follow from the postulates I - IV. Hence Ω is a regular ordering of PP's.

For $c_1 \neq 0$ and $c_2 \neq 0$, we will say that c_1P_1 is **higher than** ($>$) or **equivalent to** ($\sim$) or **lower than** ($<$) c_2P_2 according as $P_1 > P_2$ or $P_1 \sim P_2$ or $P_1 < P_2$.

Theorem 2.5.2. A mapping Λ as defined above corresponds to a regular ordering Ω of PP's such that $\bar{F}$ is always the aggregate of all highest terms of F in the sense of Ω. Any regular ordering Ω can be induced by a mapping Λ which is uniquely determined by Ω.

Proof. Most assertions of Theorem 2.5.2 follow from what we did above. Now, we have only to prove that any given Ω is induced by the mapping Λ obtained by defining $\bar{F}$ as the aggregate of all highest terms of F. It is clear that properties i and ii hold. We have to prove that property iii also holds.

Denote the highest terms of F_1 by $a'_\kappa Q'_\kappa$ and all other terms by $b'_\nu T'_\nu$. Similarly, the highest terms of F_2 may be $a''_\lambda Q''_\lambda$ and all other terms $b''_\mu T''_\mu$. Then we can write

$$F_1 = \bar{F}_1 + \sum_{\nu} b'_\nu T'_\nu \text{ with } \bar{F}_1 = \sum_{\kappa} a'_\kappa Q'_\kappa,$$

$$F_2 = \bar{F}_2 + \sum_{\mu} b''_\mu T''_\mu \text{ with } \bar{F}_2 = \sum_{\lambda} a''_\lambda Q''_\lambda,$$

where the sum over ν and μ can be empty, and

$$\forall(\kappa, \kappa_1, \nu),\ Q'_\kappa \sim Q'_{\kappa_1}, Q'_\kappa > T'_\nu,$$

$$\forall(\lambda, \lambda_1, \mu),\ Q''_\lambda \sim Q''_{\lambda_1}, Q''_\lambda > T''_\mu.$$

Then we have

$$F_1F_2 = \bar{F}_1\bar{F}_2 + \sum_{\kappa,\mu} a'_\kappa b''_\mu Q'_\kappa T''_\mu + \sum_{\lambda,\nu} a''_\lambda b'_\nu Q''_\lambda T'_\nu + \sum_{\nu,\mu} b'_\nu b''_\mu T'_\nu T''_\mu,$$

$$\bar{F}_1\bar{F}_2 = \sum_{\kappa,\lambda} a'_\kappa a''_\lambda Q'_\kappa Q''_\lambda.$$

Note that $\bar{F}_1\bar{F}_2 \neq 0$ since $\bar{F}_1 \neq 0$ and $\bar{F}_2 \neq 0$. By the postulates IV and IV$'$ of the definition of a regular ordering, we have

$$\forall(\kappa, \kappa_1, \lambda, \lambda_1),\ Q'_\kappa Q''_\lambda \sim Q'_{\kappa_1} Q''_{\lambda_1},$$

$$\forall(\kappa, \kappa_1, \lambda, \lambda_1, \mu, \nu),\ Q'_\kappa Q''_\lambda > Q'_{\kappa_1} T''_\mu,\ Q'_\kappa Q''_\lambda > Q''_{\lambda_1} T'_\nu,\ Q'_\kappa Q''_\lambda > T'_\nu T''_\mu.$$

Thus $\overline{F_1F_2} = \bar{F}_1\bar{F}_2$, so property iii is proved.

Finally, let Ω_Λ be the ordering induced by the mapping Λ obtained by defining $\bar{F}$ as the aggregate of all highest terms of F in the sense of Ω. We will show that $\Omega = \Omega_\Lambda$. For any PP's P_1, P_2, we have that

$$P_1 \sim P_2 \text{ in the sense of } \Omega \Leftrightarrow \overline{P_1 + P_2} = P_1 + P_2 \Leftrightarrow P_1 \sim P_2 \text{ in the sense of } \Omega_\Lambda,$$

$$P_1 > P_2 \text{ in the sense of } \Omega \Leftrightarrow \overline{P_1 + P_2} = P_1 \Leftrightarrow P_1 > P_2 \text{ in the sense of } \Omega_\Lambda,$$

$$\text{and dually, } P_1 < P_2 \text{ in the sense of } \Omega \Leftrightarrow P_1 < P_2 \text{ in the sense of } \Omega_\Lambda.$$

Therefore $\Omega = \Omega_\Lambda$. □

Theorem 2.5.2 simply says that given an ordering Ω, its induced mapping Λ is uniquely determined and vice versa.

The number of the weight functions in a regular sequence, i.e. the length of this sequence, defining a regular ordering Ω depends only on Ω. If this number is 1, we will call that the ordering Ω and the mapping Λ induced by Ω are **monobaric**.

For the case $m = 1$, from the begining of the proof of Theorem 2.3.5, we see that any ordering of $[x_1]$ is always monobaric.

Note that there are orderings which are not monobaric. Then it is important for algebraic discussions to prove that it is quite sufficient to consider only monobaric orderings and mappings as long as we have to do with a fixed finite set of PP's.

Let S be a finite set of different PP's. A given ordering Ω induces the order relation between the elements of S, which we can call the **projection of Ω on S** (denoted by Ω_S). Let S^* be the set of all polynomials formed with the PP's from the set S with arbitrary coefficients from a field K. Then Ω induces for each of the polynomials from S^*, a mapping which will be denoted by Λ_S.

Theorem 2.5.3. Let Ω be a regular ordering, Λ the corresponding mapping of Ω, S a finite set of PP's, S^*, Ω_S and Λ_S are defined above. Then there exists a monobaric ordering Ω' such that if the corresponding mapping is denoted by Λ', we have $\Omega_S = \Omega'_S$ and $\Lambda_S = \Lambda'_S$.

Proof. By the postulates IV and IV′ of the definition of a regular ordering, it follows that the relations $P_1 > P_2,\ P_1 < P_2,\ P_1 \sim P_2$ can be written as $P_1/P_2 > 1,\ P_1/P_2 < 1,\ P_1/P_2 \sim 1$. Then it suffices to consider the effect of Ω on those quotients of the PP's from S which are $\gtrsim 1$. Denote the sequence of these quotients by $Q_\nu\ \big(\nu \in \{1,\dots,N\}\big)$. Assume that the ordering Ω corresponds a regular sequence of weight functions, of the length d,

$$W_1(P), W_2(P), \dots, W_d(P). \tag{2.21}$$

Note that $W_\kappa(Q_\nu) \geq 0\ \big(\kappa \in \{1,\dots,d\},\ \nu \in \{1,\dots,N\}\big)$. It suffices to show that, if $d > 1$, the sequence (2.21) can be replaced with a sequence containing less than d terms and corresponding to an ordering with the same effect on $Q_\nu\ \big(\nu \in \{1,\dots,N\}\big)$.

Reordering $Q_\nu\ \big(\nu \in \{1,\dots,N\}\big)$, if necessary, we can assume that for $N_1, N_2 \geq 0$,

$$\begin{aligned} &W_1(Q_\nu) > 0\ \big(\nu \in \{1,\dots,N_1\}\big), && W_1(Q_\nu) = 0\ (\nu > N_1),\\ &W_2(Q_\nu) > 0\ \big(\nu \in \{N_1+1,\dots,N_1+N_2\}\big), && W_2(Q_\nu) = 0\ (\nu > N_1+N_2). \end{aligned}$$

If $N_1 = 0$, we can obviously drop $W_1(P)$ and reduce d. If $N_1 > 0$, let $W^*(P) := W_1(P)+W_2(P)$. Then $W^*(Q_\nu) > 0\ \big(\nu \in \{1,\dots,N_1+N_2\}\big)$. Thus we can replace both weight functions $W_1(P), W_2(P)$ by $W^*(P)$ and reduce again d by 1. Hence Theorem 2.5.3 is proved. □

For $c \in K \setminus \{0\}$, we assign generally to cP the weight of P:

$$W(cP) := W(P).$$

A polynomial in which all terms have the same weight is called **isobaric**. We assign to each isobaric polynomial F the weight of any of its terms:

$$W(F) := W(P) \quad (P \in F).$$

If a polynomial F is not isobaric, then it can be decomposed into isobaric aggregates of terms,

$$F = \varphi_0 + \varphi_1 + \cdots + \varphi_k,$$

where each φ_κ $\big(\kappa \in \{0, \ldots, k\}\big)$ is isobaric and

$$W(\varphi_0) > W(\varphi_1) > \cdots > W(\varphi_k).$$

Then for a not isobaric polynomial F, we define $W(F)$ as the maximum weight of all of its terms:

$$W(F) := W(\varphi_0).$$

The above decomposition will be called simply **the decomposition into isobaric aggregates**, where the single aggregates are always ordered according to decreasing weights. Then the isobaric aggregate φ_0 will be called the **leading aggregate** of F. It is clear that $W(F) = W(\varphi_0) > W(F - \varphi_0)$.

2.6 Convex bodies and polyhedrons

First, we recall some properties of convex bodies and polyhedrons, which will be used later.

We usually denote a general point of the m-dimensional space $\mathbb{R}^m$ by A and its coordinates by $\alpha_1, \ldots, \alpha_m$.

A bounded and closed set of points, C, is called a **convex body** if it has the **convexity property**, i.e. if A_1, A_2 are two arbitrary points of C, then all points of the rectilinear segment $\langle A_1, A_2 \rangle$ also belong to C. The **dimension of C**, $\dim C$, is defined to be the smallest integer d such that C lies in a linear d-dimensional manifold.

If $d = 0$, then C consists only one point.

A **direction** η in $\mathbb{R}^m$ is defined hy m real numbers $w_1, \ldots, w_m$, not all zero, with the condition that η remains the same if $w_1, \ldots, w_m$ are multiplied by the same positive factor. If we multiply $w_1, \ldots, w_m$ by -1, we obtain the **opposite direction to** η, $-\eta$.

For any point $A \in \mathbb{R}^m$, denote $L_\eta(A) := \sum_{\mu=1}^{m} w_\mu \alpha_\mu$. Note that for $A', A'' \in \mathbb{R}^m$, we have $L_\eta(A' + A'') = L_\eta(A') + L_\eta(A'')$.

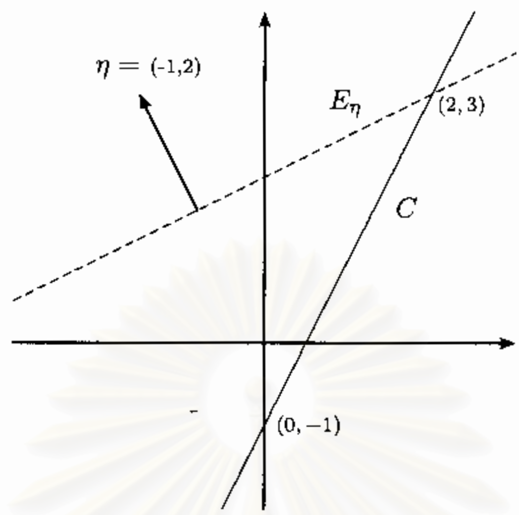
An $(m-1)$-dimensional plane normal to the direction η is the set of points A satisfying an equation

$$L_\eta(A) = d, \tag{2.22}$$

where d is an arbitrary real number. If we define d by $d := \max_{A \in C} L_\eta(A)$, then the plane (2.22) is called the **support plane of C in the direction** η (denoted by E_η). It is uniquely determined by the direction η. A convex body is uniquely determined by the set of all its supporting plane.

Denote $C_\eta := E_\eta \cap C$. Then C_η is again a convex body and if $C_\eta \subsetneq C$, we have $\dim C_\eta < \dim C$. The set C_η will be called a **linear boundary component of C**.

Example 2.6.1. Put $C := \{(\alpha_1, \alpha_2) \in \mathbb{R}^2 \mid 0 \le \alpha_1 \le 2,\ -1 \le \alpha_2 \le 3,\ \alpha_2 = 2\alpha_1 - 1\}$. Then C is a convex body in $\mathbb{R}^2$. Let $\eta := (-1, 2)$ be a direction in $\mathbb{R}^2$. Then for any $(\alpha_1, \alpha_2) \in \mathbb{R}^2$, $L_\eta(\alpha_1, \alpha_2) = -\alpha_1 + 2\alpha_2$. Note that $\max_{(\alpha_1,\alpha_2) \in C} L_\eta(\alpha_1, \alpha_2) = \max_{(\alpha_1,\alpha_2) \in C} \{-\alpha_1 + 2(2\alpha_1 - 1)\} = \max_{(\alpha_1,\alpha_2) \in C} \{3\alpha_1 - 2\} = 3 \cdot 2 - 2 = 4$.
Thus $E_\eta = \{(\alpha_1, \alpha_2) \in \mathbb{R}^2 \mid -\alpha_1 + 2\alpha_2 = 4\}$ and $C_\eta = \{(2, 3)\}$.



If $\dim C = d > 0$, then the **total boundary of C** (from the m-dimensional 'point of view'), ∂C, is $\bigcup_\eta C_\eta$.

If $\dim C_\eta = 0$, then C_η contains only one point and this point will be called a **snmmit** of C.

A linear boundary component of C_η is also a linear boundary component of C.

Assume C is a d-dimensional convex body. If there exists only a finite number of different linear boundary components of C, C is called a **convex polyhedron**. For an m-dimensional convex polyhedron C, there always exists a finite set of different directions $\eta_1, \ldots, \eta_N$ such that $\partial C = \bigcup_{\nu=1}^{N} C_{\eta_\nu}$, where each C_{η_ν} $\big(\nu \in \{1, \ldots, N\}\big)$ has the dimension $m-1$ and different C_{η_ν} $\big(\nu \in \{1, \ldots, N\}\big)$ have in common at most a linear boundary component of a dimension $< m-1$. These η_ν $\big(\nu \in \{1, \ldots, N\}\big)$ are uniquely determined.

If we have a finite set of points $A_1, \ldots, A_N$, then the 'smallest' convex polyhedron which contains $A_1, \ldots, A_N$ is the set of all points representable in the form $A = \sum_{\nu=1}^{N} t_\nu A_\nu$ where $t_1, \ldots, t_N \geq 0$ and $t_1 + \cdots + t_N = 1$. This polyhedron will be denoted by $\langle A_1, \ldots, A_N \rangle$.

All summits of $\langle A_1, \ldots, A_N \rangle$ belong to the set of the points $\{A_1, \ldots, A_N\}$.

A convex polyhedron has a finite number of summits $S_1, \dots, S_N$ and can be always form as $\langle S_1, \dots, S_N \rangle$.

Assume C' and C'' are two convex bodies in $\mathbb{R}^m$. Then $\{A' + A'' \mid A' \in C',\ A'' \in C''\}$ is also a convex body which is denoted by $C' + C''$.

If $A' = (\alpha'_1, \dots, \alpha'_m) \in C'$, $A'' = (\alpha''_1, \dots, \alpha''_m) \in C''$ and $\eta = (w_1, \dots, w_m)$ is a direction in $\mathbb{R}^m$, then we have $L_\eta(A') - d' \leq 0$ and $L_\eta(A'') - d'' \leq 0$, where $d' = \max_{A' \in C'} L_\eta(A')$ and $d'' = \max_{A'' \in C''} L_\eta(A'')$. Thus $L_\eta(A' + A'') - (d' + d'') = \big(L_\eta(A') + L_\eta(A'')\big) - (d' + d'') = \big(L_\eta(A') - d'\big) + \big(L_\eta(A'') - d''\big) \leq 0$. Note that the equality holds if and only if $A' \in C'_\eta$ and $A'' \in C''_\eta$. For any direction η, it follows that $L_\eta(A) = d' + d''$ is a supporting plane for $C' + C''$ and

$$(C' + C'')_\eta = C'_\eta + C''_\eta. \tag{2.23}$$

It is easy to see that if both C' and C'' are polyhedrons, then $C' + C''$ is also a polyhedron. Because in this case there are only a finite number of different ones among the terms $C'_\eta + C''_\eta$ on the right of (2.23).

Consider in particular the case $m = 2$, of a two-dimensional plane. Then convex polyhedrons become convex polygons. If in particular a convex polygon is a segment $\langle P_1, P_2 \rangle$, then it has to be considered as consisting of two segments of equal length but opposite directions, $\overrightarrow{P_1P_2} \cup \overleftarrow{P_1P_2}$.

We provide now our convex two-dimensional polygons with the orientation, going along the boundary in the positive sense with respect to the inside. By (2.23), it follows that the oriented sides of the polygon $C' + C''$ can only have the directions occurring in the sides of C' and of C''. Then we obtain $C' + C''$ by decomposing C' and C'' into the single oriented sides and reordering these sides in the sense of increasing angle with a fixed direction.

Now, it follows that if a triangle T is the sum of two convex polygons T_1, T_2, none of which reduces to a single point, then both T_1 and T_2 must also be triangles similar to T.

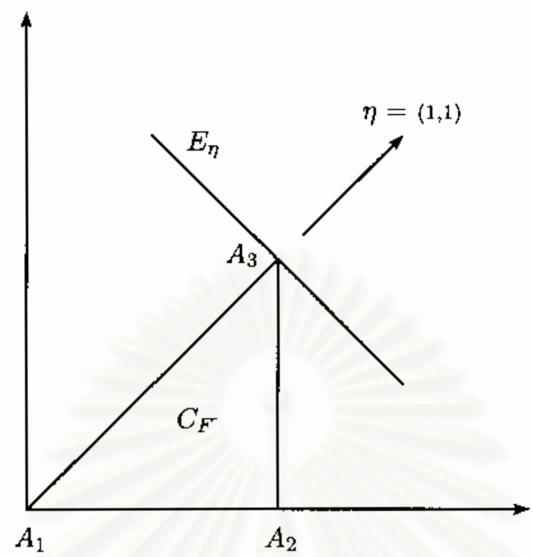
2.7 The baric polyhedron

A total view of all possible extreme aggregates in a given polynomial can be obtained by using the **baric polyhedrons** which we are going to introduce now.

Assume F is an algebraic polynomial in the form $F = \sum_{\nu=1}^{n} c_\nu P_\nu$ where $c_\nu \in K \setminus \{0\}$ $\big(\nu \in \{1, \ldots, n\}\big)$ and P_ν $\big(\nu \in \{1, \ldots, n\}\big)$ are distinct algebraic PP's of the form (2.1). Any PP of the form (2.1) corresponds to a **representative point**, A, of $\mathbb{R}^m$ with coordinates $\alpha_1, \ldots, \alpha_m$. We also define A to be the representative point of cP with $c \in K \setminus \{0\}$. Then in this way n terms of F correspond to n different points $A_1, \ldots, A_n$. The polyhedron, $C_F := \langle A_1, \ldots, A_n \rangle$, will be called the **baric polyhedron of the polynomial F**.

For a direction η, if the linear boundary component $(C_F)_\eta$ contains the representative points of some terms cP of F, then we will say that these terms **lie on** $(C_F)_\eta$ and write this as $cP \in (C_F)_\eta$, $P \in (C_F)_\eta$.

Example 2.7.1. For $m = 2$, let $P_1 := 1$, $P_2 := x_1$, $P_3 := x_1 x_2$ and $F := P_1 + P_2 + P_3$. Then the representative points of P_1, P_2, P_3 are $A_1 := (0, 0)$, $A_2 := (1, 0)$, $A_3 := (1, 1)$, respectively. Thus $C_F = \langle (0, 0), (1, 0), (1, 1) \rangle$. Let $\eta := (1, 1)$ be a direction in $\mathbb{R}^2$. Then for any $(\alpha_1, \alpha_2) \in \mathbb{R}^2$, $L_\eta(\alpha_1, \alpha_2) = \alpha_1 + \alpha_2$. We see that $\max_{(\alpha_1, \alpha_2) \in C_F} L_\eta(\alpha_1, \alpha_2) = \max_{(\alpha_1, \alpha_2) \in C_F} \alpha_1 + \alpha_2 = 2$. Hence $(E_F)_\eta = \{(\alpha_1, \alpha_2) \mid \alpha_1 + \alpha_2 = 2\}$ and $(C_F)_\eta = \{(1, 1)\} = \{A_3\}$. So $P_3 \in (C_F)_\eta$.



Theorem 2.7.2. Let F be an algebraic polynomial. For any mapping Λ as defined in Section 2.5, there exists a direction η such that $\bar{F}$ consists of all terms of F lying on $(C_F)_\eta$.

For a given direction η, if F^* is the sum of all terms of F lying on $(C_F)_\eta$, then there exists a monobaric mapping Λ for which $\bar{F} = F^*$. More generally:

Theorem 2.7.3. Consider a finite number of algebraic polynomials $F_1, \ldots, F_N$ and the corresponding baric polyhedrons $C_{F_\nu} =: C_\nu$ $\big(\nu \in \{1, \ldots, N\}\big)$. Then any mapping Λ corresponds to a direction η such that for $\nu \in \{1, \ldots, N\}$, $\bar{F}_\nu$ consists of all terms of F_ν lying on $(C_\nu)_\eta$.

Conversely, if we take an arbitrary direction η and for $\nu \in \{1, \ldots, N\}$, denote the sum of all terms of F_ν lying on $(C_\nu)_\eta$ by F_ν^*, then there exists a monobaric mapping Λ for which $\bar{F}_\nu = F_\nu^*$ $\big(\nu \in \{1, \ldots, N\}\big)$.

Proof of Theorem 2.7.3. Assume a general mapping Λ as defined in Section 2.5. By Theorem 2.5.3, the mapping $F_\nu \mapsto \bar{F}_\nu$ $\big(\nu \in \{1, \ldots, N\}\big)$ can be also achieved by a monobaric mapping and then we can assume Λ to be monobaric. Let $W(P) :=$

$w_1\alpha_1 + \cdots + w_m\alpha_m$ be the corresponding weight function. Choose the direction $\eta := (w_1, \ldots, w_m)$. Then $W(P) \equiv L_\eta(A)$. For each $\nu \in \{1, \ldots, N\}$, put $g_\nu := \max_{P \in F_\nu} W(P)$. It follows that

$$W(P) = g_\nu \ (P \in \bar{F}_\nu),\ W(P) < g_\nu \ (P \in F_\nu - \bar{F}_\nu) \quad \big(\nu \in \{1, \ldots, N\}\big). \tag{2.24}$$

We see that $g_\nu = \max_{A \in C_\nu} L_\eta(A)$ $\big(\nu \in \{1, \ldots, N\}\big)$. Thus for $\nu \in \{1, \ldots, N\}$, each plane $L_\eta(A) - g_\nu = 0$ represents a supporting plane in the direction η to C_ν. For $\nu \in \{1, \ldots, N\}$, let $P \in F_\nu$ and $A \in C_\nu$ be the representative point of P. Since $P \in \bar{F}_\nu \Leftrightarrow W(P) = g_\nu \Leftrightarrow L_\eta(A) = g_\nu \Leftrightarrow A \in (C_\nu)_\eta \Leftrightarrow P \in (C_\nu)_\eta$, it folllows that $\bar{F}_\nu$ consists of all terms of F_ν lying on $(C_\nu)_\eta$.

Conversely, assume $\eta := (w_1, \ldots, w_m)$ is an arbitrary direction. For each $\nu \in \{1, \ldots, N\}$, put $g_\nu := \max_{A \in C_\nu} L_\eta(A)$. Then the supporting plane of C_ν in the direction η is $L_\eta(A) - g_\nu = 0$. Define $W(P) := L_\eta(A)$. We have

$$W(P) = g_\nu \ (P \in F_\nu^*),\ W(P) < g_\nu \ (P \in F_\nu - F_\nu^*) \quad \big(\nu \in \{1, \ldots, N\}\big).$$

Comparing this with (2.24), we see that $\bar{F}_\nu = F_\nu^*$ for the monobaric mapping Λ defined by the weight function W(P). □

Theorem 2.7.4. If F and G are two algebraic polynomials in $x_1, \ldots, x_m$, we have

$$C_{FG} = C_F + C_G.$$

Proof. Let η be an arbitrary direction. Define the weight function $W_\eta(P) := L_\eta(A)$, where A is the representative point of a PP, P. Put $f_\eta := \max_{A \in C_F} L_\eta(A)$ and $g_\eta := \max_{A \in C_G} L_\eta(A)$. Then the supporting planes of C_F and C_G in the direction η are $L_\eta(A) -$

$f_\eta = 0$ and $L_\eta(A) - g_\eta = 0$, respectively. It follows that the supporting plane of $C_F + C_G$ is $L_\eta(A) - (f_\eta + g_\eta) = 0$. Assume Λ is the monobaric mapping defined by $W_\eta(P)$. By the proof of Theorem 2.7.3, for any PP's, $P \in F$ and $Q \in G$, we have

$$W_\eta(P) - f_\eta \begin{cases} = 0 & (P \in \bar{F}) \\ < 0 & (P \in F - \bar{F}), \end{cases}$$

$$W_\eta(Q) - g_\eta \begin{cases} = 0 & (Q \in \bar{G}) \\ < 0 & (Q \in G - \bar{G}). \end{cases}$$

Note that $W_\eta(PQ) - (f_\eta + g_\eta) = \big(W_\eta(P) + W_\eta(Q)\big) - (f_\eta + g_\eta) = \big(W_\eta(P) - f_\eta\big) + \big(W_\eta(Q) - g_\eta\big)$. Then

$$W_\eta(PQ) - (f_\eta + g_\eta) \begin{cases} = 0 & (P \in \bar{F},\ Q \in \bar{G}) \\ < 0 & (P \in F - \bar{F}) \text{ or } (Q \in G - \bar{G}). \end{cases} \tag{2.25}$$

Now, let S be an arbitrary PP from FG. Then if $S \in \overline{FG}$, since $\overline{FG} = \bar{F}\bar{G}$, S can be written as PQ where $P \in \bar{F}$ and $Q \in \bar{G}$. From (2.25), it follows that

$$W_\eta(S) - (f_\eta + g_\eta) = 0 \quad (S \in \overline{FG}).$$

On the other hand, if $S \in FG - \overline{FG}$, then S can be written as PQ, $P \in F$, $Q \in G$, where either $P \in F - \bar{F}$ or $Q \in G - \bar{G}$. From (2.25), it follows that

$$W_\eta(S) - (f_\eta + g_\eta) < 0 \quad (S \in FG - \overline{FG}).$$

Since the same relations must hold for the supporting plane of C_{FG} in the direction

η, we see that C_{FG} and C_F+C_G have the same supporting plane $L_\eta(A)-(f_\eta+g_\eta)=0$ in every direction. Therefore $C_{FG}=C_F+C_G$. □

Among all extreme aggregates of terms contained in a polynomial F, we consider in particular those aggregates which consist of one term only. Then they correspond to the summits of C_F and will be called ***S* terms of *F***.

Let F be a polynomial and P^* an S term of F. Assume that $F = GH$ where G and H are polynomials. Consider all weight functions $W(P)$ such that P^* is the highest term of F with respect to $W(P)$.

We will show that there is exactly one S term of G and one S term of H which are the highest terms of G and H, respectively, with respect to these weight functions $W(P)$.

To see this, take one of the weight functions $W(P)$ and the corresponding mapping Λ. Then we have $P^* = \bar{F} = \overline{GH} = \bar{G}\bar{H}$. Thus both G and H are monomials and there exists only one pair of terms of G and H such that their product is exactly P^*. Let $W_1(P)$ and $W_2(P)$ be weight functions such that P^* is the highest term of F with respect to both $W_1(P)$ and $W_2(P)$. Then there exist monomials $\bar{G}_1, \bar{G}_2, \bar{H}_1, \bar{H}_2$ such that $P^* = \bar{G}_1\bar{H}_1 = \bar{G}_2\bar{H}_2$ where $\bar{G}_1, \bar{G}_2$ are the highest terms of G with respect to $W_1(P)$ and $W_2(P)$, respectively and $\bar{H}_1, \bar{H}_2$ are the highest terms of H with respect to $W_1(P)$ and $W_2(P)$, respectively. Since $W_1(P^*) = W_1(\bar{G}_2\bar{H}_2) = W_1(\bar{G}_2) + W_1(\bar{H}_2) \le W_1(\bar{G}_1) + W_1(\bar{H}_1) = W_1(\bar{G}_1\bar{H}_1) = W_1(P^*)$, $W_1(\bar{G}_2) + W_1(\bar{H}_2) = W_1(\bar{G}_1) + W_1(\bar{H}_1)$. Since $W_1(\bar{G}_2) \le W_1(\bar{G}_1)$ and $W_1(\bar{H}_2) \le W_1(\bar{H}_1)$, $W_1(\bar{G}_2) = W_1(\bar{G}_1)$ and $W_1(\bar{H}_2) = W_1(\bar{H}_1)$. Thus $\bar{G}_1 = \bar{G}_2$ and $\bar{H}_1 = \bar{H}_2$ because $\bar{G}_1, \bar{G}_2, \bar{H}_1, \bar{H}_2$ are monomials. Therefore $\bar{G}$ must be the same for all of our $W(P)$ and the same holds for $\bar{H}$.

The corresponding result holds also for a product of more than two polynomials.

CHAPTER III

IRREDUCIBILITY

3.1 General observations on reducibility of polynomials

In this chapter, we assume that K is a field of characteristic 0.

Let F be an algebraic polynomial given in the form $F = \sum_{\nu} c_\nu P_\nu$ where $c_\nu \in K \setminus \{0\}$ and P_ν are distinct algebraic PP's. We will say that F is **reducible** if we can write $F = GH$ where G and H are proper polynomials. Then G and H are called **proper factors** of F. And F is called **irreducible** if F is not reducible. Although primarily one is interested in this connection in integer polynomials, it is more convenient to operate with rational polynomials. Indeed, dealing with rational polynomials we can use the m-r-transformations as defined in Section 2.1 of Chapter II, with $a_{\mu\nu} \in \mathbb{Z}$ such that $\det[a_{\mu\nu}] = \pm 1$ and this often considerably simplify the discussion.

On the other hand, it can be seen that a reducibility problem for rational polynomials is essentially equivalent to a reducibility problem for integer polynomials. To see this, we will give the definition of a **primitive** polynomial.

An integer polynomial which is not divisible by any of the variables $x_1, \ldots, x_m$ will be called a **primitive** polynomial.

Proposition 3.1.1.

A. The product of two primitive polynomials is again primitive.

B. The product of a primitive polynomial with a PP, which is $\neq 1$, is not primitive.

C. Any rational polynomial F can be written as $F = PF^*$ where P is a PP and F^* is a primitive polynomial. F^* is uniquely determined by F. We will call F^* the **primitive kernel** of F.

D. If $F = GH$ where F, G, H are proper polynomials, then $F^* = G^*H^*$ where the primitive polynomials G^* and H^* are also proper.

Proof. A and B are obvious. To show C, let F be any rational polynomial.

Case 1. F is an integer polynomial. If F is primitive, choose $P = 1$ and $F^* = F$. Otherwise, let P be a PP such that F/P is primitive. Then we choose $F^* = F/P$.

Case 2. F is not an integer polynomial, i.e. F contains a rational PP which is not integer. Let P_1 be a rational PP such that F/P_1 is an integer polynomial. By Case 1, $F/P_1 = P_2F^*$ where P_2 is a PP and F^* is a primitive polynomial. Then we choose $P = P_1P_2$.

To show that F^* is uniquely determined by F, let P_1, P_2 be PP's and F_1^*, F_2^* primitive polynomials such that $F = P_1F_1^* = P_2F_2^*$. If $P_1 \neq P_2$, then $P_1/P_2 \neq 1$. By B, we have that $F_2^* = (P_1/P_2)F_1^*$ is not primitive, which is a contradiction. Thus $P_1 = P_2$, so $F_1^* = F_2^*$.

Finally, to show D, assume that $F = P_1F^*$, $G = P_2G^*$, $H = P_3H^*$ where P_1, P_2, P_3 are PP's and F^*, G^*, H^* are primitive kernels of F, G, H, respectively. By the uniqueness of F^*, we have that $F^* = G^*H^*$. Since G is proper and $G = P_2G^*$, G^* is not a constant. Since G^* is primitive, G^* is not a nonconstant monomial. Then G^* is not a monomial, i.e. G^* is proper. Similarly, H^* is proper. □

By Proposition 3.1.1 D, we see that the kernel of a reducible rational polynomial is reducible in the domain of integer polynomials.

In some cases it can be proved that a given rational polynomial F is irreducible not only in the domain of rational polynomials but even in the domain of all algebraic polynomials, i.e. F cannot be represented as a product $F = GH$ where G and H are proper algebraic polynomials. On this level of investigation, it is reasonable to consider also the irreducibility or reducibility of algebraic polynomials.

Assume that we have the decomposition of the algebraic polynomial F, $F = GH$ where G and H are proper algebraic polynomials. Let D be the smallest common denominator of all exponents in F, G, H. Then we obtain the decomposition of $F(x_1^D, \ldots, x_m^D)$ in two proper rational factors. However it is more convenient to operate with algebraic polynomials as such.

In dealing with such problems we can use again the m-r-transformations as defined in Section 2.1 of Chapter II, with $a_{\mu\nu} \in \mathbb{Q}$ such that $\det[a_{\mu\nu}] \neq 0$.

We will say that PP's $P_1, \ldots, P_k$ are **algebraically independent** over a field K if there is no nonzero rational polynomial $F(y_1, \ldots, y_k)$ with coefficients from K such that $F(P_1, \ldots, P_k) = 0$. And we will say that PP's $P_1, \ldots, P_k$ are **algebraically dependent** over K if they are not algebraically independent over K.

Proposition 3.1.2. If PP's $P_1, \ldots, P_k$ are algebraically dependent, then there exist $s_\kappa \in \mathbb{Z}$ $\big(\kappa \in \{1, \ldots, k\}\big)$, not all zero, such that $P_1^{s_1} P_2^{s_2} \ldots P_k^{s_k} = 1$.

Proof. Since $P_1, \ldots, P_k$ are algebraically dependent, there exist $\sigma_\kappa^{(\nu)} \in \mathbb{Z}$ $\big(\kappa \in \{1, \ldots, k\}\big)$ and $c_\nu \in K \setminus \{0\}$ such that

$$\sum_\nu c_\nu P_1^{\sigma_1^{(\nu)}} P_2^{\sigma_2^{(\nu)}} \ldots P_k^{\sigma_k^{(\nu)}} = 0.$$

If this relation is satisfied after introducing the expressions of each $P_1 \ldots, P_k$ in the variables $x_1, \ldots, x_m$, then there must exist at least two different expressions

$$P_1^{\sigma'_1} \ldots P_k^{\sigma'_k},\ P_1^{\sigma''_1} \ldots P_k^{\sigma''_k}$$

which become identical when expressed in $x_1, \ldots, x_m$, so we can cancel one another. Thus we have the relation

$$P_1^{\sigma_1'-\sigma_1''} \ldots P_k^{\sigma_k'-\sigma_k''} = 1$$

where $\sigma_\kappa' - \sigma_\kappa'' \in \mathbb{Z}$ $\big(\kappa \in \{1, \ldots, k\}\big)$ and not all of them are zero. $\square$

A polynomial F will be called **homogeneous** if all PP's in F have the same dimension.

Proposition 3.1.3. Let $k, D \in \mathbb{N}$ and $c_\nu \in K \setminus \{0\}$ $\big(\nu \in \{1, \ldots, k\}\big)$.
If $c_1x_1^D + c_2x_2^D + \cdots + c_kx_k^D = FG$, where F and G are proper integer polynomials, then F and G must be homogeneous polynomials of the dimensions which are smaller than D and the derivatives $F_{x_\kappa}, G_{x_\kappa} \neq 0$ $\big(\kappa \in \{1, \ldots, k\}\big)$.

Proof. Observe that F can be decomposed into $F_1 + F_2 + \cdots + F_r$ where $r \geq 1$, each F_i $\big(i \in \{1, \ldots, r\}\big)$ is a nonzero homogeneous polynomial of the dimension a_i and $0 \leq a_1 < a_2 < \cdots < a_r$. Also, G can be decomposed into $G_1 + G_2 + \cdots + G_s$ where $s \geq 1$, each G_j $\big(j \in \{1, \ldots, s\}\big)$ is a nonzero homogeneous polynomial of the dimension b_j and $0 \leq b_1 < b_2 < \cdots < b_s$. Note that $F_1G_1, F_rG_s \neq 0$ and F_1G_1, F_rG_s are of the dimensions a_1b_1, a_rb_s, respectively. From $c_1x_1^D + c_2x_2^D + \cdots + c_kx_k^D = FG$, then $a_1b_1 = a_rb_s$. Thus $r = s = 1$, so F and G are homogeneous polynomials. Denote the dimensions of F and G by a and b, respectively. Since F and G are proper, $a, b > 0$. From $c_1x_1^D + c_2x_2^D + \cdots + c_kx_k^D = FG$, then $a + b = D$. Thus $a, b < D$. Suppose that there exists $\kappa \in \{1, \ldots, k\}$ such that the derivative $F_{x_\kappa} = 0$. It follows that G must contains an integer PP P which can be written as $P = x_\kappa^D Q$ where Q is an integer PP. So $a \geq D$, which is a contradiction. Hence the derivative $F_{x_\kappa} \neq 0$ $\big(\kappa \in \{1, \ldots, k\}\big)$. Similarly, the derivative $G_{x_\kappa} \neq 0$ $\big(\kappa \in \{1, \ldots, k\}\big)$. $\square$

Lemma 3.1.4. The polynomial

$$x_1^D + x_2^D + \cdots + x_k^D \quad (k \geq 3, D \geq 1) \tag{3.1}$$

is irreducible in the domain of integer polynomials.

Proof. First, we will assume $D \geq 3$. Suppose that

$$x_1^D + x_2^D + \cdots + x_k^D = FG, \tag{3.2}$$

where F and G are proper integer polynomials. By Proposition 3.1.3, F and G must be homogeneous polynomials. Denote the dimensions of F and G by a and b, respectively. From the proof of Proposition 3.1.3, we have $a, b < D$. Differentiating both sides of (3.2) with respect to x_k, we obtain $Dx_k^{D-1} = F_{x_k}G + G_{x_k}F$. Write $F_{x_k} = x_k^\alpha f$, $G_{x_k} = x_k^\beta g$, where f and g are polynomials which are not divisible by x_k. By Proposition 3.1.3, we have that the derivatives $F_{x_k}, G_{x_k} \neq 0$. Then $0 \leq \alpha \leq a-1 \leq D-2$ and $0 \leq \beta \leq b-1 \leq D-2$. Without loss of generality, we can assume $\alpha \leq \beta$ since we can interchange F and G. Note that $Dx_k^{D-1} = x_k^\alpha fG + x_k^\beta gF = x_k^\alpha(fG + x_k^{\beta-\alpha}gF)$. Multiplying both sides by $x_k^{-\alpha}$,

$$Dx_k^{D-1-\alpha} = fG + x_k^{\beta-\alpha}gF. \tag{3.3}$$

Since $\alpha \leq D-2$, $D-1-\alpha \geq 1$. Thus $Dx_k^{D-1-\alpha}$ is divisible by x_k. If G is divisible by x_k, then $x_1^D + x_2^D + \cdots + x_k^D = FG$ is also divisible by x_k, which is impossible. Thus G is not divisible by x_k, so fG is also not divisible by x_k. It follows that $\beta = \alpha$. Taking $x_k = 0$ in (3.3) and denoting the corresponding values of f, g, F, G by f_0, g_0, F_0, G_0, respectively, it follows that

$$f_0 G_0 = -g_0 F_0. \tag{3.4}$$

Note that both F_0 and G_0 have no nonconstant factors which are monomials. Otherwise $x_1^D + x_2^D + \cdots + x_{k-1}^D = F_0 G_0$ would be divisible by the nonconstant monomial, which is impossible. If F_0 and G_0 have a common proper factor, say H, then $x_1^D + x_2^D + \cdots + x_{k-1}^D = F_0 G_0$ is divisible by H^2. So $x_1^D + x_2^D + \cdots + x_{k-1}^D = F_0 G_0 = H^2 I$ where I is an integer polynomial. Differentiating both sides with respect to $x_1, \ldots, x_k$, we obtain

$$\begin{aligned} Dx_1^{D-1} &= 2HH_{x_1} I + H^2 I_{x_1}, \\ Dx_2^{D-1} &= 2HH_{x_2} I + H^2 I_{x_2}, \\ &\vdots \\ Dx_{k-1}^{D-1} &= 2HH_{x_{k-1}} I + H^2 I_{x_{k-1}}. \end{aligned}$$

It follows that $Dx_1^{D-1}, Dx_2^{D-1}, \ldots, Dx_{k-1}^{D-1}$ have a proper factor H in common, which is impossible since $k \geq 3$. Thus F_0 and G_0 have no proper factors in common. By (3.4), we have that $f_0 G_0$ is divisible by F_0 and $g_0 F_0$ is divisible by G_0. Let J be a nonconstant irreducible factor of F_0. Then J is not a monomial, i.e. J is proper. Thus J is not a factor of G_0. Since $f_0 G_0$ is divisible by F_0, $f_0 G_0$ is also divisible by J. So f_0 must be divisible by J. Hence f_0 is divisible by F_0. And we can prove in the similar way that g_0 is divisible by G_0. But the dimensions of f_0 and g_0 are smaller than the dimensions of F_0 and G_0, respectively. This is a contradiction, and Lemma 3.1.3 is proved in the case $D \geq 3$.

For the case $D = 1$, it is obvious that $x_1 + x_2 + \cdots + x_k$ is always irreducible in the domain of integer polynomials.

Finally, assume $D = 2$. Suppose that $x_1^2 + x_2^2 + \cdots + x_k^2 = FG$, where F and G are proper integer polynomials. By Proposition 3.1.3, F and G must be homogeneous polynomials of the dimensions 1 and the derivatives $F_{x_\kappa}, G_{x_\kappa} \neq 0$ $(\kappa \in \{1, \ldots, k\})$. Then $F = a_1x_1 + \cdots + a_kx_k$, $G = b_1x_1 + \cdots + b_kx_k$ where $a_\kappa, b_\kappa \in K \setminus \{0\}$ $(\kappa \in \{1, \ldots, k\})$. Note that $a_1b_2, a_2b_1 \neq 0$. So FG contains the term $(a_1b_2 + a_2b_1)x_1x_2$ but $x_1^2 + x_2^2 + \cdots + x_k^2$ does not contain such term. This is a contradiction. $\square$

Corollary 3.1.5. The polynomial

$$x_1^D + x_2^D + \cdots + x_k^D + 1 \quad (k \geq 2, D \geq 1) \tag{3.5}$$

is irreducible in the domain of integer polynomials.

Proof. We claim that $x_1, \ldots, x_{k-1}, x_k/x_{k+1}$ are algebraically independent. Suppose not, then, by Proposition 3.1.2, there exist $s_\kappa \in \mathbb{Z}$ $(\kappa \in \{1, \ldots, k\})$, not all zero, such that $x_1^{s_1} \ldots x_{k-1}^{s_{k-1}}(x_k/x_{k+1})^{s_k} = 1$. So we have $x_1^{s_1} \ldots x_{k-1}^{s_{k-1}} x_k^{s_k} x_{k+1}^{-s_k} = 1$. This contradicts the fact that $x_1, \ldots, x_{k+1}$ are algebraically independent. Replacing x_k in (3.5) with x_k/x_{k+1}, we have

$$x_1^D + \cdots + x_{k-1}^D + (x_k/x_{k+1})^D + 1. \tag{3.6}$$

It can be seen that if (3.6) is irreducible in the domain of integer polynomials, then so is (3.5). Next, claim that $x_1x_{k+1}, \ldots, x_{k-1}x_{k+1}, x_k, x_{k+1}$ are algebraically independent. Suppose not, then, by Proposition 3.1.2, there exist $s_\kappa \in \mathbb{Z}$ $(\kappa \in \{1, \ldots; k+1\})$, not all zero, such that $(x_1x_{k+1})^{s_1} \ldots (x_{k-1}x_{k+1})^{s_{k-1}} x_k^{s_k} x_{k+1}^{s_{k+1}} = 1$. So we have $x_1^{s_1} \ldots x_k^{s_k} x_{k+1}^{s_1 + \cdots + s_{k-1} + s_{k+1}} = 1$. This contradicts the fact that $x_1, \ldots, x_{k+1}$ are algebraically independent. Then multiplying (3.6) by x_{k+1}^D, we have

$$(x_1x_{k+1})^D + (x_2x_{k+1})^D + \cdots + x_k^D + x_{k+1}^D. \tag{3.7}$$

By Lemma 3.1.4, it follows that (3.7) is irreducible in the domain of integer polynomials. Then so is (3.6), and Corollary 3.1.5 is proved. □

Corollary 3.1.6. The polynomials (3.1) and (3.5) are irreducible even in the domain of algebraic polynomials.

Proof. Suppose that

$$x_1^D + x_2^D + \cdots + x_k^D = FG, \tag{3.8}$$

where F and G are proper algebraic polynomials. Let M be the smallest common denominator of all exponents in F and G. Replacing each x_κ $\big(\kappa \in \{1, \ldots, k\}\big)$ in (3.8) with x_κ^M $\big(\kappa \in \{1, \ldots, k\}\big)$, we have

$$x_1^{DM} + x_2^{DM} + \cdots + x_k^{DM} = F(x_1^M, \ldots, x_k^M)G(x_1^M, \ldots, x_k^M).$$

Note that $F(x_1^M, \ldots, x_k^M), G(x_1^M, \ldots, x_k^M)$ are proper rational polynomials. Write

$$F(x_1^M, \ldots, x_k^M)G(x_1^M, \ldots, x_k^M) = PF_1G_1,$$

where P is a rational PP and F_1, G_1 are integer polynomials such that F_1G_1 is not divisible by Q for any integer PP $Q \neq 1$. Denote $P := x_1^{\alpha_1} \ldots x_k^{\alpha_k}$ where $\alpha_\kappa \in \mathbb{Z}$ $\big(\kappa \in \{1, \ldots, k\}\big)$. Let $P_1 := x_1^{\max\{0,\alpha_1\}} \ldots x_k^{\max\{0,\alpha_k\}}$ and $P_2 := x_1^{\min\{0,\alpha_1\}} \ldots x_k^{\min\{0,\alpha_k\}}$. Obviously, $P = P_1P_2$. Then we have

$$P_2^{-1}(x_1^{DM} + x_2^{DM} + \cdots + x_k^{DM}) = P_1F_1G_1.$$

Note that both P_1, P_2^{-1} are integer PP's. If $P_1 \neq 1$, then P_2^{-1} is not divisible by P_1, so $x_1^{DM} + x_2^{DM} + \cdots + x_k^{DM}$ must be divisible by P_1, which is a contradiction. Thus $P_1 = 1$. And if $P_2^{-1} \neq 1$, then P_1 is not divisible by P_2^{-1}, so F_1G_1 must be divisible by P_2^{-1}, which is a contradiction. Thus $P_2^{-1} = 1$, so $P_2 = 1$. Hence $P = 1$. It follows that

$$x_1^{DM} + x_2^{DM} + \cdots + x_k^{DM} = F_1G_1.$$

This contradicts Lemma 3.1.4. Therefore (3.1) is irreducible in the domain of algebraic polynomials. That (3.5) is irreducible in the domain of algebraic polynomials is proved in the similar way. □

Corollary 3.1.7. Let $n \geq 3$ and $P_1, \ldots, P_n$ be algebraic PP's in $x_1, \ldots, x_m$ which are algebraically independent. Then the polynomial

$$\sum_{\nu=1}^{n} c_\nu P_\nu \quad (c_1c_2 \ldots c_n \neq 0) \tag{3.9}$$

is irreducible even in the domain of algebraic polynomials.

Proof. First, we show that $n \leq m$. Suppose $n > m$. If we take $P_1^{s_1}P_2^{s_2} \ldots P_n^{s_n} = 1$ and introduce the expressions of $P_1, P_2, \ldots, P_n$ in the variables $x_1, \ldots, x_m$, then this leads to m equations with n unknowns $(s_1, \ldots, s_n)$. Thus there is a nontrivial solution $s_\kappa \in \mathbb{Z}$ $\big(\kappa \in \{1, \ldots, n\}\big)$, not all zero, such that $P_1^{s_1}P_2^{s_2} \ldots P_n^{s_n} = 1$. This contradicts the assumption that $P_1, \ldots, P_n$ are algebraically independent, and so $n \leq m$. By an m-r-transformation, we can introduce m new variables y_ν such that $y_\nu := P_\nu$ $\big(\nu \in \{1, \ldots, n\}\big)$. Then (3.9) becomes

$$\sum_{\nu=1}^{n} c_\nu y_\nu. \tag{3.10}$$

Introducing $z_\nu := c_\nu y_\nu$ $\big(\nu \in \{1, \ldots, n\}\big)$, (3.10) becomes

$$z_1 + z_2 + \cdots + z_n. \tag{3.11}$$

By Corollary 3.1.6, it follows that (3.11) is irreducible in the domain of algebraic polynomials. Then so are (3.10) and (3.9). □

Corollary 3.1.7 can be generalized to

Theorem 3.1.8. If $n+1$ algebraic PP's are such that $P_1/P_0, \ldots, P_n/P_0$ are algebraically independent, then the algebraic polynomial

$$\sum_{\nu=0}^{n} c_\nu P_\nu \quad (c_0 c_1 \ldots c_n \neq 0,\ n \geq 2) \tag{3.12}$$

is irreducible in the domain of all algebraic polynomials.

Proof. Let $Q_\nu := \dfrac{c_\nu}{c_0} P_\nu / P_0 \ \big(\nu \in \{1, \ldots, n\}\big)$. Then dividing the polynomial (3.12) by $c_0 P_0$, we have

$$1 + Q_1 + \cdots + Q_n. \tag{3.13}$$

Since $Q_1, \ldots, Q_n$ are algebraically independent, we can again introduce n new variables $z_\nu := Q_\nu \ \big(\nu \in \{1, \ldots, n\}\big)$. Then (3.13) becomes

$$1 + z_1 + \cdots + z_n. \tag{3.14}$$

By Corollary 3.1.6, it follows that (3.14) is irreducible in the domain of algebraic polynomials. Then so are (3.13) and (3.12). □

3.2 A criterion for absolute irreducibility

Assume that a polynomial F with coefficients from a field K is a proper irreducible polynomial with respect to K. Then it can happen that there exists an algebraic extension of K, K^*, such that F has a proper factor $\varphi(x_1, \ldots, x_m)$ with coefficients from K^*. In this case, we say that F becomes **reducible in K^***. But if there does not exist any algebraic extension of K in which F becomes reducible, F is called **absolutely irreducible**.

Example 3.2.1. 1) $x_1^2 + x_2^2 + x_3^2$ is an absolutely irreducible polynomial (by Corollary 3.1.6).

2) $x_1^2 - 2x_2^2$ is irreducible with respect to $\mathbb{Q}$ but becomes reducible in $\mathbb{Q}(\sqrt{2})$.

We show that $x_1^2 - 2x_2^2$ is irreducible with respect to $\mathbb{Q}$. suppose that $x_1^2 - 2x_2^2 = FG$, where F and G are proper integer polynomials with coefficients from $\mathbb{Q}$. By Proposition 3.1.3, F and G must be homogeneous polynomials of the dimensions 1 and the derivatives $F_{x_1}, F_{x_2}, G_{x_1}, G_{x_2} \neq 0$. Then $F = a_1x_1 + a_2x_2,\ G = b_1x_1 + b_2x_2$ where $a_1, a_2, b_1, b_2 \in \mathbb{Q} \setminus \{0\}$. Thus $x_1^2 - 2x_2^2 = FG = a_1b_1x_1^2 + (a_1b_2 + a_2b_1)x_1x_2 + a_2b_2x_2^2$. Comparing the coefficients on both sides, we obtain $a_1b_1 = 1,\ a_1b_2 + a_2b_1 = 0,\ a_2b_2 = -2$. So $b_1 = \frac{1}{a_1},\ b_2 = -\frac{2}{a_2}$, and $-\frac{2a_1}{a_2} + \frac{a_2}{a_1} = 0$. Multiplying by a_1a_2, we have $-2a_1^2 + a_2^2 = 0$. It follows that $\left(\frac{a_2}{a_1}\right)^2 = 2$, which is impossible.

Note that $x_1^2 - 2x_2^2 = (x_1 - \sqrt{2}x_2)(x_1 + \sqrt{2}x_2)$. Hence $x_1^2 - 2x_2^2$ is reducible in $\mathbb{Q}(\sqrt{2})$.

We will develop a criterion which allows us in many cases to prove the absolute irreducibility.

Assume that we have the decomposition of the integer polynomial F, $F = GH$ where G and H are proper integer polynomials. The factor polynomials G and H can he multiplied with an arbitrary coefficient $t \neq 0$ and $\frac{1}{t}$, respectively. Then in this way the coefficients of G and H shifted into a field K^* which is possibly too large. We see that if the coefficients of G are denoted by $\alpha_1, \alpha_2, \ldots$ and the coefficients of H are denoted by $\beta_1, \beta_2, \ldots$, then all products $\alpha_\nu\beta_\mu$ lie in the 'smallest' field over K, $K(\alpha_\nu\beta_\mu)$, in which the decomposition $F = GH$ can be obtained by using suitable common factors. To see this, assume $G = \alpha_1P_1 + \cdots + \alpha_rP_r$ and $H =$

$\beta_1 Q_1 + \cdots + \beta_s Q_s$, where $r, s \geq 1$ and for $\nu \in \{1, \ldots, r\}$, $\mu \in \{1, \ldots, s\}$, P_ν, Q_μ are PP's and $\alpha_\nu, \beta_\mu \in K \setminus \{0\}$. Let $G' := \beta_1 G = \alpha_1\beta_1 P_1 + \cdots + \alpha_r\beta_1 P_r$ and $H' := \frac{1}{\beta_1}H = Q_1 + \frac{\beta_2}{\beta_1}Q_2 + \cdots + \frac{\beta_s}{\beta_1}Q_s$. Then $F = GH = G'H'$ and we see that all coefficients of G' and H' lie in $K(\alpha_\nu\beta_\mu)$. In particular, all coefficients of G and H lie in $K(\alpha_\nu\beta_\mu)$ if one of them is $= 1$. Therefore we can **norm** the polynomial F by taking the coefficient one of its S terms $= 1$. Then the correspondings S term in G and H have the coefficients 1. In this case we will say that F, G, H are **normed**. Observe that if a polynomial, $f(x)$, in one variable x, is normed, then all of its coefficients are rational functions of its roots.

Note that if there exists the field K^* over K in which F becomes reducible, K^* need not to be finite or algebraic over K. However, it can be always replaced with a finite algebraic extension of K. To prove this, assume the decomposition

$$F(x_1, \ldots, x_m) = G(x_1, \ldots, x_m)H(x_1, \ldots, x_m)$$

where all coefficients of G and H lie in K^* and F, G, H are normed. Using the Kronecker's substitution, $x_1 = x, x_2 = x^g, x_3 = x^{g^2}, \ldots, x_m = x^{g^{m-1}}$. Then we obtain

$$F(x, x^g, \ldots, x^{g^{m-1}}) = G(x, x^g, \ldots, x^{g^{m-1}})H(x, x^g, \ldots, x^{g^{m-1}})$$

where if the integer g is chosen sufficiently large, then no terms in G and H are mixed up and the sequence of the coefficients remains the same. So we have on both sides polynomials in one variable x and the roots of these polynomials are the roots of the left hand polynomial which has coefficients in K. Thus these roots are algebraic with respect to K. Since G and H are normed, their coefficients are rational functions of their roots which are also algebraic with respect to K. Hence F becomes reducible in the field K^* obtained from K by adjunction of all coefficients of G and H. We see that the field K^* is a finite algebraic extension of K.

Theorem 3.2.2. Consider m variables $x_1, \ldots, x_m$, algebraically independent with respect to K, and an integer polynomial $F(x_1, \ldots, x_m)$ with coefficients from K and irreducible with respect to K. Assume that F has a proper integer factor $\psi(x_1, \ldots, x_m)$ which is absolutely irreducible and assumed to be normed. Let K^* be the field obtained from K by adjunction of all coefficients of ψ and let $k := [K^* : K]$.

Then each S term of F is k-th power of the corresponding S term of ψ.

In particular, if the greatest common divisor of the exponents of all S terms of F is 1, then F is absolutely irreducible.

Proof. Let n be the degree of ψ in $x_1, \ldots, x_m$ (i.e. the maximal dimension of all PP's occurring in ψ). Let n' be the smallest degree of an absolutely irreducible integer factor of F and let φ_1 be such factor which assumed to be normed, where if $n' = n$, we take $\varphi_1 := \psi$. Let K' be the field obtained from K by adjunction of all coefficients of φ_1 and let $k' := [K' : K]$. Since the characteristic of K is 0, K' can be written as $K(\rho_1)$ where ρ_1 is a primitive element of K', of degree k' with respect to K.

Then each coefficients of φ_1 can be written as an integer polynomials in ρ_1, so we can write $\varphi_1 = \phi(\rho_1, x_1, \ldots, x_m)$ where ϕ is an integer polynomial of its $m+1$ variables with coefficients from K. Let $\rho_2, \ldots, \rho_{k'}$ be all conjugates of ρ_1 and let $\varphi_\kappa := \phi(\rho_\kappa, x_1, \ldots, x_m)$ $\left(\kappa \in \{1, \ldots, k'\}\right)$. It follows that each φ_κ $\left(\kappa \in \{1, \ldots, k'\}\right)$ is also a factor of F and must be absolutely irreducible, since otherwise F would have a proper factor of degree $< n'$. Moreover, all φ_κ are distinct since otherwise the number of conjugates of ρ_1 would be $\leq k' - 1$ and all coefficients of φ_1 would lie in an extension of K of degree $< k'$. Since φ_1 is normed, $\varphi_2, \ldots, \varphi_{k'}$ are also normed. We claim that $\varphi_\kappa / \varphi_\lambda$ cannot be independent of $x_1, \ldots, x_m$ if $\kappa \neq \lambda$. Suppose that

$\varphi_\kappa/\varphi_\lambda = a$ where $\kappa \neq \lambda$ and $a \in K'$. Then $\varphi_\kappa = a\varphi_\lambda$. Since φ_κ and φ_λ are normed, $a = 1$. Thus $\varphi_\kappa = \varphi_\lambda$, which is a contradiction. Hence F must be divisible by $\prod_{\kappa=1}^{k'} \varphi_\kappa(x_1, \dots, x_m)$. Note that $\prod_{\kappa=1}^{k'} \phi(y_\kappa, x_1, \dots, x_m)$ is a symmetric polynomial over $K[x_1, \dots, x_m]$ in k' variables, $y_1, \dots, y_{k'}$. Since $\rho_1, \dots, \rho_{k'}$ are all roots of the minimal polynomial of ρ_1 over K, it follows that $\prod_{\kappa=1}^{k'} \phi(\rho_\kappa, x_1, \dots, x_m) \in K[x_1, \dots, x_m]$, i.e. $\prod_{\kappa=1}^{k'} \varphi_\kappa(x_1, \dots, x_m) \in K[x_1, \dots, x_m]$. And $\prod_{\kappa=1}^{k'} \varphi_\kappa(x_1, \dots, x_m)$ is also normed because $\varphi_1, \dots, \varphi_{k'}$ are normed. Since F is irreducible in K, $F = b \prod_{\kappa=1}^{k'} \varphi_\kappa(x_1, \dots, x_m)$ where $b \in K$. But ψ is a factor of F, then it must be divisible by φ_κ for some $\kappa \in \{1, \dots, k'\}$. Since ψ is absolutely irreducible, $\psi = c\varphi_\kappa$ where $c \in K$. Thus $n' = n$, so $\psi = \varphi_\kappa$. Then we obtain $K' = K^*$ and $k' = k$.

Observe that if $\psi = \varphi_1$ contains a term $c(\rho_1)x_1^{\alpha_1} \dots x_m^{\alpha_m}$ where $c(\rho_1)$ is a nonzero polynomial in ρ_1 with coefficients from K, then each φ_κ $\big(\kappa \in \{1, \dots, k\}\big)$ contains the term $c(\rho_\kappa)x_1^{\alpha_1} \dots x_m^{\alpha_m}$ where $c(\rho_\kappa)$ is the conjugate of $c(\rho_1)$. Then $c(\rho_\kappa) \neq 0$. We see that different φ_κ contain exactly the same PP and therefore have identical baric polyhedrons: $C_\psi = C_{\varphi_1} = \dots = C_{\varphi_k}$. It follows that if an S term P^* of F corresponds to the S term $c(\rho_1)x_1^{\alpha_1} \dots x_m^{\alpha_m}$ in ψ, then the corresponding term in φ_κ $\big(\kappa \in \{1, \dots, k\}\big)$ is $c(\rho_\kappa)x_1^{\alpha_1} \dots x_m^{\alpha_m}$ and therefore $P^* = x_1^{k\alpha_1} \dots x_m^{k\alpha_m} \prod_{\kappa=1}^{k} c(\rho_\kappa)$.

Finally, assume that the greatest common divisor of the exponents of all S terms of F is 1. Then $k = 1$. Thus $F = b\varphi_1(x_1, \dots, x_m)$, so F is absolutely irreducible. Therefore Theorem 3.2.2 is proved. □

From Theorem 3.2.2, it follows that the degrees of all highest terms of F in any of the possible lexicographic orderings are divisible by k.

3.3 An analogue of Eisenstein-Schönemann theorem

Let J be the set of all integer polynomials in $x_1, \ldots, x_m$ with coefficients from a field K. We will consider a weight function $W(F)$ such that $W(x_\nu) > 0$ $\big(\nu \in \{1, \ldots, m\}\big)$ and the corresponding monoharic mapping. We will show that the additivity property of $W(F)$ remains conserved for not necessarily isobaric polynomials. Let F and G be polynomials from J which decomposed into isobaric aggregates:

$$F = \varphi_0 + \varphi_1 + \cdots + \varphi_k,$$

$$G = \psi_0 + \psi_1 + \cdots + \psi_l.$$

Since the leading aggregate of a product is the product of the leading aggregates of factors, the leading aggregate of FG is $\varphi_0\psi_0$, and it follows that

$$W(FG) = W(\varphi_0\psi_0) = W(\varphi_0) + W(\psi_0) = W(F) + W(G).$$

We are now going to prove a lemma which is an analogue to a certain degree of the Eisenstein-Schönemann theorem in the theory of numbers.

Lemma 3.3.1. Let z be a variable which is independent of J.
Consider the polynomial

$$Z := \varphi + \sum_{\pi=1}^{p} \psi_\pi z^{\pi k} + \chi z^n, \tag{3.15}$$

where $n > pk \geq 2$, φ, χ and ψ_π $\big(\pi \in \{1, \ldots, p\}\big)$ are polynomials from J and $\varphi\chi \neq 0$.
Assume that

$$W(\varphi) > \max\{W(\chi), W(\psi_1), \ldots, W(\psi_p)\}, \tag{3.16}$$

the polynomial φ has no multiple factors and $\gcd(\varphi, \chi, \psi_1, \ldots, \psi_p) = 1$.

Suppose that Z is a product of two polynomials depending on z:

$$Z = FG, \tag{3.17}$$

$$F = f_0 + f_1 z^{u_1} + \cdots + f_s z^{u_s}, \quad 0 < u_1 < \cdots < u_s, \; s \geq 1, \tag{3.18}$$

$$G = g_0 + g_1 z^{v_1} + \cdots + g_t z^{v_t}, \quad 0 < v_1 < \cdots < v_t, \; t \geq 1, \tag{3.19}$$

where $f_\sigma, g_\tau \in J \setminus \{0\}$ $\big(\sigma \in \{0, \ldots, s\},\; \tau \in \{0, \ldots, t\}\big)$.

Then $\gcd(\varphi, \psi_1, \ldots, \psi_p) = 1$, all exponents u_σ, v_τ $\big(\sigma \in \{0, \ldots, s\},\; \tau \in \{0, \ldots, t\}\big)$ are divisible by k and therefore n is also divisible by k.

Proof. Let J_z be the set of all integer polynomials in z with coefficients from J. By (3.16), we can choose $\epsilon > 0$ such that $W(\varphi) > W(\psi_\pi) + n\epsilon$ $\big(\pi \in \{1, \ldots, p\}\big)$, $W(\varphi) > W(\chi) + n\epsilon$. In order to define a weight function in J_z whose restriction on J is W, it suffices to put $W(z) := \epsilon$. Then $W(\psi_\pi z^{\pi k}) = W(\psi_\pi) + \pi k W(z) = W(\psi_\pi) + \pi k\epsilon \leq W(\psi_\pi) + pk\epsilon < W(\psi_\pi) + n\epsilon < W(\varphi)$ $\big(\pi \in \{1, \ldots, p\}\big)$ and $W(\chi z^n) = W(\chi) + nW(z) = W(\chi) + n\epsilon < W(\varphi)$, so $W(Z) = W(\varphi)$ and $W(Z - \varphi) < W(\varphi)$. From (3.17) - (3.19), we can write $Z = f_0 g_0 + \phi z$ where $\phi \in J_z$, comparing this with (3.15), it follows that $f_0 g_0 = \varphi$, so $W(f_0) + W(g_0) = W(f_0 g_0) = W(\varphi)$. Note that $\gcd(f_0, g_0) = 1$ since $\varphi = f_0 g_0$ has no multiple factors. Denote the leading aggregate of φ by $\bar{\varphi}$ and the leading aggregates of f_0 and g_0 by $\bar{f}_0$ and $\bar{g}_0$, respectively. Since the leading aggregate of a product is the product of the leading aggregates of factors, $\bar{\varphi} = \bar{f}_0 \bar{g}_0$. But $\bar{\varphi}$ is in (3.15), then $\bar{\varphi}$ is also the leading aggregate of Z. From (3.17), it follows that $\bar{f}_0$ and $\bar{g}_0$ are the leading aggregates of F and G, respectively. Thus $W(F) = W(f_0) > W(F - f_0)$ and $W(G) = W(g_0) > W(F - g_0)$. In particular,

$$W(f_\sigma) < W(f_0) \; \big(\sigma \in \{1, \ldots, s\}\big) \quad \text{and} \quad W(g_\tau) < W(g_0) \; \big(\tau \in \{1, \ldots, t\}\big). \tag{3.20}$$

We are going to prove that $\gcd(\varphi, \psi_1, \ldots, \psi_p) = 1$. Suppose not, then there exists an irreducible nonconstant polynomial ω from J which is a common divisor of φ and ψ_π $(\pi \in \{1, \ldots, p\})$. Then we have that $FG = Z \equiv \chi z^n = f_s g_t z^n \pmod{\omega}$. Let $F_1 := H_0 z^{U_0} + \cdots + H_{s_1} z^{U_{s_1}}$, $G_1 := K_0 z^{V_0} + \cdots + K_{t_1} z^{V_{t_1}}$ be polynomials from J_z such that $F \equiv F_1 \pmod{\omega}$ and $G \equiv G_1 \pmod{\omega}$. If one of the expressions F_1, G_1 consists of more than one term, then we have that

$$\chi z^n \equiv FG \equiv H_0 K_0 z^{U_0+V_0} + \cdots + H_{s_1} K_{t_1} z^{U_{s_1}+V_{t_1}} \pmod{\omega} \tag{3.21}$$

where $U_{s_1} + V_{t_1} > U_0 + V_0$. Since $H_0, K_0, H_{s_1}, K_{t_1}$ are not divisible by ω, so are $H_0 K_0$ and $H_{s_1} K_{t_1}$. Thus (3.21) is impossible. It follows that $F \equiv f_s z^{u_s} \pmod{\omega}$ and $G \equiv g_t z^{v_t} \pmod{\omega}$. Then $f_0 \equiv g_0 \equiv 0 \pmod{\omega}$. Hence $\varphi = f_0 g_0$ have the factor ω^2, which is a contradiction.

In the following part of the proof, the notation $o(z^N)$ means an integer polynomial which is divisible by z^{N+1}.

Suppose that not all u_σ are divisible by k. Let u_{σ_0} be the first u_σ in (3.18) which is not divisible by k. So $u_{\sigma_0} = lk + \alpha$ where $\alpha, l \in \mathbb{Z}$, $0 < \alpha < k$, $l \geq 0$. Then F can be rewritten, ordered in ascending powers of z, as

$$F = \sum_{\lambda=0}^{l} \gamma_\lambda z^{\lambda k} + \gamma z^{lk+\alpha} + o(z^{lk+\alpha}), \quad \gamma := f_{\sigma_0} \neq 0,$$

where not all γ_λ need be $\neq 0$. If G can be written as $G = \sum_{\lambda=0}^{l} \delta_\lambda z^{\lambda k} + o(z^{lk+\alpha})$, then the product $Z = FG$ must contain the term $\gamma g_0 z^{lk+\alpha}$, which cannot be cancelled. Since $u_{\sigma_0} \leq u_s < u_s + v_t = n$, $\gamma g_0 z^{lk+\alpha} = \gamma g_0 z^{u_{\sigma_0}} \neq \chi z^n$. This is a contradiction. Thus there exists $\tau_0 \in \{0, \ldots, t\}$ such that $v_{\tau_0} = rk + \beta$ where $\beta, r \in \mathbb{Z}$, $0 < \beta < k$, $r \geq 0$ and $rk + \beta \leq lk + \alpha$. Then G can be rewritten, ordered in ascending powers of z, as

$$G = \sum_{\rho=0}^{r} \delta_\rho z^{\rho k} + \delta z^{rk+\beta} + \cdots, \quad \delta := g_{\tau_0} \neq 0.$$

If $rk+\beta < lk+\alpha$, then we can interchange F and G and arrive at a contradiction as done above. Thus we have only to consider the case $lk+\alpha = rk+\beta$. So $l = r$ and $\alpha = \beta$. Then FG must contain the term $(f_0\delta + g_0\gamma)z^{lk+\alpha}$. Since $lk+\alpha$ is not divisible by k and $< n$, $f_0\delta + g_0\gamma = 0$, so $f_0 g_{\tau_0} = -g_0 f_{\sigma_0}$. Since $\gcd(f_0, g_0) = 1$, f_0 and g_0 have no nontrivial common divisors in J. Thus $\frac{g_{\tau_0}}{g_0}$ and $\frac{f_{\sigma_0}}{f_0}$ must be polynomials from J, say $f := \frac{f_{\sigma_0}}{f_0}$ and $g := \frac{g_{\tau_0}}{g_0}$. Then $f_{\sigma_0} = f_0 f$ and $g_{\tau_0} = g_0 g$, so $W(f_{\sigma_0}) = W(f_o) + W(f) \geq W(f_0)$ and $W(g_{\tau_0}) = W(g_o) + W(g) \geq W(g_0)$, which contradicts (3.20). Finally, it follows that n is divisible by k since $n = u_s v_t$. Therefore Lemma 3.3.1 is proved. □

3.4 An application of Puiseux developments

For $a \in \mathbb{Q}$, we will denote the greatest integer which is $\leq a$ by $[a]$.

Lemma 3.4.1. Let $n, m \in \mathbb{N}$ and put

$$r := n\left[\frac{m+1}{2}\right] - 1, \tag{3.22}$$

$$Z^* := x^m + y^{nm} + f(x,y),$$

where $f(x,y)$ is an integer polynomial with numerical coefficients such that $f(0,0) \neq 0$ and for every PP, $x^\lambda y^\kappa$, which occurs in f, we have $\lambda n + \kappa \leq r$.

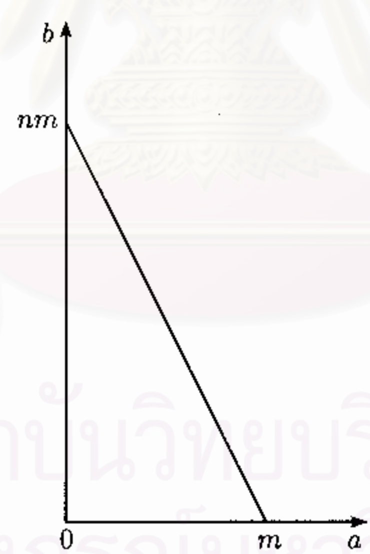
Then Z^* is absolutely irreducible in the domain of integer polynomials.

Proof. By (3.22), we obtain

$$r \leq \frac{n(m+1)}{2} - 1 = nm\left(\frac{1}{2} + \frac{1}{2m} - \frac{1}{nm}\right) \leq nm\left(1 - \frac{1}{nm}\right) < nm.$$

Then every PP, $x^\lambda y^\kappa$, which occurs in f, we have $\lambda n \leq \lambda n + \kappa \leq r < nm$, so $\lambda < m$ and $\kappa < nm$. Thus the degree of f in x is $< m$. We claim that Z^* cannot have a proper factor which is independent of x. Suppose that $Z^* = FG$ where F and G are proper integer polynomials and F is independent of x. Then G can be written in the form $G = g(y)x^m + G_1$ where the degree of G_1 in x is $< m$. Thus $Z^* = FG = F\big(g(y)x^m + G_1\big) = Fg(y)x^m + FG_1$. Since F is independent of x, the degree of FG_1 in x is $< m$. Comparing the coefficients of x^m on both sides, we have $1 = Fg(y)$, so $F = 1$, which is a contradiction, and the claim is verified. For $m = 1$, it follows that if Z^* is reducible, then Z^* must have a proper factor which is independent of x, contradicting the claim. So Z^* is irreducible for $m = 1$. Now, assume that $m \geq 2$.

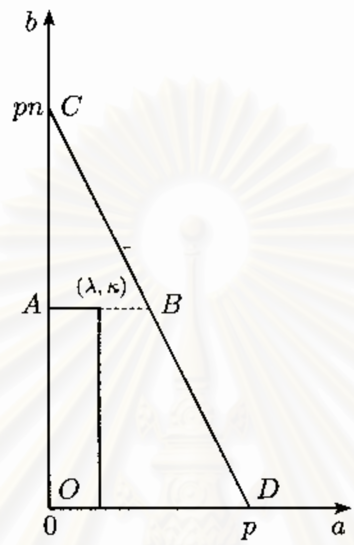
Under our assumption, we see that the baric diagram of Z^* is:



Suppose that $Z^* = FG$ where F and G are proper integer polynomials. By the above claim, we have that the degrees of F and G with respect to x must be > 0. Since the degree of $Z^* = FG$ in x is m, it follows that the degree of F in x or the degree of G in x must be $\leq \dfrac{m}{2}$. Let p be the degree of F in x. We can assume that $p \leq \dfrac{m}{2}$ by interchanging F and G if necessary. By Theorem 2.7.4, we have

$C_{Z^*} = C_{FG} = C_F + C_G$. Since the baric polygon of Z^* is a triangle, the baric polygons of F and G must also be triangles similar to the baric triangle of Z^*.

Then the baric triangle of F is :



So the degree of F with respect to y is pn. Write $F = \sum_{\lambda,\kappa} a_{\lambda\kappa} x^\lambda y^\kappa$. From the above diagram, we have that for any λ, κ, $\frac{\lambda}{p} \leq \frac{AB}{OD} = \frac{AC}{OC}$ and $\frac{\kappa}{pn} = \frac{OA}{OC}$. Then $\frac{\lambda}{p} + \frac{\kappa}{pn} \leq \frac{AC}{OC} + \frac{OA}{OC} = 1$, so $\kappa \leq n(p-\lambda)$. Rewriting F as $F = \sum_{\lambda=0}^{p} x^\lambda f_{p-\lambda}(y)$. For $\lambda \in \{0, 1, \ldots, p\}$, the degree of $f_{p-\lambda}(y)$ is $\leq n(p-\lambda)$.

The function $x(y)$, defined by $Z^* = 0$, has m Puiseux developments in decreasing powers of y in the neighbourhood of $y = \infty$. Since the Newton diagram of Z^* is the hypotenuse of its baric triangle, the first terms of these Puiseux developments are obtained from

$$x^m + y^{nm} = 0, \; x = \epsilon y^n, \; \epsilon^m = -1.$$

Then we have $|x| \sim |y|^n$, with $y \to \infty$. For $\lambda \in \{0, 1, \ldots, p\}$, since the degree of $f_{p-\lambda}(y)$ is $\leq n(p-\lambda)$, $f_{p-\lambda}(y) = O(y^{n(p-\lambda)})$ $(y \to \infty)$. Since every PP, $x^\lambda y^\kappa$, which occurs in f, we have $\lambda n + \kappa \leq r$, it follows that $f(x,y) = O(y^r)$ $(y \to \infty)$. Then $\frac{f(x,y)}{y^{nm}} = O\left(\frac{1}{y^{nm-r}}\right)$ $(y \to \infty)$. From $Z^* = 0$, we obtain

$$x^m = -y^{nm}\left(1+\frac{f(x,y)}{y^{nm}}\right) = -y^{nm}\left(1+O\left(\frac{1}{y^{nm-r}}\right)\right), \text{ so}$$
$$x = \epsilon y^n\left(1+O\left(\frac{1}{y^{nm-r}}\right)\right), \quad \epsilon^m = -1.$$

It follows that for $\lambda \in \{1,\ldots,p\}$,

$$x^\lambda = \epsilon^\lambda y^{\lambda n}\left(1+O\left(\frac{1}{y^{nm-r}}\right)\right) = \epsilon^\lambda y^{\lambda n} + \epsilon^\lambda y^{\lambda n} O\left(\frac{1}{y^{nm-r}}\right) = \epsilon^\lambda y^{\lambda n} + O\left(\frac{1}{y^{n(m-\lambda)-r}}\right),$$

and multiplying by $f_{p-\lambda}(y)$, we have

$$\begin{aligned} x^\lambda f_{p-\lambda}(y) &= \epsilon^\lambda y^{\lambda n} f_{p-\lambda}(y) + O\left(\frac{1}{y^{n(m-\lambda)-r}}\right) f_{p-\lambda}(y) \\ &= \epsilon^\lambda y^{\lambda n} f_{p-\lambda}(y) + O\left(\frac{1}{y^{n(m-p)-r}}\right), \end{aligned}$$

where the relation corresponding to $\lambda = 0$ is trivial.

It is easy to see that $\left[\frac{m}{2}\right] + \left[\frac{m+1}{2}\right] = m$. Then

$$n(m-p) - r = n(m-p) - n\left[\frac{m+1}{2}\right] + 1 \geq n\left(m - \left[\frac{m}{2}\right] - \left[\frac{m+1}{2}\right]\right) + 1 = 1.$$

It follows that for $\lambda \in \{0,1,\ldots,p\}$,

$$x^\lambda f_{p-\lambda}(y) = \epsilon^\lambda y^{\lambda n} f_{p-\lambda}(y) + O\left(\frac{1}{y}\right). \tag{3.23}$$

Note that the formula (3.23) holds for every of the m branches of $x(y)$, assigning to ϵ the corresponding one of its m values. Therefore p of these branches satisfy the equation

$$F\big(x(y), y\big) = 0. \tag{3.24}$$

Taking in (3.23) one of the values of ϵ for which (3.24) is satisfied. Summing (3.23) for $\lambda \in \{0, 1, \ldots, p\}$, we obtain

$$0 = F\big(x(y), y\big) = \sum_{\lambda=0}^{p} x^{\lambda} f_{p-\lambda}(y) = \sum_{\lambda=0}^{p} \epsilon^{\lambda} y^{\lambda n} f_{p-\lambda}(y) + O\Big(\frac{1}{y}\Big).$$

We see that $\sum_{\lambda=0}^{p} \epsilon^{\lambda} y^{\lambda n} f_{p-\lambda}(y)$ is a polynomial in y and $O\Big(\dfrac{1}{y}\Big) \to 0$ $(y \to \infty)$. Then

$$F(\epsilon y^n, y) \equiv \sum_{\lambda=0}^{p} \epsilon^{\lambda} y^{\lambda n} f_{p-\lambda}(y) = 0.$$

Taking $y = 0$, we have $F(0,0) = 0$. Since $Z^* = FG$, $f(0,0) = Z^*(0,0) = F(0,0)G(0,0)$ $= 0$. This is a contradiction. Hence Lemma 3.4.1 is proved. □

Remark 3.4.2. The number r in Lemma 3.4.1 can be replaced by $r^* := \dfrac{nm}{2} - 1$. Observe that if m is even, then $\left[\dfrac{m+1}{2}\right] = \dfrac{m}{2}$, so $r^* = r$.

Corollary 3.4.3. The absolute irreducibility of Z^* in Lemma 3.4.1 holds under the hypothesis of the lemma also in the domain of algebraic polynomials, if we replace r with $r^* := \dfrac{nm}{2} - 1$ in the case of odd $m > 1$.

Proof. Suppose that $Z^* = FG$ where F and G are proper algebraic polynomials. Let M be the smallest common denominator of all exponents in F, G and $w := 2M$. Then we can write $Z^*(x,y) = F(x^{1/w}, y^{1/w})G(x^{1/w}, y^{1/w})$, where $F(u,v)$ and $G(u.v)$ can be assumed to be integer polynomials. Replacing $x^{1/w}$ by ξ and $y^{1/w}$ by η, we obtain

$$\xi^{wm} + \eta^{wnm} + f(\xi^w, \eta^w) = Z^*(\xi^w, \eta^w) = F(\xi, \eta)G(\xi, \eta). \tag{3.25}$$

If we replace m in Lemma 3.4.1 by wm, since w is even, the corresponding r becomes

$$\rho := n\left[\frac{wm+1}{2}\right] - 1 = \frac{wnm}{2} - 1.$$

If $nm = 1$, then $n = m = 1$, $r = 1 \cdot \left[\frac{1+1}{2}\right] - 1 = 0$. It follows that f must be a constant, so the conditions of Lemma 3.4.1 are satisfied. If $nm > 1$, by our new assumption, we have that for every PP, $x^\lambda y^\kappa$, in f, $\lambda n + \kappa \le r^* = \frac{nm}{2} - 1$. Note that the corresponding PP in $f(\xi^w, \eta^w)$ is $\xi^{w\lambda}\eta^{w\kappa}$ and $w\lambda n + w\kappa \le wr^*$. Since $wr^* = \frac{wnm}{2} - w < \frac{wnm}{2} - 1 = \rho$, $w\lambda n + w\kappa \le \rho$. By Lemma 3.4.1, we have that (3.25) is impossible. □

Corollary 3.4.4. If Z^* is an algebraic polynomial of the form

$$Z^* := x^\alpha + y^{n\alpha} + \varphi(x^{1/w}, y^{1/w}),$$

where $\alpha \in \mathbb{Q}^+$, $n, w \in \mathbb{N}$ and φ is an integer polynomial in $x^{1/w}$ and $y^{1/w}$ such that $\varphi(0,0) \ne 0$ and every PP, $x^\lambda y^\kappa$, which occurs in φ, we have $\lambda n + \kappa \le r^* := \frac{n\alpha}{2} - 1$, then Z is absolutely irreducible in the domain of all algebraic polynomials.

Proof. Suppose that $Z^* = FG$ where F and G are proper algebraic polynomials. We can choose w such that $w\alpha$ becomes an even integer and that the decomposition of Z^* becomes

$$Z^* = F(x^{1/w}, y^{1/w})G(x^{1/w}, y^{1/w}), \tag{3.26}$$

where F and G are integer polynomials in $x^{1/w}$ and $y^{1/w}$. Replacing $x^{1/w}$ and $y^{1/w}$ in (3.26) with ξ and η, respectively, we obtain

$$\xi^{w\alpha} + \eta^{wn\alpha} + \varphi(\xi,\eta) = F(\xi,\eta)G(\xi,\eta). \tag{3.27}$$

If we replace m in Lemma 3.4.1 by $w\alpha$, since $w\alpha$ is even, the corresponding r becomes

$$\rho := n\left[\frac{w\alpha+1}{2}\right] - 1 = \frac{wn\alpha}{2} - 1.$$

Since for every PP, $x^\lambda y^\kappa$, in $\varphi(x^{1/w}, y^{1/w})$, we have $\lambda n + \kappa \le r^*$, it follows that for every PP, $\xi^{w\lambda}\eta^{w\kappa}$, in $\varphi(\xi,\eta)$, we have $w\lambda n + w\kappa \le wr^* = \frac{wn\alpha}{2} - w < \frac{wn\alpha}{2} - 1 = \rho$. By Lemma 3.4.1, we have that the docomposition (3.27) is impossible. □

3.5 Irreducibility of polynomials with 2 or 3 terms

First, we consider a rational polynomial with two distinct terms

$$ax_1^{u_1}\dots x_m^{u_m} + bx_1^{v_1}\dots x_m^{v_m}, \quad ab \neq 0. \tag{3.28}$$

Theorem 3.5.1. The polynomial (3.28) is absolutely irreducible in the domain of rational polynomials if and only if $\gcd(u_1 - v_1, \dots, u_m - v_m) = 1$.

Proof. Let $c := \frac{b}{a}$, $\alpha_\mu := v_\mu - u_\mu$ $\big(\mu \in \{1,\dots,m\}\big)$ and $Z := 1 + cx_1^{\alpha_1}\dots x_m^{\alpha_m}$. Then $ax_1^{u_1}\dots x_m^{u_m} + bx_1^{v_1}\dots x_m^{v_m} = ax_1^{u_1}\dots x_m^{u_m} Z$, so we will prove that Z is absolutely irreducible if and only if $\gcd(\alpha_1,\dots,\alpha_m) = 1$.

($\rightarrow$) Suppose that $\gcd(\alpha_1,\dots,\alpha_m) = d$ where $d \in \mathbb{Z}$ and $d > 1$. Then for $\mu \in \{1,\dots,m\}$, we have $\alpha_\mu = d\beta_\mu$ with $\beta_\mu \in \mathbb{Z}$. Let $P := x_1^{\beta_1}\dots x_m^{\beta_m}$. Thus we have $Z = 1 + cP^d = 1-(-c)P^d = 1-(\epsilon c^{1/d}P)^d = (1-\epsilon c^{1/d}P)(1+\epsilon c^{1/d}P+\dots+(\epsilon c^{1/d}P)^{d-1})$ where $\epsilon^d = -1$, so Z is reducible in the field $K(c^{1/d},\epsilon)$.

($\leftarrow$) Assume $\gcd(\alpha_1,\dots,\alpha_m) = 1$. It is well known that it is possible to find $\alpha_{\mu\nu} \in \mathbb{Q}$ $\big(\mu \in \{2,\dots,m\},\ \nu \in \{1,\dots,m\}\big)$ such that

$$\det\begin{bmatrix} \alpha_1 & \dots & \alpha_m \\ \alpha_{21} & \dots & \alpha_{2m} \\ \vdots & & \vdots \\ \alpha_{m1} & \dots & \alpha_{mm} \end{bmatrix} = 1.$$

If we now apply the m-r-transformation, $y_1 := x_1^{\alpha_1} \dots x_m^{\alpha_m}$, $y_\mu := x_1^{\alpha_{\mu 1}} \dots x_m^{\alpha_{\mu m}}$ $\big(\mu \in \{2, \dots, m\}\big)$, then Z becomes $1+cy_1$. Suppose $Z(x_1 \dots x_m) = F(x_1 \dots x_m)G(x_1 \dots x_m)$ where F and G are proper rational polynomials with coefficients in some algebraic extension of K. Observe that $x_\mu = y_1^{\gamma_{\mu 1}} \dots y_m^{\gamma_{\mu m}}$ $\big(\mu \in \{1, \dots, m\}\big)$ where $\gamma_{\mu\nu} \in \mathbb{Z}$ $\big(\mu \in \{1, \dots, m\},\ \nu \in \{1, \dots, m\}\big)$. Introducing the expressions of F and G in the variables $y_1, \dots, y_m$, we can assume that $F(y_1, \dots, y_m)$ and $G(y_1, \dots, y_m)$ are integer polynomials. Since F and G are proper, the degrees of $F(y_1, \dots, y_m)$ and $G(y_1, \dots, y_m)$ must be ≥ 1. Then the degree of $1 + cy_1 = Z(y_1 \dots y_m) = F(y_1 \dots y_m)G(y_1 \dots y_m)$ is ≥ 2, which is a contradiction. Hence $Z(x_1 \dots x_m)$ is absolutely irreducible. □

Now, we consider a rational polynomial with three distinct terms

$$aP_1 + bP_2 + cP_3, \quad abc \neq 0. \tag{3.29}$$

Theorem 3.5.2. The polynomial (3.29) is absolutely irreducible even in the domain of algebraic polynomials, if $P_2/P_1, P_3/P_1$ are algebraically independent.

If $P_2/P_1, P_3/P_1$ are not independent and P_1, P_2, P_3 are algebraic PP's, then (3.29) is reducible in the domain of algebraic polynomials. If $P_2/P_1, P_3/P_1$ are not independent and P_1, P_2, P_3 are rational PP's, then (3.29) is reducible in the domain of rational polynomials.

Proof. The first part of Theorem 3.5.2 follows immediately from Theorem 3.1.8 for $n = 2$.

We are now going to prove the remaining part of Theorem 3.5.2. Assume that $P_2/P_1,\ P_3/P_1$ are not independent. Let $a' := \dfrac{b}{a},\ b' := \dfrac{c}{a},\ P_1' := P_2/P_1,\ P_2' := P_3/P_1$ and $Z := 1 + a'P_1' + b'P_2'$. Then obviously, $a'b' \neq 0$, P_1', P_2' are not independent and $aP_1 + bP_2 + cP_3 = aP_1 Z$. We will prove that if P_1, P_2, P_3 are algebraic PP's, then Z is reducible in the domain of algebraic polynomials, and if P_1, P_2, P_3 are rational PP's, then Z is reducible in the domain of rational polynomials. Put $P_1' := x_1^{\alpha_1} \dots x_m^{\alpha_m}$ and $P_2' := x_1^{\beta_1} \dots x_m^{\beta_m}$. Since P_1', P_2' are not independent, by Proposition 3.1.2, there exist $u, v \in \mathbb{Z}$, not all zero, such that $P_1'^v = P_2'^u$. If $u = 0$, we have $v \neq 0$ and $P_1'^v = 1$. Thus $P_1' = 1$, so $P_1 = P_2$, which is a contradiction. Then $u \neq 0$. Similarly, since $P_1 \neq P_3$, we have $v \neq 0$. We can assume that $u > 0$ since we can replace u by $-u$. Since $P_2 \neq P_3$, $P_1' \neq P_2'$, so $u \neq v$. Note that $x_1^{v\alpha_1} \dots x_m^{v\alpha_m} = P_1'^v = P_2'^u = x_1^{u\beta_1} \dots x_m^{u\beta_m}$. Then we obtain

$$v\alpha_\mu = u\beta_\mu \quad \big(\mu \in \{1, \dots, m\},\ u, v \in \mathbb{Z} \setminus \{0\},\ u > 0,\ u \neq v\big). \tag{3.30}$$

Put $\gamma_\mu := \dfrac{\alpha_\mu}{u} = \dfrac{\beta_\mu}{v}$ $\big(\mu \in \{1, \dots, m\}\big)$ and $Q := x_1^{\gamma_1} \dots x_m^{\gamma_m}$. So $P_1' = Q^u$, $P_2' = Q^v$ and $Z = 1 + a'Q^u + b'Q^v$.

First, assume that P_1', P_2' are algebraic PP's, not all rational, i.e. not all of the α_μ, β_μ are integers. Since $u, v \neq 0$ and $u \neq v$, Z has at least two proper linear factors in Q over some algebraic extension of K.

Now, assume that P_1', P_2' are rational PP's, i.e. $\alpha_\mu, \beta_\mu \in \mathbb{Z}$ $\big(\mu \in \{1, \dots, m\}\big)$. Let $u' := \dfrac{u}{\gcd(u,v)}$ and $v' := \dfrac{v}{\gcd(u,v)}$. Thus $u', v' \in \mathbb{Z} \setminus \{0\}$, $u' > 0$, $u' \neq v'$, $\gcd(u', v') = 1$ and $v'\alpha_\mu = u'\beta_\mu$ $\big(\mu \in \{1, \dots, m\}\big)$. It follows that $u' | \alpha_\mu$ and $v' | \beta_\mu$ $\big(\mu \in \{1, \dots, m\}\big)$, so $u' | \gcd(\alpha_1, \dots, \alpha_m)$ and $v' | \gcd(\beta_1, \dots, \beta_m)$. Then

$\gcd(\alpha_1, \dots, \alpha_m) = u'k$ and $\gcd(\beta_1, \dots, \beta_m) = v'l$ where $k, l \in \mathbb{Z}$ and $k > 0$. Let $A_\mu := \dfrac{\alpha_\mu}{\gcd(\alpha_1, \dots, \alpha_m)}$, $B_\mu := \dfrac{\beta_\mu}{\gcd(\beta_1, \dots, \beta_m)}$ $\big(\mu \in \{1, \dots, m\}\big)$, $M := v' \gcd(\alpha_1, \dots, \alpha_m)$ and $N := u' \gcd(\beta_1, \dots, \beta_m)$. Observe that $\gcd(A_1, \dots, A_m) = \gcd(B_1, \dots, B_m) = 1$. Since $x_1^{MA_1} \dots x_m^{MA_m} = x_1^{v'\alpha_1} \dots x_m^{v'\alpha_m} = x_1^{u'\beta_1} \dots x_m^{u'\beta_m} = x_1^{NB_1} \dots x_m^{NB_m}$,

$MA_\mu = NB_\mu$ $\big(\mu \in \{1, \dots, m\}\big)$. Thus we have

$|v'|u'k = |v'|\gcd(\alpha_1,\ldots,\alpha_m) = |M| = |M|\gcd(A_1,\ldots,A_m) = \gcd(MA_1,\ldots,MA_m)$ $= \gcd(NB_1,\ldots,NB_m) = |N|\gcd(B_1,\ldots,B_m) = |N| = N = u'\gcd(\beta_1,\ldots,\beta_m) =$ $u'v'l$, so $l = \pm k$. It follows that $\gcd(\alpha_1,\ldots,\alpha_m)\beta_\mu = ku'\beta_\mu = kv'\alpha_\mu = \pm lv'\alpha_\mu =$ $\pm\gcd(\beta_1,\ldots,\beta_m)\alpha_\mu$ $(\mu \in \{1,\ldots,m\})$. Hence we can choose u and v in (3.30) as $\gcd(\alpha_1,\ldots,\alpha_m)$ and $\pm\gcd(\beta_1,\ldots,\beta_m)$, respectively. Then $\gamma_\mu \in \mathbb{Z}$ $(\mu \in \{1,\ldots,m\})$, so Q is a rational PP. Thus the proper linear factors of Z in Q are rational polynomials. Therefore Theorem 3.5.2 is proved. □

3.6 Polynomials with 4 terms. General discussion

If we consider now the general algebraic polynomial with four distinct PP's,

$$aP_1 + bP_2 + \gamma P_3 + dP_4, \quad ab\gamma d \neq 0, \tag{3.31}$$

we have to distinguish three cases according as among the quotients

$$P_2/P_1, P_3/P_1, P_4/P_1, \tag{3.32}$$

there are 3,2 or 1 independents.

Proposition 3.6.1. If all quotients (3.32) are independent, then the polynomial (3.31) is always absolutely irreducible in the domain of algebraic polynomials.

Proof. This follows from Theorem 3.1.8 with $n = 3$. □

Proposition 3.6.2. If there is only one independent among the quotients (3.32), the polynomial (3.31) is always reducible in the domain of algebraic polynomials, and if all quotients (3.32) are rational PP's, (3.31) is reducible even in the domain of rational polynomials.

Proof. Let $a' := \frac{b}{a}$, $b' := \frac{\gamma}{a}$, $\gamma' := \frac{d}{a}$, $P_1' := P_2/P_1$, $P_2' := P_3/P_1$, $P_3' := P_4/P_1$ and $Z := 1 + a'P_1' + b'P_2' + \gamma' P_3'$. Then obviously, $a'b'\gamma' \neq 0$, P_1', P_2', P_3' are not independent and $aP_1 + bP_2 + \gamma P_3 + dP_4 = aP_1 Z$. We will prove that Z is reducible in the domain of algebraic polynomials, and if all quotients (3.32) are rational PP's, then Z is reducible in the domain of rational polynomials. Put $P_1' := x_1^{\alpha_1} \dots x_m^{\alpha_m}$, $P_2' := x_1^{\beta_1} \dots x_m^{\beta_m}$ and $P_3' := x_1^{\gamma_1} \dots x_m^{\gamma_m}$. Since P_1', P_2' are not independent, we can show as we did in the proof of Theorem 3.5.2 that there exist $e, f \in \mathbb{Z} \setminus \{0\}$, $f > 0$ such that $e\alpha_\mu = f\beta_\mu$ $(\mu \in \{1, \dots, m\})$. Similarly, since P_1', P_3' are not independent, there exist $g, h \in \mathbb{Z} \setminus \{0\}$, $h > 0$ such that $g\alpha_\mu = h\gamma_\mu$ $(\mu \in \{1, \dots, m\})$. Then $fg\beta_\mu = eg\alpha_\mu = eh\gamma_\mu$ $(\mu \in \{1, \dots, m\})$. Dividing by $efgh$, we have $\frac{\beta_\mu}{eh} = \frac{\alpha_\mu}{fh} = \frac{\gamma_\mu}{fg}$ $(\mu \in \{1, \dots, m\})$. Let $u := fh$, $v := eh$ and $w := fg$. Then $u, v, w \in \mathbb{Z} \setminus \{0\}$, $u > 0$ and

$$\frac{\alpha_\mu}{u} = \frac{\beta_\mu}{v} = \frac{\gamma_\mu}{w} \quad (\mu \in \{1, \dots, m\}). \tag{3.33}$$

Note that u, v, w are distinct since P_1', P_2', P_3' are distinct. Put $\delta_\mu := \frac{\alpha_\mu}{u} = \frac{\beta_\mu}{v} = \frac{\gamma_\mu}{w}$ $(\mu \in \{1, \dots, m\})$ and $Q := x_1^{\delta_1} \dots x_m^{\delta_m}$. So $P_1' = Q^u$, $P_2' = Q^v$, $P_3' = Q^w$ and $Z = 1 + a'Q^u + b'Q^v + \gamma' Q^w$. Writing $Z = 0$, since $u, v, w \neq 0$ and are all distinct, we obtain an algebraic equation of a degree ≥ 3, so Z has at least three proper linear factors in Q over some algebraic extension of K.

Now, assume that P_1', P_2', P_3' are rational PP's, i.e. $\alpha_\mu, \beta_\mu, \gamma_\mu \in \mathbb{Z}$ $(\mu \in \{1, \dots, m\})$. Since $\frac{\alpha_\mu}{u} = \frac{\beta_\mu}{v}$ $(\mu \in \{1, \dots, m\})$, as we did in the proof of Theorem 3.5.2, we can choose u and v in (3.33) as $\gcd(\alpha_1, \dots, \alpha_m)$ and $\pm \gcd(\beta_1, \dots, \beta_m)$, respectively. And since $\frac{\alpha_\mu}{u} = \frac{\gamma_\mu}{w}$ $(\mu \in \{1, \dots, m\})$, we can also choose w in (3.33) as $\pm \gcd(\gamma_1, \dots, \gamma_m)$. Then $\delta_\mu \in \mathbb{Z}$ $(\mu \in \{1, \dots, m\})$, so Q is a rational PP. Thus Z is reducible in the domain of rational polynomials. Therefore Proposition 3.6.2 is proved. $\square$

From now on, we consider the case that there are exactly two independent ones among the quotients (3.32).

The condition can be expressed in a simpler way, by introducing the representative points of P_1, P_2, P_3, P_4 in the corresponding m-dimensional space, E. Let

$$P_1 := x_1^{\alpha_1} \dots x_m^{\alpha_m},\ P_2 := x_1^{\beta_1} \dots x_m^{\beta_m},\ P_3 := x_1^{\gamma_1} \dots x_m^{\gamma_m},\ P_4 := x_1^{\delta_1} \dots x_m^{\delta_m},$$

and the corresponding representative points in E be

$$X_1 := (\alpha_1, \dots, \alpha_m),\ X_2 := (\beta_1, \dots, \beta_m),\ X_3 := (\gamma_1, \dots, \gamma_m),\ X_4 := (\delta_1, \dots, \delta_m),$$

respectively. We claim that X_1, X_2, X_3, X_4 are not collinear. Suppose not. Then we have $\overrightarrow{X_1X_2} \,//\, \overrightarrow{X_1X_3}$, $\overrightarrow{X_1X_2} \,//\, \overrightarrow{X_1X_4}$, and $\overrightarrow{X_1X_3} \,//\, \overrightarrow{X_1X_4}$. So there exist $s_1, s_2, s_3 \in \mathbb{R}$ such that $(\beta_1 - \alpha_1, \dots, \beta_m - \alpha_m) = s_1(\gamma_1 - \alpha_1, \dots, \gamma_m - \alpha_m), (\beta_1 - \alpha_1, \dots, \beta_m - \alpha_m) = s_2(\delta_1 - \alpha_1, \dots, \delta_m - \alpha_m)$ and $(\gamma_1 - \alpha_1, \dots, \gamma_m - \alpha_m) = s_3(\delta_1 - \alpha_1, \dots, \delta_m - \alpha_m)$. It follows that $\beta_\mu - \alpha_\mu = s_1(\gamma_\mu - \alpha_\mu)$, $\beta_\mu - \alpha_\mu = s_2(\delta_\mu - \alpha_\mu)$ and $\gamma_\mu - \alpha_\mu = s_3(\delta_\mu - \alpha_\mu)$ $\big(\mu \in \{1, \dots, m\}\big)$. Since $\alpha_\mu, \beta_\mu, \gamma_\mu, \delta_\mu \in \mathbb{Q}$ $\big(\mu \in \{1, \dots, m\}\big)$, $s_1, s_2, s_3 \in \mathbb{Q}$. We have that
$P_2/P_1 = x_1^{\beta_1 - \alpha_1} \dots x_m^{\beta_m - \alpha_m} = x_1^{s_1(\gamma_1 - \alpha_1)} \dots x_m^{s_1(\gamma_m - \alpha_m)} = (x_1^{\gamma_1 - \alpha_1} \dots x_m^{\gamma_m - \alpha_m})^{s_1} = (P_3/P_1)^{s_1}$
$P_2/P_1 = x_1^{\beta_1 - \alpha_1} \dots x_m^{\beta_m - \alpha_m} = x_1^{s_2(\delta_1 - \alpha_1)} \dots x_m^{s_2(\delta_m - \alpha_m)} = (x_1^{\delta_1 - \alpha_1} \dots x_m^{\delta_m - \alpha_m})^{s_2} = (P_4/P_1)^{s_2}$,
$P_3/P_1 = x_1^{\gamma_1 - \alpha_1} \dots x_m^{\gamma_m - \alpha_m} = x_1^{s_3(\delta_1 - \alpha_1)} \dots x_m^{s_3(\delta_m - \alpha_m)} = (x_1^{\delta_1 - \alpha_1} \dots x_m^{\delta_m - \alpha_m})^{s_3} = (P_4/P_1)^{s_3}$.
Thus any two quotients in (3.32) are not independent, which contradicts our assumption. Hence X_1, X_2, X_3, X_4 are not collinear. Then the corresponding baric diagram is either a triangle or a quadrangle.

For the case that the corresponding baric diagram is a triangle, we choose the notation so that X_1, X_2, X_3 are three summits of the triangle, and if the point X_4 lies on one of the sides, then the opposite summit is X_1.

In both cases the points X_1, X_2, X_3 are not collinear.

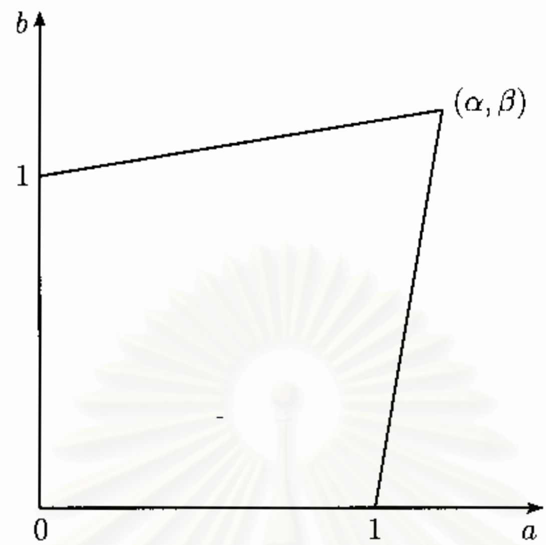
Let $a' := \frac{b}{a},\ b' := \frac{\gamma}{a},\ \gamma' := \frac{d}{a},\ P_1' := P_2/P_1,\ P_2' := P_3/P_1,\ P_3' := P_4/P_1$ and

$$Z := 1 + a'P_1' + b'P_2' + \gamma' P_3'. \tag{3.34}$$

Obviously, $a'b'\gamma' \neq 0$, and $aP_1 + bP_2 + \gamma P_3 + dP_4 = aP_1 Z$. This amounts to bringing the point X_1 into the origin, and the corresponding term in $aP_1 + bP_2 + \gamma P_3 + dP_4$ becomes 1. We can assume that P_1', P_2' are independent. By an m-r-transformation, we introduce $y_1 := P_1'$ and $y_2 := P_2'$ as new variables. Since P_1', P_2', P_3' are not independent, by Proposition 3.1.2, we have that $P_3' = P_1'^{\alpha} P_2'^{\beta} = y_1^{\alpha} y_2^{\beta}$ where $\alpha, \beta \in \mathbb{Q}$. Then $Z = 1 + a'y_1 + b'y_2 + \gamma' y_1^{\alpha} y_2^{\beta}$.

We now show that $\alpha, \beta > 0$. If the baric polygon of Z is a triangle, this triangle becomes now, in the $a - b$-plane:

Note that the point (α, β) lies either inside of this triangle or on the hypotenuse, so $\alpha, \beta > 0$. And if the baric polygon of Z is a quadrangle, since the inside of a convex quadrangle goes by an affine transformation always into the inside of the corresponding quadrangle, the situation is as in the diagram:



We see in this case that also $\alpha, \beta > 0$.

Take $y_1' := a'y_1$ and $y_2' := b'y_2$. Then $Z = 1 + y_1' + y_2' + c{y_1'}^{\alpha}{y_2'}^{\beta}$ where $c := \frac{\gamma'}{a'^{\alpha}b'^{\beta}}$. Let M be a common denominator of α and β, $p := M\alpha$ and $q := M\beta$. So $p, q \in \mathbb{Z}^+$. We choose M such that $p, q \geq 2$. Then putting $y_1' =: x'^M$ and $y_2' =: y'^M$, we obtain finally Z in the form

$$Z = 1 + x'^M + y'^M + cx'^p y'^q \quad (c \neq 0,\ p, q \in \mathbb{Z}^+). \tag{3.35}$$

If the baric polygon of Z in (3.35) is a triangle, we must have $p + q \leq M$. Since $p, q > 0$, it follows that $p, q < M$. Suppose that Z is reducible in the domain of integer polynomials. If we apply Lemma 3.3.1, replacing there z with x', n with M and k with p, we obtain in the notations of Lemma 3.3.1 that $\varphi = 1 + y'^M$, $\psi_1 = cy'^q$ and $\chi = 1$. Thus if we use the degree in y' as weight, all conditions of Lemma 3.3.1 are satisfied. It follows that $\frac{M}{p} \in \mathbb{Z}^+$. Similarly, $\frac{M}{q} \in \mathbb{Z}^+$. Also, we have that the factors of Z are polynomials in x'^p and y'^q. Since $p, q \neq M$, $\frac{M}{p}, \frac{M}{q} \geq 2$. Introduce $x := x'^p$ and $y := y'^q$ as new variables. Let $m := \frac{M}{p}$ and $n := \frac{M}{q}$. Then we have to consider the reducible polynomials of the shape

$$Z = 1 + x^m + y^n + cxy \quad (c \neq 0,\ m, n \geq 2). \tag{3.36}$$

3.7 Four term polynomials with a baric triangle

From now on, we assume that c ∈ $\mathbb{R}$ or $\mathbb{C}$. Without loss of generality, we can assume that in (3.36), $m \geq n$. Suppose that (3.36) is reducible in the domain of integer polynomials. Then we have

$$x^m + y^n + cxy + 1 = F(x, y)G(x, y), \tag{3.37}$$

where $F(x, y)$ and $G(x, y)$ are proper integer polynomials. Replacing y with y^m, we obtain

$$x^m + y^{nm} + cxy^m + 1 = F(x, y^m)G(x, y^m). \tag{3.38}$$

First, assume that $n \geq 4,\ m \geq 5$. If for $f = cxy^m,\ \lambda = 1,\ \kappa = m$, we have

$$n + m \leq r := n\left[\frac{m+1}{2}\right] - 1, \tag{3.39}$$

then it follows from Lemma 3.4.1 that (3.38) is impossible.

If m is even, then $m = 2k$ for some $k \in \mathbb{Z}$. Since $m \geq 6$, $k \geq 3$. The condition (3.39) becomes $n + 2k \leq nk - 1$, i.e. $n(k-1) \geq 2k + 1$. Since $n \geq 4$, it suffices to prove that $4(k-1) \geq 2k + 1$, i.e. $2k \geq 5$ and this is satisfied since $k \geq 3$. On the other hand, if m is odd, then $m = 2k + 1$ for some $k \in \mathbb{Z}$. Since $m \geq 5$, $k \geq 2$. The condition (3.39) becomes $n + 2k + 1 \leq n(k+1) - 1$, i.e. $nk \geq 2k + 2$. Since $n \geq 4$, it suffices to prove that $4k \geq 2k + 2$, i.e. $2k \geq 2$ and this is satisfied since $k \geq 3$. Thus (3.38) is impossible. Therefore Z in this case is irreducible.

Now, we have to consider the remaining cases:

1. $m \geq 5,\ 2 \leq n \leq 3$,

2. $m = 4,\ 2 \leq n \leq 4$,

3. $m = 3,\ 2 \leq n \leq 3$,

4. $m = 2,\ n = 2$.

Lemma 3.7.1. The factors of Z in (3.37) cannot be independent of y. In particular, if $2 \leq n \leq 3$, then Z must have a linear factor in y.

Proof. Suppose that $Z = F(x)G(x,y)$ where $F(x)$ and $G(x,y)$ are proper integer polynomials. Then we have $x^m + y^n + cxy + 1 = F(x)G(x,y)$, so the degree of $G(x,y)$ in y is n. Since $n \geq 2$, we can write $G(x,y) = G_2(x,y)y^2 + G_1(x)y + G_0(x)$, where $G_2(x,y), G_1(x), G_0(x)$ are integer polynomials and the degree of $G_2(x,y)$ in y is $n-2$. So $x^m + y^n + cxy + 1 = F(x)G_2(x,y)y^2 + F(x)G_1(x)y + F(x)G_0(x)$. Comparing the coefficients of y on both sides, we have $cx = F(x)G_1(x)$, which is impossible since $F(x)$ is proper. $\square$

Moreover, we can similarly show that the factors of Z in (3.37) cannot be independent of x.

Case 1. $m \geq 5,\ 2 \leq n \leq 3$.

By Lemma 3.7.1, Z has a linear factor in y, then there exists a polynomial $\varphi(x)$ such that if we replace y with $\varphi(x)$ in Z, we have $\varphi^n + x^m + cx\varphi + 1 = 0$, so

$$\varphi^n = -x^m - cx\varphi - 1. \tag{3.40}$$

Since $m \geq 5,\ 2 \leq n \leq 3$, the degree of φ is ≥ 2. Denote the highest term of φ by ϵx^p where $\epsilon^n = -1$. Then $p \geq 2$. From (3.40), since $np \geq 2p > p+1$, it follows that $np = m$, so $p = \dfrac{m}{n}$. If we denote the next term in φ by αx^q, then the first two terms of φ^n are $\epsilon^n x^{np} + n\epsilon^{n-1}\alpha x^{(n-1)p+q}$. Since the first term of $-cx\varphi$ is $-c\epsilon x^{p+1}$, we have $(n-1)p+q = p+1$, so $(n-2)p+q = 1$. If $n = 3$, then $p+q = 1$, which is impossible since $p \geq 2$. Thus $n = 2$, so $q = 1$ and $m = 2p$.

Writing φ as $\varphi = \epsilon x^p + \alpha x + \beta$, we have

$$\varphi^2 = (\epsilon x^p + \alpha x + \beta)^2 = \epsilon^2 x^{2p} + 2\epsilon\alpha x^{p+1} + 2\epsilon\beta x^p + \alpha^2 x^2 + 2\alpha\beta x + \beta^2. \tag{3.41}$$

Since $2p = m \geq 5$, $p \geq 3$, so all exponents on the right side of (3.41) are distinct. Substituting $\varphi = \epsilon x^p + \alpha x + \beta$ into (3.40), we obtain

$$\varphi^2 = -x^{2p} - cx\varphi - 1 = -x^{2p} - c\epsilon x^{p+1} - c\alpha x^2 - c\beta x - 1. \tag{3.42}$$

Comparing the coefficients of x^0 on the right sides of (3.41) and (3.42), we have $\beta^2 = -1$, so $\beta \neq 0$. Thus φ^2 in (3.41) contains the term $2\epsilon\beta x^p$, but (3.42) does not contain such term. This is a contradiction. Therefore Z is irreducible.

Case 2. $m = 4,\ 2 \leq n \leq 4$.

First, assume that Z has no linear factors in y. By Lemma 3.7.1, we have $m = n = 4$, then Z becomes

$$Z = x^4 + y^4 + cxy + 1 \tag{3.43}$$

and its decomposition into a product of two quadratic factors can be written as

$$Z = (h + h_1 + c_1)(k + k_1 + c_2), \tag{3.44}$$

where h, k are homogeneous quadratic polynomials, h_1, k_1 are homogeneous linear polynomials in x, y and c_1, c_2 are constants. It follows that $c_1c_2 = 1$, so $c_2 = \dfrac{1}{c_1}$.

Moreover, we have $hk = x^4 + y^4$. Note that

$$\begin{aligned} x^4 + y^4 &= y^4\left(\left(\frac{x}{y}\right)^4 + 1\right) \\ &= y^4\left(\frac{x}{y} - i\epsilon\right)\left(\frac{x}{y} + i\epsilon\right)\left(\frac{x}{y} - \epsilon\right)\left(\frac{x}{y} + \epsilon\right) \\ &= (x - i\epsilon y)(x + i\epsilon y)(x - \epsilon y)(x + \epsilon y), \end{aligned} \tag{3.45}$$

where $\epsilon = e^{\pi i/4}$. We see that $x^4 + y^4$ has no multiple factors, so h and k have no common factors. Since Z does not have any cubic terms, the cubic terms on the right in (3.44) are $k_1 h + h_1 k = 0$. Then k_1 must be divisible by k and h_1 must be divisible by h. Since the dimensions of k_1 and h_1 are smaller than the dimensions of k and h, it follows that $h_1 = k_1 = 0$. The decomposition (3.44) becomes

$$Z = (h + c_1)\left(k + \frac{1}{c_1}\right) = hk + \left(\frac{1}{c_1}h + c_1 k\right) + 1. \tag{3.46}$$

Since in any decomposition $hk = x^4 + y^4$, a fixed linear factor of $x^4 + y^4$ is combined with one of the three other factors, from (3.45), we obtain three possible decompositions of $x^4 + y^4$:

(A) $h = (x - i\epsilon y)(x + i\epsilon y) = x^2 + iy^2,\ k = (x - \epsilon y)(x + \epsilon y) = x^2 - iy^2$,

(B) $h = (x - i\epsilon y)(x - \epsilon y) = x^2 - i\sqrt{2}xy - y^2,\ k = (x + i\epsilon y)(x + \epsilon y) = x^2 + i\sqrt{2}xy - y^2$,

(C) $h = (x - i\epsilon y)(x + \epsilon y) = x^2 + \sqrt{2}xy + y^2,\ k = (x + i\epsilon y)(x - \epsilon y) = x^2 - \sqrt{2}xy + y^2$.

Now, we have to choose c, c_1 and h, k such that (3.46) holds. Comparing the quadratic terms of (3.43) and (3.46), we have

$$\frac{1}{c_1}h + c_1 k = cxy. \tag{3.47}$$

Comparing the coefficients of x^2 on both sides of (3.47), we obtain in all three cases the condition $\frac{1}{c_1} + c_1 = 0$, so ${c_1}^2 = -1$, i.e. $c_1 = \pm i$. Comparing the coefficients of y^2 on hoth sides of (3.47), we obtain in Case (A), $\frac{i}{c_1} - ic_1 = 0$, so $c_1 - \frac{1}{c_1} = 0$, i.e. ${c_1}^2 = 1$. Thus Case (A) is impossible. Similarly, we obtain in Cases (B) and (C) $\frac{1}{c_1} + c_1 = 0$, i.e. $\frac{1}{c_1} = -c_1$.

Comparing the coefficients of xy on both sides of (3.47), we obtain in Case (B), $-\frac{i\sqrt{2}}{c_1} + i\sqrt{2}c_1 = c$, so

$$c = 2\sqrt{2}ic_1.$$

We obtain in Case (C), $\frac{\sqrt{2}}{c_1} - \sqrt{2}c_1 = c$, so

$$c = -2\sqrt{2}c_1.$$

Substituting these values in (3.43) and (3.46), if $c_1 = i$, we have the decompositions

$$\begin{aligned} x^4 + y^4 - 2\sqrt{2}xy + 1 &= (x^2 - i\sqrt{2}xy - y^2 + i)(x^2 + i\sqrt{2}xy - y^2 - i) \quad \text{(Case (B))}, \\ x^4 + y^4 - 2\sqrt{2}ixy + 1 &= (x^2 + \sqrt{2}xy + y^2 + i)(x^2 - \sqrt{2}xy + y^2 - i) \quad \text{(Case (C))}. \end{aligned} \tag{3.48}$$

If $c_1 = -i$, we have the decompositions

$$\begin{aligned} x^4 + y^4 + 2\sqrt{2}xy + 1 &= (x^2 - i\sqrt{2}xy - y^2 - i)(x^2 + i\sqrt{2}xy - y^2 + i) \quad \text{(Case (B))}, \\ x^4 + y^4 + 2\sqrt{2}ixy + 1 &= (x^2 + \sqrt{2}xy + y^2 - i)(x^2 - \sqrt{2}xy + y^2 + i) \quad \text{(Case (C))}. \end{aligned} \tag{3.49}$$

We see that (3.49) is obtained by replacing i with $-i$ in (3.48), i.e. (3.49) is the complex conjugate of (3.48).

Now, we consider the possibility that Z has a linear factor in y in Case 2 (as well as in Cases 3 and 4). By Lemma 3.7.1, this linear factor must contain both x and y, so it can be written as $y - H(x)$, where $H(x)$ is an integer polynomial of degree ≥ 1. Replacing y with $H(x)$ in (3.36), we obtain

$$x^m + H(x)^n + cxH(x) + 1 = 0. \tag{3.50}$$

Case 2.1. $m = 4,\ n = 2$. Then (3.36) becomes

$$Z = 1 + x^4 + y^2 + cxy, \tag{3.51}$$

and (3.50) becomes $x^4 + H(x)^2 + cxH(x) + 1 = 0$. It follows that the degree of $H(x)$ is 2. Let $H(x) := \alpha x^2 + \beta x + \gamma$. Then

$$\begin{aligned} 0 &= x^4 + (\alpha x^2 + \beta x + \gamma)^2 + cx(\alpha x^2 + \beta x + \gamma) + 1 \\ &= (\alpha^2 + 1)x^4 + (2\alpha\beta + c\alpha)x^3 + (\beta^2 + 2\alpha\gamma + c\beta)x^2 + (2\beta\gamma + c\gamma)x + \gamma^2 + 1. \end{aligned}$$

Comparing the coefficients on both sides, we obtain $\alpha^2 + 1 = 2\alpha\beta + c\alpha = \beta^2 + 2\alpha\gamma + c\beta = 2\beta\gamma + c\gamma = \gamma^2 + 1 = 0$. Then $\alpha = \pm i,\ \gamma = \pm i$. From $2\alpha\beta + c\alpha = 0$, we have $2\beta + c = 0$, so $c = -2\beta$. Replacing $c = -2\beta$ in $\beta^2 + 2\alpha\gamma + c\beta = 0$, we obtain $\beta^2 + 2\alpha\gamma - 2\beta^2 = 0$, so $\beta^2 = 2\alpha\gamma$.

Case (a) $\alpha = \gamma = i$. Then $\beta^2 = -2$, so $\beta = \pm\sqrt{2}i$.

If $\beta = \sqrt{2}i$, then $c = -2\sqrt{2}i$ and $H(x) = ix^2 + \sqrt{2}ix + i$. So we have that $y - ix^2 - \sqrt{2}ix - i$ is a factor of Z in (3.51). Thus we obtain the decomposition

$$x^4 + y^2 - 2\sqrt{2}ixy + 1 = (y - ix^2 - \sqrt{2}ix - i)(y + ix^2 - \sqrt{2}ix + i)$$
$$= (x^2 + \sqrt{2}x + iy + 1)(x^2 - \sqrt{2}x - iy + 1). \qquad (3.52)$$

If $\beta = -\sqrt{2}i$, then $c = 2\sqrt{2}i$ and $H(x) = ix^2 - \sqrt{2}ix + i$. So we have that $y - ix^2 + \sqrt{2}ix - i$ is a factor of Z in (3.51). Thus we obtain the decomposition

$$x^4 + y^2 + 2\sqrt{2}ixy + 1 = (y - ix^2 + \sqrt{2}ix - i)(y + ix^2 + \sqrt{2}ix + i)$$
$$= (x^2 - \sqrt{2}x + iy + 1)(x^2 + \sqrt{2}x - iy + 1). \qquad (3.53)$$

Case (b) $\alpha = i,\ \gamma = -i$. Then $\beta^2 = 2$, so $\beta = \pm\sqrt{2}$.

If $\beta = \sqrt{2}$, then $c = -2\sqrt{2}$ and $H(x) = ix^2 + \sqrt{2}x - i$. So we have that $y - ix^2 - \sqrt{2}x + i$ is a factor of Z in (3.51). Thus we obtain the decomposition

$$x^4 + y^2 - 2\sqrt{2}xy + 1 = (y - ix^2 - \sqrt{2}x + i)(y + ix^2 - \sqrt{2}x - i)$$
$$= (x^2 - \sqrt{2}ix + iy - 1)(x^2 + \sqrt{2}ix - iy - 1). \qquad (3.54)$$

If $\beta = -\sqrt{2}$, then $c = 2\sqrt{2}$ and $H(x) = ix^2 - \sqrt{2}x - i$. So we have that $y - ix^2 + \sqrt{2}x + i$ is a factor of Z in (3.51). Thus we obtain the decomposition

$$x^4 + y^2 + 2\sqrt{2}xy + 1 = (y - ix^2 + \sqrt{2}x + i)(y + ix^2 + \sqrt{2}x - i)$$
$$= (x^2 + \sqrt{2}ix + iy - 1)(x^2 - \sqrt{2}ix - iy - 1). \qquad (3.55)$$

Case (c) $\alpha = -i,\ \gamma = i$. Then $\beta^2 = 2$, so $\beta = \pm\sqrt{2}$.

If $\beta = \sqrt{2}$, then $c = -2\sqrt{2}$ and $H(x) = -ix^2 + \sqrt{2}x + i$. So we have that $y + ix^2 - \sqrt{2}x - i$ is a factor of Z in (3.51). Thus we obtain the decomposition (3.54).

If $\beta = -\sqrt{2}$, then $c = 2\sqrt{2}$ and $H(x) = -ix^2 - \sqrt{2}x + i$. So we have that

$y + ix^2 + \sqrt{2}x - i$ is a factor of Z in (3.51). Thus we obtain the decomposition (3.55).

Case (d) $\alpha = \gamma = -i$. Then $\beta^2 = -2$, so $\beta = \pm\sqrt{2}i$.

If $\beta = \sqrt{2}i$, then $c = -2\sqrt{2}i$ and $H(x) = -ix^2 + \sqrt{2}ix - i$. So we have that $y + ix^2 - \sqrt{2}ix + i$ is a factor of Z in (3.51). Thus we obtain the decomposition (3.52).

If $\beta = -\sqrt{2}i$, then $c = 2\sqrt{2}i$ and $H(x) = -ix^2 - \sqrt{2}ix - i$. So we have that $y + ix^2 + \sqrt{2}ix + i$ is a factor of Z in (3.51). Thus we obtain the decomposition (3.53).

Case 2.2. $m = 4,\ n = 3$. Then (3.50) becomes

$$x^4 + H(x)^3 + cxH(x) + 1 = 0. \tag{3.56}$$

It follows that the degree of $H(x)$ is ≤ 1. But the degree of $H(x)$ is ≥ 1, then the degree of $H(x)$ is 1, so the degree of $H(x)^3 + cxH(x) + 1$ is 3. Thus (3.56) is impossible. Therefore Z in this case is irreducible.

Case 2.3. $m = 4,\ n = 4$. Then (3.50) becomes

$$x^4 + H(x)^4 + cxH(x) + 1 = 0.$$

It follows that the degree of $H(x)$ is ≤ 1. But the degree of $H(x)$ is ≥ 1, then the degree of $H(x)$ is 1. Let $H(x) := \alpha x + \beta$ where $\alpha \neq 0$. Then $-\alpha\left(x - \frac{1}{\alpha}y + \frac{\beta}{\alpha}\right) = y - \alpha x - \beta$ is a factor of Z. Thus we can assume in this case that Z has a factor of the form $x - uy - v$.

Case 3. $m = 3,\ 2 \leq n \leq 3$.

Case 3.1. $m = 3,\ n = 2$. Then (3.50) becomes

$$x^3 + H(x)^2 + cxH(x) + 1 = 0. \tag{3.57}$$

It follows that the degree of $H(x)$ is ≤ 1. But the degree of $H(x)$ is ≥ 1, then the degree of $H(x)$ is 1, so the degree of $H(x)^2+cxH(x)+1$ is 2. Thus (3.57) is impossible. Therefore Z in this case is irreducible.

Case 3.2. $m = 3,\ n = 3$. Then (3.50) becomes

$$x^3 + H(x)^3 + cxH(x) + 1 = 0.$$

It follows that the degree of $H(x)$ is ≤ 1. But the degree of $H(x)$ is ≥ 1, then the degree of $H(x)$ is 1. Similar to Case 2.3, we can also assume in this case that Z has a factor of the form $x - uy - v$.

Case 4. $m = 2,\ n = 2$. Then (3.36) becomes $Z = 1 + x^2 + y^2 + cxy$. By Lemma 3.7.1, we have that any factor of Z must contain both x and y. Since the degrees of Z in x and y are 2, it follows that the degrees of any factor of Z in x and y are 1. Thus we can assume in this case that Z has a factor of the form $x - uy - v$.

We have now three remaining cases to consider in detail :

$$m = n = 4\,; \quad m = n = 3\,; \quad m = n = 2.$$

In any of these cases, we may assume that Z has a factor of the form $x - uy - v$.

Replacing x in (3.36) with $uy - v$, we obtain

$$(uy + v)^m = -y^n - cuy^2 - cvy - 1. \tag{3.58}$$

Since $v^m = -1$, $v \neq 0$, so $(uy + v)^m$ has $m + 1$ distinct terms. But the right side of (3.58) has at most four terms, it follows that $m \leq 3$ and therefore there are no linear factors in the case $m = n = 4$.

Assume now $m = n = 3$. Then (3.58) becomes

$$u^3y^3 + 3u^2vy^2 + 3uv^2y + v^3 = (uy + v)^3 = -y^3 - cuy^2 - cvy - 1.$$

Comparing the coefficients on both sides, we obtain

$$u^3 = -1,\ 3u^2v = -cu,\ 3uv^2 = -cv,\ v^3 = -1.$$

Then $(-u)^3 = (-v)^3 = 1$ and $c = -3uv$. Let $\epsilon := uv$ and $\epsilon_1 := -u$. So we have $\epsilon^3 = (uv)^3 = 1$, ${\epsilon_1}^3 = (-u)^3 = 1$, $c = -3\epsilon$. Note that $-v = -\dfrac{\epsilon}{u} = \dfrac{\epsilon}{\epsilon_1} = \dfrac{\epsilon}{\epsilon_1}{\epsilon_1}^3 = \epsilon{\epsilon_1}^2$. If these relations are satisfied, then we have a linear factor $x + \epsilon_1 y + \epsilon{\epsilon_1}^2$, where the three values of c are $-3, -3e^{2\pi i/3}, -3e^{4\pi i/3}$. For each value of c, taking for ϵ_1 its three possible values, we obtain in each case three distinct linear factors of Z and Z is their product. The simplest of the three formulas is the following formula, classical in the theory of the division of circle:

$$\begin{aligned} x^3 + y^3 + 1 - 3xy &= (x + y + 1)(x^2 + y^2 + 1 - x - y - xy) \\ &= (x + y + 1)(x + e^{2\pi i/3}y + e^{4\pi i/3})(x + e^{4\pi i/3}y + e^{2\pi i/3}). \end{aligned} \tag{3.59}$$

The other formulas are obtained from (3.59) by replacing there y with $e^{2\pi i/3}y$ and $e^{4\pi i/3}y$.

Finally, assume $m = n = 2$. Then (3.58) becomes

$$u^2y^2 + 2uvy + v^2 = (uy + v)^2 = (-1 - cu)y^2 - cvy - 1.$$

Comparing the coefficients on both sides, we obtain

$$u^2 = -1 - cu,\ 2uv = -cv,\ v^2 = -1.$$

Then $c = -2u$, so $u^2 = -1 + 2u^2$, and $u^2 = 1$.

Thus we have for $u = 1,\ c = -2$,

$$x^2 + y^2 + 1 - 2xy = (x - y + i)(x - y - i),$$

and for $u = -1,\ c = 2$,

$$x^2 + y^2 + 1 + 2xy = (x + y + i)(x + y - i).$$

Summarizing, we have for $m = n = 4$ or $(m = 4,\ n = 2)$, Z in (3.36) is reducible if and only if

$$c = \pm 2\sqrt{2}, \quad \pm 2\sqrt{2}i\,; \tag{3.60}$$

for $m = n = 3$, Z in (3.36) is reducible if and only if

$$c = -3\epsilon, \quad \text{where } \epsilon^3 = 1\,; \tag{3.61}$$

and for $m = n = 2$, Z in (3.36) is reducible if and only if

$$c = \pm 2. \tag{3.62}$$

Recall that for $m = n = 4$, we obtain the decompositions

$$x^4 + y^4 - 2\sqrt{2}xy + 1 = (x^2 - i\sqrt{2}xy - y^2 + i)(x^2 + i\sqrt{2}xy - y^2 - i),$$

$$x^4 + y^4 - 2\sqrt{2}ixy + 1 = (x^2 + \sqrt{2}xy + y^2 + i)(x^2 - \sqrt{2}xy + y^2 - i),$$

$$x^4 + y^4 + 2\sqrt{2}xy + 1 = (x^2 - i\sqrt{2}xy - y^2 - i)(x^2 + i\sqrt{2}xy - y^2 + i),$$

$$x^4 + y^4 + 2\sqrt{2}ixy + 1 = (x^2 + \sqrt{2}xy + y^2 - i)(x^2 - \sqrt{2}xy + y^2 + i).$$

We now confirm that each factor in the above decompositions is irreducible, i.e. $x^2 \pm i\sqrt{2}xy - y^2 \pm i$ and $x^2 \pm \sqrt{2}xy + y^2 \pm i$ are irreducible. Introduce $\bar{x} := i\sqrt{i}x$ and $\bar{y} := \sqrt{i}y$ as new variables. Since $\bar{x}^2 - \sqrt{2}\bar{x}\bar{y} + \bar{y}^2 + 1$ is in the form (3.36) where $m = n = 2$ and c $= -\sqrt{2}$, it follows that $\bar{x}^2 - \sqrt{2}\bar{x}\bar{y} + \bar{y}^2 + 1$ is irreducible. Then $x^2 + i\sqrt{2}xy - y^2 + i = i(\bar{x}^2 - \sqrt{2}\bar{x}\bar{y} + \bar{y}^2 + 1)$ is irreducible. The remaining factors are proved irreducible similarly.

Returning to the general form of the polynomial Z in (3.34), we have completed now the discussion of the case that P_1' and P_2' in (3.34) are independent and $P_3' = P_1'^{\alpha} P_2'^{\beta},\ \alpha, \beta > 0,\ \alpha + \beta \leq 1$, where the inequalities on α and β signify that the baric polyhedron of Z is a triangle.

We have found that Z in (3.36) can be only reducible if

$$m = n = 4\,; \quad m = 4,\ n = 2\,; \quad m = n = 3\,; \quad m = n = 2,$$

that is

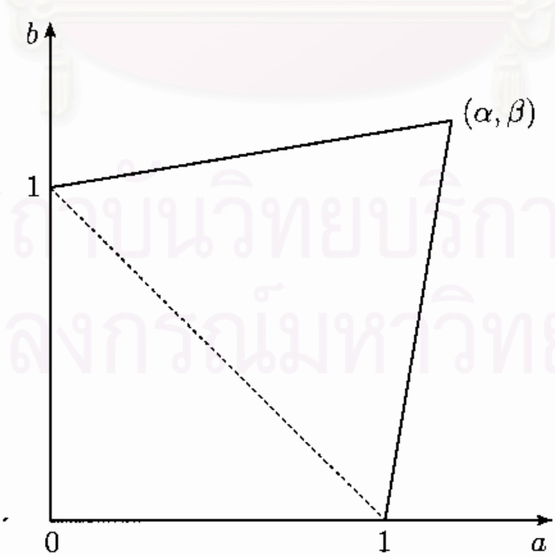
$$\alpha = \beta = \frac{1}{4}\,; \quad \alpha = \frac{1}{4},\ \beta = \frac{1}{2}\,; \quad \alpha = \beta = \frac{1}{3}\,; \quad \alpha = \beta = \frac{1}{2},$$

because $\alpha = \dfrac{1}{m}$ and $\beta = \dfrac{1}{n}$. For the coefficients a', b', γ', we obtain the condition $\gamma' = ca'^{\alpha} b'^{\beta} = ca'^{1/m} b'^{1/n}$, where the values of c corresponding to the four cases of m, n are given by (3.60) - (3.62). If all these conditions are satisfied, then Z is reducible in the domain of algebraic polynomials.

If we consider the irreducibility of Z in the domain of rational polynomials, we have to add the condition that ${P'_1}^{1/m}$ and ${P'_2}^{1/n}$ are rational since $x = (a'P'_1)^{1/m}$ and $y = (b'P'_2)^{1/n}$.

3.8 Four term polynomials with a baric plane quadrangle

We consider now a general four term polynomial with a baric plane quadrangle. In this case, we start with some reductions of the problem. Assume that one of the terms is 1. Then it can be written as $1 + aP_1 + bP_2 + \gamma P_3$, where P_1 and P_2 correspond to the two summits of the baric quadrangle adjacent to the summit at the origin. Since P_1, P_2, P_3 are not independent, by Proposition 3.1.2, we have that $P_3 = {P_1}^{\alpha} {P_2}^{\beta}$ where $\alpha, \beta \in \mathbb{Q}$. Introducing $\xi := aP_1$ and $\eta := bP_2$ as new variables, so our polynomial can be written as $1 + \xi + \eta + c\xi^{\alpha}\eta^{\beta}$, where $c \neq 0$. The following diagram shows the baric quadrangle of $1 + \xi + \eta + c\xi^{\alpha}\eta^{\beta}$.



We see from the diagram that $\alpha, \beta > 0$ and $\alpha + \beta > 1$. Let n be a common denominator of α and β, $p := n\alpha$ and $q := n\beta$. So $p, q \in \mathbb{Z}^+$. We choose n such that $p, q \geq 2$.

Putting $\xi =: x^n$ and $\eta =: y^n$, we obtain

$$Z := 1 + x^n + y^n + cx^p y^q \quad (c \neq 0,\ p, q \in \mathbb{Z}^+,\ p + q > n). \tag{3.63}$$

We investigate the case that Z is reducible in the domain of algebraic polynomials. We can choose n such that Z becomes reducible in the domain of rational and even integer polynomials. In fact, we let n be a common denominator of α, β and all exponents in the factors of Z. Then we can restrict ourselves to the consideration of the reducibility of (3.63) in the domain of integer polynomials.

First, assume that $p = n$ or $q = n$. Without loss of generality, assume $p = n$. Then (3.63) becomes

$$Z = x^n(1 + cy^q) + (1 + y^n).$$

Let $R := -\dfrac{1 + y^n}{1 + cy^q}$ and choose n such that R is not a constant. Since $\dfrac{Z}{1 + cy^q} = x^n - R$, it follows that all n roots of the equation, $Z = 0$, with respect to x have the form $\epsilon R^{1/n}$ for a fixed choice of $R^{1/n}$ and an arbitrary n-th root of unity, ϵ. Suppose that the polynomial $F^*(x, y)$ is a factor of Z of degree $m < n$ with respect to x. Let $F^* := F_m(y)x^m + F_{m-1}(y)x^{m-1} + \cdots + F_1(y)x + F_0(y)$ and

$$F := \frac{F^*}{F_m(y)} = x^m + \frac{F_{m-1}(y)}{F_m(y)} x^{m-1} + \cdots + \frac{F_1(y)}{F_m(y)} x + \frac{F_0(y)}{F_m(y)}. \tag{3.64}$$

Then F is also a factor of Z of degree m with respect to x. Thus all roots of the equation, $F = 0$, with respect to x also have the form $\epsilon R^{1/n}$, so we can write

$$F = (x - \epsilon_1 R^{1/n}) \ldots (x - \epsilon_m R^{1/n}), \tag{3.65}$$

where $\epsilon_1, \ldots, \epsilon_m$ are n-th roots of unity. Comparing the coefficients of x^0 on the right sides of (3.64) and (3.65), we obtain $\dfrac{F_0(y)}{F_m(y)} = (-1)^m\epsilon_1\ldots\epsilon_m R^{m/n}$, then $R^{m/n} = (-1)^m \dfrac{F_0(y)}{\epsilon_1\ldots\epsilon_m F_m(y)}$, so $R^{m/n}$ is a rational function in y. Put $g := \gcd(m,n)$ and $s := \dfrac{n}{g}$. Since $m < n$, $n \neq g$. Then $s > 1$. There exist $a, b \in \mathbb{Z}$ such that $an - bm = g$. It follows that $R^{1/s} = R^{g/n} = R^{(an-bm)/n} = R^{a-bm/n} = R^a(R^{m/n})^{-b}$. Since R and $R^{m/n}$ are rational functions in y, $R^{1/s}$ is a rational function in y, and we can write $R^{1/s} = \dfrac{f(y)}{g(y)}$ where f and g are relatively prime polynomials in y. Thus $\dfrac{f^s}{g^s} = R = -\dfrac{1+y^n}{1+cy^q}$, so $(1+y^n)g^s = -(1+cy^q)f^s$. Suppose f is not a constant. Since $s > 1$, f^s has the multiple factors which cannot occur in $(1+y^n)g^s$ as f and g are relatively prime and $1+y^n$ has no multiple factors. Then f must be a constant. Similarly, g must be a constant, so $R = \dfrac{f^s}{g^s}$ is a constant, which is a contradiction. Hence Z does not have a factor of degree $m < n$ in x for $p = n$.

Assume now that Z has a factor of degree n in x, say $F(x,y)$. Suppose $Z = F(x,y)G(x,y)$. Then $x^n(1+cy^q)+(1+y^n) = F(x,y)G(x,y)$, so we can write $F(x,y) := F_n(y)x^n + F_0(y)$ and $G(x,y) := G(y)$. Thus $x^n(1+cy^q) + (1+y^n) = \big(F_n(y)x^n + F_0(y)\big)G(y) = F_n(y)G(y)x^n + F_0(y)G(y)$. Comparing the coefficients on both sides, we obtain $1+cy^q = F_n(y)G(y)$ and $1+y^n = F_0(y)G(y)$, so $1+cy^q$ and $1+y^n$ have common factors.

Write $c := e^{-\xi\pi i}$ with $\xi \in \mathbb{C}$. Note that $1+cy^q = 1+e^{-\xi\pi i}y^q = 1+\big(e^{-\xi\pi i/q}y\big)^q = \prod_{\kappa=0}^{q-1}\big(e^{-\xi\pi i/q}y - e^{(2\kappa+1)\pi i/q}\big) = \big(e^{-\xi\pi i/q}\big)^q\prod_{\kappa=0}^{q-1}\big(y - e^{(\xi+2\kappa+1)\pi i/q}\big) = c\prod_{\kappa=0}^{q-1}\big(y-e^{(\xi+2\kappa+1)\pi i/q}\big)$ and $1+y^n = \prod_{\lambda=0}^{n-1}\big(y-e^{(2\lambda+1)\pi i/n}\big)$. Since $1+cy^q$ and $1+y^n$ have common factors, there exist $\kappa \in \{0,\ldots,q-1\}$ and $\lambda \in \{0,\ldots,n-1\}$ such that $e^{(\xi+2\kappa+1)\pi i/q} = e^{(2\lambda+1)\pi i/n}$. We have that $\dfrac{(\xi+2\kappa+1)\pi}{q} \equiv \dfrac{(2\lambda+1)\pi}{n} \pmod{2\pi}$, so $\dfrac{\xi+2\kappa+1}{q} \equiv \dfrac{2\lambda+1}{n} \pmod 2$. Then $\dfrac{\xi+2\kappa+1}{q} = \dfrac{2\lambda+1}{n} + 2r$ for some $r \in \mathbb{Z}$. Thus $\xi = \dfrac{(2\lambda+1)q}{n} + 2rq - 2\kappa - 1$, and $c = \exp(1-(2\lambda+1)q/n)\pi i$.

From now on, assume that $p \neq n$ and $q \neq n$.

We will show that if $p < n$ and $q < n$, then Z in (3.63) is always irreducible. Suppose that Z is reducible. If we apply Lemma 3.3.1, replacing there z with x and k with p, we obtain in the notations of Lemma 3.3.1 that $\varphi = 1 + y^n$, $\psi_1 = cy^q$ and $\chi = 1$. Thus if we use the degree in y as weight, all conditions of Lemma 3.3.1 are satisfied. It follows that n is divisible by p. And similarly, n is divisible by q. Then $\frac{n}{p}, \frac{n}{q} \in \mathbb{Z}^+$. Since $p, q \neq n$, $\frac{n}{p}, \frac{n}{q} \geq 2$. So $p, q \leq \frac{n}{2}$. Thus $p + q \leq n$, which is a contradiction.

From now on, we assume that $p > n$ and $q \neq n$ since we can interchange x with y. Observe that if $q < n$, then the form (3.63) can be somewhat simplified. In this case, we can apply Lemma 3.3.1, replacing there z with x and n with p, we obtain in the notations of Lemma 3.3.1 that $\varphi = 1 + y^n$, $\psi_1 = 1$ and $\chi = cy^q$. Thus if we use the degree in y as weight, all conditions of Lemma 3.3.1 are satisfied. It follows that p is divisible by n. Then $p = nr$ for some $r \in \mathbb{Z}^+$. Since $p \neq n$, $r > 1$. By changing the notations, we can reduce (3.63) to the form

$$Z = 1 + x + y^n + cx^py^q \quad (c \neq 0,\ 1 < q < n,\ p > 1). \tag{3.66}$$

Lemma 3.8.1. If Z in (3.66) is reducible, then the factors of Z cannot be independent of x.

Proof. Suppose that $Z = F(y)G(x, y)$ where $F(y)$ and $G(x, y)$ are proper integer polynomials. Then we have $1 + x + y^n + cx^py^q = F(y)G(x, y)$, so the degree of $G(x, y)$ in x is p. Since $p \geq 2$, we can write $G(x, y) = G_2(x, y)x^2 + G_1(y)x + G_0(y)$, where $G_2(x, y), G_1(y), G_0(y)$ are integer polynomials and the degree of $G_2(x, y)$ in x is $p - 2$. So $1 + x + y^n + cx^py^q = F(y)G_2(x, y)x^2 + F(y)G_1(y)x + F(y)G_0(y)$. Comparing the coefficients of x on both sides, we have $1 = F(y)G_1(y)$, which is impossible since $F(y)$ is proper. □

We will show that in the cases $p = 2$ and $p = 3$ (3.66) is always irreducible. First, consider the case $p = 2$, then (3.66) becomes

$$Z = 1 + x + y^n + cx^2y^q.$$

Suppose that Z is reducible. By Lemma 3.8.1, we have the decomposition

$$\begin{aligned}1 + x + y^n + cx^2y^q &= \big(F_1(y)x + F_0(y)\big)\big(G_1(y)x + G_0(y)\big)\\ &= F_1(y)G_1(y)x^2 + \big(F_1(y)G_0(y) + F_0(y)G_1(y)\big)x + F_0(y)G_0(y),\end{aligned}$$

where $F_1(y), G_1(y) \neq 0$. Comparing the coefficients on both sides, we obtain

$$cy^q = F_1(y)G_1(y), \tag{3.67}$$

$$1 = F_1(y)G_0(y) + F_0(y)G_1(y), \tag{3.68}$$

$$1 + y^n = F_0(y)G_0(y). \tag{3.69}$$

By (3.69), since $F_0(y)$ and $G_0(y)$ have coefficients in a field, we may assume that both are monic. Write $F_0(y) = y^{f_0} + \gamma_{f_0-1}y^{f_0-1} + \cdots + \gamma_1 y + \gamma_0$. If $\gamma_0 = 0$, then $y|\, F_0(y)$. By (3.69), it follows that $y|\,(1 + y^n)$, which is impossible. Thus $\gamma_0 \neq 0$. And write $G_0(y) = y^{g_0} + \delta_{g_0-1}y^{g_0-1} + \cdots + \delta_1 y + \delta_0$. Also, by (3.69), it follows that $\delta_0 \neq 0$. By (3.67), we can write $F_1(y) = \alpha y^{f_1}$ and $G_1(y) = \beta y^{g_1}$ where $\alpha, \beta \neq 0$, $\alpha\beta = c$, $f_1, g_1 \geq 0$ and $f_1 + g_1 = q$. Then (3.68) becomes

$$1 = \alpha y^{f_1}G_0(y) + \beta y^{g_1}F_0(y). \tag{3.70}$$

If $f_1, g_1 > 0$, then the right side of (3.70) is divisible by y, so $y|\,1$, which is impossible. Thus $f_1 = 0$ or $g_1 = 0$.

Case 1. $f_1 = 0$. Then $g_1 = q$, $F_1(y) = \alpha$ and $G_1(y) = \beta y^q$. Comparing the degrees of (3.68), we have $g_0 = f_0 + q$. Comparing the degrees of (3.69), we have $n = f_0 + g_0$, so $n = f_0 + (f_0 + q) = q + 2f_0$. Since $n > q$, it follows that $f_0 > 0$. By (3.68), we have

$$1 = \alpha G_0(y) + \beta y^q F_0(y).$$

Comparing the coefficients of y^{g_0} on both sides, we obtain $0 = \alpha + \beta$, so $\alpha = -\beta$. Then $G_0(y) = \frac{1}{\alpha}\big(1 - \beta y^q F_0(y)\big) = \frac{1}{\alpha}\big(1 + \alpha y^q F_0(y)\big)$. Replacing $G_0(y) = \frac{1}{\alpha}\big(1 + \alpha y^q F_0(y)\big)$ in (3.69), we obtain $1 + y^{q+2f_0} = \frac{1}{\alpha} F_0(y)\big(1 + \alpha y^q F_0(y)\big)$, so

$$\begin{aligned}
\alpha + \alpha y^{q+2f_0} &= F_0(y) + \alpha y^q \big(F_0(y)\big)^2 \\
&= (y^{f_0} + \gamma_{f_0-1} y^{f_0-1} + \cdots + \gamma_1 y + \gamma_0) \\
&\quad + \alpha y^q \big[y^{2f_0} + (\gamma_{f_0-1} + \gamma_{f_0-1}) y^{2f_0-1} \\
&\quad + (\gamma_{f_0-2} + \gamma_{f_0-1}\gamma_{f_0-1} + \gamma_{f_0-2}) y^{2f_0-2} \\
&\quad + \cdots + (\gamma_0 + \gamma_{f_0-1}\gamma_1 + \gamma_{f_0-2}\gamma_2 + \cdots + \gamma_0) y^{f_0} \\
&\quad + \cdots + (\gamma_2\gamma_0 + \gamma_1\gamma_1 + \gamma_0\gamma_2) y^2 + (\gamma_1\gamma_0 + \gamma_0\gamma_1) y + \gamma_0^2\big].
\end{aligned}$$

Comparing the coefficients of y^{q+2f_0-1} on both sides, we obtain $0 = \alpha(\gamma_{f_0-1} + \gamma_{f_0-1})$. Since $\alpha \neq 0$, $\gamma_{f_0-1} = 0$. Comparing the coefficients of y^{q+2f_0-2} on both sides, we obtain $0 = \alpha(\gamma_{f_0-2} + \gamma_{f_0-1}\gamma_{f_0-1} + \gamma_{f_0-2})$. Since $\alpha \neq 0$ and $\gamma_{f_0-1} = 0$, $\gamma_{f_0-2} = 0$. Also, by comparing the coefficients of $y^{q+2f_0-3}, \ldots, y^{q+2f_0-f_0+1}$ on both sides, we obtain $\gamma_{f_0-3} = \cdots = \gamma_{f_0-f_0+1} = 0$. Finally, Comparing the coefficients of $y^{q+2f_0-f_0} = y^{q+f_0}$ on both sides, we obtain $0 = \alpha(\gamma_0 + \gamma_{f_0-1}\gamma_1 + \gamma_{f_0-2}\gamma_2 + \cdots + \gamma_0)$. Since $\alpha \neq 0$ and $\gamma_{f_0-1} = \cdots = \gamma_1 = 0$, $\gamma_0 = 0$. This is a contradiction.

Case 2. $g_1 = 0$. Then $f_1 = q$, $F_1(y) = \alpha y^q$ and $G_1(y) = \beta$. Comparing the degrees of (3.68), we have $q + g_0 = f_0$. Comparing the degrees of (3.69), we have $n = f_0 + g_0$, so $n = (q+g_0)+g_0 = q+2g_0$. Since $n > q$, it follows that $g_0 > 0$. By (3.68), we have

$$1 = \alpha y^q G_0(y) + \beta F_0(y).$$

Comparing the coefficients of y^{f_0} on both sides, we obtain $0 = \alpha+\beta$, so $\beta = -\alpha$. Then $F_0(y) = \frac{1}{\beta}\big(1 - \alpha y^q G_0(y)\big) = \frac{1}{\beta}\big(1 + \beta y^q G_0(y)\big)$. Replacing $F_0(y) = \frac{1}{\beta}\big(1 + \beta y^q G_0(y)\big)$ in (3.69), we obtain $1 + y^{q+2g_0} = \frac{1}{\beta}\big(1 + \beta y^q G_0(y)\big)G_0(y)$, so

$$\begin{aligned}\beta + \beta y^{q+2g_0} &= G_0(y) + \beta y^q \big(G_0(y)\big)^2 \\ &= (y^{g_0} + \delta_{g_0-1}y^{g_0-1} + \cdots + \delta_1 y + \delta_0) \\ &\quad + \beta y^q \big[y^{2g_0} + (\delta_{g_0-1} + \delta_{g_0-1})y^{2g_0-1} \\ &\quad + (\delta_{g_0-2} + \delta_{g_0-1}\delta_{g_0-1} + \delta_{g_0-2})y^{2g_0-2} \\ &\quad + \cdots + (\delta_0 + \delta_{g_0-1}\delta_1 + \delta_{g_0-2}\delta_2 + \cdots + \delta_0)y^{g_0} \\ &\quad + \cdots + (\delta_2\delta_0 + \delta_1\delta_1 + \delta_0\delta_2)y^2 + (\delta_1\delta_0 + \delta_0\delta_1)y + \delta_0^2\big].\end{aligned}$$

Comparing the coefficients of y^{q+2g_0-1} on both sides, we obtain $0 = \beta(\delta_{g_0-1} + \delta_{g_0-1})$. Since $\beta \neq 0$, $\delta_{g_0-1} = 0$. Comparing the coefficients of y^{q+2g_0-2} on both sides, we obtain $0 = \beta(\delta_{g_0-2} + \delta_{g_0-1}\delta_{g_0-1} + \delta_{g_0-2})$. Since $\beta \neq 0$ and $\delta_{g_0-1} = 0$, $\delta_{g_0-2} = 0$. Also, by comparing the coefficients of $y^{q+2g_0-3}, \ldots, y^{q+2g_0-g_0+1}$ on both sides, we obtain $\delta_{g_0-3} = \cdots = \delta_{g_0-g_0+1} = 0$. Finally, Comparing the coefficients of $y^{q+2g_0-g_0} = y^{q+g_0}$ on both sides, we obtain $0 = \beta(\delta_0 + \delta_{g_0-1}\delta_1 + \delta_{g_0-2}\delta_2 + \cdots + \delta_0)$. Since $\beta \neq 0$ and $\delta_{g_0-1} = \cdots = \delta_1 = 0$, $\delta_0 = 0$. This is a contradiction.

Hence for the case $p = 2$, (3.66) is irreducible.

Now, consider the case $p = 3$, then (3.66) becomes

$$Z = 1 + x + y^n + cx^3y^q.$$

Suppose that Z is reducible. By Lemma 3.8.1, we have the decomposition

$$\begin{aligned} 1 + x + y^n + cx^3y^q &= \big(F_1(y)x + F_0(y)\big)\big(G_2(y)x^2 + G_1(y)x + G_0(y)\big) \\ &= F_1(y)G_2(y)x^3 + \big(F_1(y)G_1(y) + F_0(y)G_2(y)\big)x^2 \\ &\quad + \big(F_1(y)G_0(y) + F_0(y)G_1(y)\big)x + F_0(y)G_0(y), \end{aligned}$$

where $F_1(y), G_2(y) \neq 0$. Comparing the coefficients on both sides, we obtain

$$cy^q = F_1(y)G_2(y), \tag{3.71}$$

$$0 = F_1(y)G_1(y) + F_0(y)G_2(y), \tag{3.72}$$

$$1 = F_1(y)G_0(y) + F_0(y)G_1(y), \tag{3.73}$$

$$1 + y^n = F_0(y)G_0(y). \tag{3.74}$$

By (3.74), since $F_0(y)$ and $G_0(y)$ have coefficients in a field, we may assume that both are monic. Write $F_0(y) = y^{f_0} + \gamma_{f_0-1}y^{f_0-1} + \cdots + \gamma_1 y + \gamma_0$. If $\gamma_0 = 0$, then $y|\, F_0(y)$. By (3.74), it follows that $y|\,(1+y^n)$, which is impossible. Thus $\gamma_0 \neq 0$. By (3.71), we can write $F_1(y) = \alpha y^{f_1}$ and $G_2(y) = \beta y^{g_2}$ where $\alpha, \beta \neq 0$, $\alpha\beta = c$, $f_1, g_2 \geq 0$ and $f_1 + g_2 = q$. Then (3.72) becomes

$$0 = \alpha y^{f_1}G_1(y) + \beta y^{g_2}F_0(y). \tag{3.75}$$

If $f_1 > g_2 > 0$, dividing (3.75) by y^{g_2}, we have

$$0 = \alpha y^{f_1 - g_2} G_1(y) + \beta F_0(y).$$

Then $y|\, F_0(y)$. By (3.74), it follows that $y|\,(1+y^n)$, which is impossible.

If $g_2 > f_1 > 0$, dividing (3.75) by y^{f_1}, we have

$$0 = \alpha G_1(y) + \beta y^{g_2 - f_1} F_0(y).$$

Then $y|\, G_1(y)$. By (3.73), it follows that $y|\, \big(1 - F_1(y)G_0(y)\big)$. Since $f_1 > 0$, $y|\, F_1(y)$. Thus $y|\, 1$, which is impossible.

We have now three remaining cases to consider :

$$f_1 = g_2 = \frac{q}{2}; \quad f_1 = 0; \quad g_2 = 0.$$

Case 1. $f_1 = g_2 = \frac{q}{2}$. Then $F_1(y) = \alpha y^{q/2}$ and $G_2(y) = \beta y^{q/2}$. Denote the degrees of $G_0(y)$ and $G_1(y)$ by g_0 and g_1, respectively. Comparing the degrees of (3.72), we have $\frac{q}{2} + g_1 = f_0 + \frac{q}{2}$, so $g_1 = f_0$. Comparing the degrees of (3.73), we have $\frac{q}{2} + g_0 = f_0 + g_1$, so $g_0 = f_0 + g_1 - \frac{q}{2} = 2f_0 - \frac{q}{2}$. Comparing the degrees of (3.74), we have $n = f_0 + g_0$, so $n = f_0 + \left(2f_0 - \frac{q}{2}\right) = 3f_0 - \frac{q}{2}$. Since $n > q$, it follows that $f_0 > \frac{q}{2}$. By (3.72), we have $0 = \alpha y^{q/2} G_1(y) + \beta y^{q/2} F_0(y)$. Then $G_1(y) = -\frac{\beta}{\alpha} F_0(y)$. By (3.73), we have

$$1 = \alpha y^{q/2} G_0(y) - \frac{\beta}{\alpha}\big(F_0(y)\big)^2.$$

Comparing the coefficients of y^{2f_0} on both sides, we obtain $0 = \alpha - \frac{\beta}{\alpha}$, so $\alpha = \frac{\beta}{\alpha}$. Then $G_0(y) = \frac{1}{\alpha y^{q/2}}\left(1 + \frac{\beta}{\alpha}\big(F_0(y)\big)^2\right) = \frac{1}{\alpha y^{q/2}}\left(1 + \alpha\big(F_0(y)\big)^2\right)$. Replacing $G_0(y) = \frac{1}{\alpha y^{q/2}}\left(1 + \alpha\big(F_0(y)\big)^2\right)$ in (3.74), we obtain $1 + y^{3f_0 - q/2} = \frac{1}{\alpha y^{q/2}} F_0(y)\left(1 + \alpha\big(F_0(y)\big)^2\right)$, so

$$\alpha y^{q/2} + \alpha y^{3f_0} = F_0(y)\Big(1 + \alpha\big(F_0(y)\big)^2\Big) \tag{3.76}$$

If $y|\, F_0(y)$, by (3.74), it follows that $y|\,(1+y^n)$, which is impossible. Then $y \nmid F_0(y)$. By (3.76), it follows that $y \,\Big|\, \Big(1+\alpha\big(F_0(y)\big)^2\Big)$. Note that $1+\alpha\big(F_0(y)\big)^2 = 1+\alpha\big[y^{2f_0} + (\gamma_{f_0-1}+\gamma_{f_0-1})y^{2f_0-1} + (\gamma_{f_0-2}+\gamma_{f_0-1}\gamma_{f_0-1}+\gamma_{f_0-2})y^{2f_0-2} + \cdots + (\gamma_0+\gamma_{f_0-1}\gamma_1+\gamma_{f_0-2}\gamma_2 + \cdots + \gamma_0)y^{f_0} + \cdots + (\gamma_2\gamma_0+\gamma_1\gamma_1+\gamma_0\gamma_2)y^2 + (\gamma_1\gamma_0+\gamma_0\gamma_1)y + \gamma_0^2\big]$. Thus $1+\alpha\gamma_0^2 = 0$. Then (3.76) becomes

$$\begin{aligned}
\alpha y^{q/2} + \alpha y^{3f_0} = {} & (y^{f_0} + \gamma_{f_0-1}y^{f_0-1} + \cdots + \gamma_1 y + \gamma_0)\alpha\big[y^{2f_0} \\
& + (\gamma_{f_0-1}+\gamma_{f_0-1})y^{2f_0-1} + (\gamma_{f_0-2}+\gamma_{f_0-1}\gamma_{f_0-1}+\gamma_{f_0-2})y^{2f_0-2} \\
& + \cdots + (\gamma_0+\gamma_{f_0-1}\gamma_1+\gamma_{f_0-2}\gamma_2+\cdots+\gamma_0)y^{f_0} \\
& + \cdots + (\gamma_2\gamma_0+\gamma_1\gamma_1+\gamma_0\gamma_2)y^2 + (\gamma_1\gamma_0+\gamma_0\gamma_1)y\big], \text{ so} \\
y^{q/2} + y^{3f_0} = {} & (y^{f_0} + \gamma_{f_0-1}y^{f_0-1} + \cdots + \gamma_1 y + \gamma_0)\big[y^{2f_0} \\
& + (\gamma_{f_0-1}+\gamma_{f_0-1})y^{2f_0-1} + (\gamma_{f_0-2}+\gamma_{f_0-1}\gamma_{f_0-1}+\gamma_{f_0-2})y^{2f_0-2} \\
& + \cdots + (\gamma_0+\gamma_{f_0-1}\gamma_1+\gamma_{f_0-2}\gamma_2+\cdots+\gamma_0)y^{f_0} \\
& + \cdots + (\gamma_2\gamma_0+\gamma_1\gamma_1+\gamma_0\gamma_2)y^2 + (\gamma_1\gamma_0+\gamma_0\gamma_1)y\big].
\end{aligned}$$

Comparing the coefficients of y^{3f_0-1} on both sides, we obtain $0 = (\gamma_{f_0-1}+\gamma_{f_0-1}) + \gamma_{f_0-1}$. Then $\gamma_{f_0-1} = 0$. Comparing the coefficients of y^{3f_0-2} on both sides, we obtain $0 = (\gamma_{f_0-2}+\gamma_{f_0-1}\gamma_{f_0-1}+\gamma_{f_0-2})+\gamma_{f_0-1}(\gamma_{f_0-1}+\gamma_{f_0-1})+\gamma_{f_0-2}$. Since $\gamma_{f_0-1}=0$, $\gamma_{f_0-2}=0$. Also, by comparing the coefficients of $y^{3f_0-3}, \ldots, y^{3f_0-f_0+1}$ on both sides, we obtain $\gamma_{f_0-3} = \cdots = \gamma_{f_0-f_0+1} = 0$. Finally, Comparing the coefficients of $y^{3f_0-f_0} = y^{2f_0}$ on hoth sides, we obtain $0 = (\gamma_0+\gamma_{f_0-1}\gamma_1+\gamma_{f_0-2}\gamma_2+\cdots+\gamma_0)+\cdots+\gamma_1(\gamma_{f_0-1}+\gamma_{f_0-1})+\gamma_0$. Since $\gamma_{f_0-1} = \cdots = \gamma_1 = 0$, $\gamma_0 = 0$. This is a contradiction.

Case 2. $f_1 = 0$. Then $g_2 = q$, $F_1(y) = \alpha$ and $G_2(y) = \beta y^q$. Denote the degrees of $G_0(y)$ and $G_1(y)$ by g_0 and g_1, respectively. Comparing the degrees of (3.72), we have $g_1 = f_0 + q$. Comparing the degrees of (3.73), we have $g_0 = f_0 + g_1$, so $g_0 = f_0 + (f_0 + q) = 2f_0 + q$. Comparing the degrees of (3.74), we have $n = f_0 + g_0$, so $n = f_0 + (2f_0 + q) = 3f_0 + q$. Since $n > q$, it follows that $f_0 > 0$. By (3.72), we have $0 = \alpha G_1(y) + \beta y^q F_0(y)$. Then $G_1(y) = -\frac{\beta}{\alpha} y^q F_0(y)$. By (3.73), we have

$$1 = \alpha G_0(y) - \frac{\beta}{\alpha} y^q \big(F_0(y)\big)^2.$$

Comparing the coefficients of y^{g_0} on both sides, we obtain $0 = \alpha - \frac{\beta}{\alpha}$, so $\alpha = \frac{\beta}{\alpha}$. Then $G_0(y) = \frac{1}{\alpha}\Big(1 + \frac{\beta}{\alpha} y^q \big(F_0(y)\big)^2\Big) = \frac{1}{\alpha}\Big(1 + \alpha y^q \big(F_0(y)\big)^2\Big)$. Replacing $G_0(y) = \frac{1}{\alpha}\Big(1 + \alpha y^q \big(F_0(y)\big)^2\Big)$ in (3.74), we obtain $1 + y^{3f_0+q} = \frac{1}{\alpha} F_0(y)\Big(1 + \alpha y^q \big(F_0(y)\big)^2\Big)$, so

$$\begin{aligned}
\alpha + \alpha y^{3f_0+q} &= F_0(y) + \alpha y^q F_0(y)\big(F_0(y)\big)^2 \\
&= (y^{f_0} + \gamma_{f_0-1} y^{f_0-1} + \cdots + \gamma_1 y + \gamma_0) + \alpha y^q (y^{f_0} + \gamma_{f_0-1} y^{f_0-1} \\
&\quad + \cdots + \gamma_1 y + \gamma_0)\big[y^{2f_0} + (\gamma_{f_0-1} + \gamma_{f_0-1}) y^{2f_0-1} \\
&\quad + (\gamma_{f_0-2} + \gamma_{f_0-1}\gamma_{f_0-1} + \gamma_{f_0-2}) y^{2f_0-2} \\
&\quad + \cdots + (\gamma_0 + \gamma_{f_0-1}\gamma_1 + \gamma_{f_0-2}\gamma_2 + \cdots + \gamma_0) y^{f_0} \\
&\quad + \cdots + (\gamma_2\gamma_0 + \gamma_1\gamma_1 + \gamma_0\gamma_2) y^2 + (\gamma_1\gamma_0 + \gamma_0\gamma_1) y + \gamma_0^2\big].
\end{aligned}$$

Comparing the coefficients of y^0 on both sides, we obtain $\alpha = \gamma_0$. Then

$$\alpha y^{3f_0+q} = (y^{f_0} + \gamma_{f_0-1}y^{f_0-1} + \cdots + \gamma_1 y) + \alpha y^q (y^{f_0} + \gamma_{f_0-1}y^{f_0-1}$$
$$+ \cdots + \gamma_1 y + \gamma_0)\big[y^{2f_0} + (\gamma_{f_0-1} + \gamma_{f_0-1})y^{2f_0-1}$$
$$+ (\gamma_{f_0-2} + \gamma_{f_0-1}\gamma_{f_0-1} + \gamma_{f_0-2})y^{2f_0-2}$$
$$+ \cdots + (\gamma_0 + \gamma_{f_0-1}\gamma_1 + \gamma_{f_0-2}\gamma_2 + \cdots + \gamma_0)y^{f_0}$$
$$+ \cdots + (\gamma_2\gamma_0 + \gamma_1\gamma_1 + \gamma_0\gamma_2)y^2 + (\gamma_1\gamma_0 + \gamma_0\gamma_1)y + \gamma_0^2\big]. \tag{3.77}$$

It follows that $y^q | (y^{f_0} + \gamma_{f_0-1}y^{f_0-1} + \cdots + \gamma_1 y)$. Thus $q \leq f_0$ and $\gamma_{q-1} = \cdots = \gamma_1 = 0$. Dividing (3.77) by y^q, we have

$$\alpha y^{3f_0} = (y^{f_0-q} + \gamma_{f_0-1}y^{f_0-1-q} + \cdots + \gamma_q y^{q-q}) + \alpha(y^{f_0} + \gamma_{f_0-1}y^{f_0-1}$$
$$+ \cdots + \gamma_1 y + \gamma_0)\big[y^{2f_0} + (\gamma_{f_0-1} + \gamma_{f_0-1})y^{2f_0-1}$$
$$+ (\gamma_{f_0-2} + \gamma_{f_0-1}\gamma_{f_0-1} + \gamma_{f_0-2})y^{2f_0-2}$$
$$+ \cdots + (\gamma_0 + \gamma_{f_0-1}\gamma_1 + \gamma_{f_0-2}\gamma_2 + \cdots + \gamma_0)y^{f_0}$$
$$+ \cdots + (\gamma_2\gamma_0 + \gamma_1\gamma_1 + \gamma_0\gamma_2)y^2 + (\gamma_1\gamma_0 + \gamma_0\gamma_1)y + \gamma_0^2\big].$$

Comparing the coefficients of y^{3f_0-1} on both sides, we obtain $0 = \alpha\big((\gamma_{f_0-1} + \gamma_{f_0-1}) + \gamma_{f_0-1}\big)$. Since $\alpha \neq 0$, $\gamma_{f_0-1} = 0$. Comparing the coefficients of y^{3f_0-2} on both sides, we obtain $0 = \alpha\big((\gamma_{f_0-2}+\gamma_{f_0-1}\gamma_{f_0-1}+\gamma_{f_0-2})+\gamma_{f_0-1}(\gamma_{f_0-1}+\gamma_{f_0-1})+\gamma_{f_0-2}\big)$. Since $\alpha \neq 0$ and $\gamma_{f_0-1} = 0$, $\gamma_{f_0-2} = 0$. Also, by comparing the coefficients of $y^{3f_0-3}, \ldots, y^{3f_0-f_0+1}$ on both sides, we obtain $\gamma_{f_0-3} = \cdots = \gamma_{f_0-f_0+1} = 0$. Finally, Comparing the coefficients of $y^{3f_0-f_0} = y^{2f_0}$ on both sides, we obtain $0 = \alpha\big((\gamma_0 + \gamma_{f_0-1}\gamma_1 + \gamma_{f_0-2}\gamma_2 + \cdots + \gamma_0) + \cdots + \gamma_1(\gamma_{f_0-1} + \gamma_{f_0-1}) + \gamma_0\big)$. Since $\alpha \neq 0$ and $\gamma_{f_0-1} = \cdots = \gamma_1 = 0$, $\gamma_0 = 0$. This is a contradiction.

Case 3. $g_2 = 0$. Then $f_1 = q$, $F_1(y) = \alpha y^q$ and $G_2(y) = \beta$. By (3.72), we have $0 = \alpha y^q G_1(y) + \beta F_0(y)$. Then $F_0(y) = -\frac{\alpha}{\beta} y^q G_1(y)$. Thus $y^q | F_0(y)$. By (3.74), it follows that $y^q | (1 + y^n)$, which is impossible.

Hence for the case $p = 3$, (3.66) is irreducible.

REFERENCES

[1] Ostrowski, A. M. On the multiplication and factorization of polynomials: I. Lexicographic orderings and extreme aggregates of terms. **Aequationes Math**. 13(1975): 201-228.

[2] Ostrowski, A. M. On the multiplication and factorization of polynomials: II. Irreducibility discussion. **Aequationes Math.** 14(1976): 1-32.

VITA

Miss Amarisa Chantanasiri was born on March 20, 1980 in Bangkok, Thailand. She graduated with a Bachelor of Science in Mathematics with first class honours from Chulalongkorn University in 2001. She has got a scholarship from the Development and Promotion for Science and Technology Talents Project (DPST) since 1998. For her Master degree, she has studied Mathematics at the Department of Mathematics, Faculty of Science, Chulalongkorn University.