

**Functional equations involving Laurent
polynomials and meromorphic functions, with
applications to dynamics and Diophantine
equations**

by
Sijun Liu

A dissertation submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
(Mathematics)
in The University of Michigan
2014

Doctoral Committee:

Professor Michael E. Zieve, Chair
Professor Jeffrey C. Lagarias
Visiting Assistant Professor Dani Neftin
Assistant Professor Andrew Snowden
Professor James P. Tappenden

To my wife Tianjun

ACKNOWLEDGEMENTS

I would like to express my sincere gratitude my advisor, Professor Michael Zieve, for everything he has done for me over the past four years. I would not have been able to proceed this far without his continuous encouragement, generous support, patient guidance and and plentiful advice. I would like to thank him for his patient guidance which leads me step by step into the wonderland of number theory, for providing me such an interesting and meaningful thesis topic and for providing me all the support and all the help I need during the past four years. I am very lucky to have such a perfect advisor.

I would like to thank Professor Danny Neftin and Jeffery Lagarias for reading my thesis and providing many helpful comments on my thesis. I would like to thank Tara McQueen, Kathryn Beeman for their encouragement and help at Michigan. I would like to thank Maria Ryen for her help on my English. I would like to thank my colleagues Linqun Ma, Jingchen Wu, Yu-Jui Huang, Yilun Wu, Zhipeng Liu, Zhixian Zhu, Kin-Kwan Leung, Hieu Ngo, Yuting Yang, Yefeng Shen, Xin Zhou, Zhou Zhou, with whom I never felt alone.

I would like to give my special thanks to my wife, Tianjun, for her love and understanding for this six-year long-distance relationship. With her every place on the planet is my warm home. She is an inseparable part of my life and I cannot imagine what my life during these years would have been like without her constant love and support. To her I dedicate this thesis.

TABLE OF CONTENTS

DEDICATION	ii
ACKNOWLEDGEMENTS	iii
LIST OF FIGURES	vi
LIST OF TABLES	vii
 CHAPTER	
I. Introduction	1
1.1 Main theorem	1
1.2 Application I: Complex functional equations	7
1.3 Application II: Diophantine equations and near-injectivity of rational functions	10
II. Proof of Theorem I.5 and Theorem I.6	14
2.1 Notation and terminology	14
2.2 Outline of the thesis	15
2.3 Proof of Theorem I.5	16
2.3.1 Case 1: $\mathbb{K}(r) = \mathbb{K}(s)$	17
2.3.2 Case 2: $\mathbb{K}(r) \neq \mathbb{K}(s)$, but $\mathbb{K}(u) = \mathbb{K}(v)$	18
2.3.3 Case 3: $\mathbb{K}(u) \neq \mathbb{K}(v)$	20
2.4 Proof of Theorem I.6	20
III. Preliminaries	22
3.1 Decomposability	23
3.2 Curves and function fields	25
3.3 Function field tower	25
3.4 Ramification and genus	28
3.4.1 Places and ramification	28
3.4.2 Monodromy groups, Riemann's existence theorem and ramification	29
3.4.3 Abhyankar's lemma, genus and Riemann-Hurwitz formula	31
3.5 Degree of the composite of two extensions of a function field	34
3.6 Facts on the factorization of certain polynomials	36
3.7 Ramification and decomposability	37
3.8 Inequalities connected with the Riemann-Hurwitz formula	40
3.9 Equivalent and strongly equivalent functions	43
IV. Indecomposable genuine Laurent polynomial case: Part I	44
4.1 Setup and some inequalities	45

4.2	Large degree cases: when $n = \deg(f) \geq 26$	49
4.3	Proof of Theorem IV.1	53
V. Indecomposable genuine Laurent polynomial case: Part II		55
5.1	Monodromy groups of indecomposable genuine Laurent polynomials	56
5.2	Wreath products as monodromy groups	58
5.2.1	The structure of τ_i 's	58
5.2.2	Genus of the two components	62
5.3	Proof of Theorem V.1	64
VI. Decomposable case: indecomposable genuine Laurent polynomial composed with cyclic polynomial		65
VII. Decomposable case: polynomial composed with genuine Laurent polynomial: Part I		69
7.1	When P satisfies case 1 or case 6 (where $\gcd(r, s) = 1$) in Theorem VII.3	72
7.2	When P satisfies case 4 in Theorem VII.3	81
7.3	Proof of Theorem VII.1	92
VIII. Decomposable case: polynomial composed with genuine Laurent polynomial: Part II		94
IX. The case that $f(X) - cf(Y)$ is irreducible		96
9.1	Riemann-Hurwitz genus formula and reduced sequences	96
9.2	Main result: Classification of f for which $F_{f,c}(X, Y)$ is irreducible of genus at most 1	99
9.3	The case $ \Lambda_c =2$	101
9.4	The case $ \Lambda_c \geq 3$	102
9.4.1	The case $A = A_m = 1$, $m = 4$, and the case $A = A_m = 2$, $m = 3$	104
9.4.2	The case $A = A_m = 0$, $A_m^{(1)} = 1$, with $n \geq 5$	105
9.4.3	The case $A = A_m = 1$, $m = 3$, with $n \geq 7$	108
9.4.4	The remaining cases	109
9.5	Summary and proof of Theorem IX.6	113
X. The case that $f(X) - cf(Y)$ is reducible		118
10.1	Indecomposable case	118
10.2	Decomposable case I: $f = P \circ L$	124
10.2.1	The cases where the pair (P, c) is in Table 10.2	125
10.2.2	The case $P = T_2$ and $c \in \mathbb{K}^* \setminus \{1\}$	128
10.2.3	The case $P = X^a(X - 1)^b$	132
10.2.4	The classification of genuine Laurent polynomials f where $f(X) - cf(Y)$ is reducible with a genus zero or one factor	134
10.3	Decomposable case II: $f = \tilde{f} \circ X^m$	135
10.3.1	When $F_{\tilde{f},c}$ is irreducible	136
10.3.2	When $F_{\tilde{f},c}$ is reducible	137
BIBLIOGRAPHY		139

LIST OF FIGURES

Figure

2.1	Tower of function fields	19
3.1	Function field tower	25
3.2	Function field tower	26
3.3	Tower of function fields	27
7.1	Tower of function fields	71

LIST OF TABLES

Table

1.1	$F_h(X, Y)$ has a genus 0 or 1 irreducible factor: sporadic cases part I	5
1.2	$F_h(X, Y)$ has a genus 0 or 1 irreducible factor: sporadic cases part II	6
1.3	$F_h(X, Y)$ has a genus 0 or 1 irreducible factor: $h = T_n \circ L$	6
1.4	$F_{h,c}$ sporadic cases part I	6
1.5	$F_{h,c}$ sporadic cases part II	7
4.1	Indecomposable genuine Laurent polynomials f where $F_f(X, Y)$ has genus 0 or 1	45
4.2	Ramification types of Laurent polynomials f from Table 4.1	46
5.1	$F_h(X, Y)$ is reducible with a genus 0 or 1 irreducible factor (indecomposable case)	56
5.2	Ramification information of factors of $F_h(X, Y)$ in Table 5.1	56
5.3	Affine group cases	57
5.4	Almost simple group cases	57
6.1	$F_L(X^m, Y^m)$ where L is indecomposable genuine Laurent polynomial	66
7.1	Sporadic cases	72
7.2	$T_n \circ L$ case, ramification in $\mathbb{K}(x)/\mathbb{K}(u)$	82
9.1	$F_{f,c}$ is irreducible of genus at most 1	101
10.1	$cf(Y) = f(\mu(Y))$ and $F_f(X, \mu(Y))$ has an irreducible factor of genus 0 or 1	124
10.2	$P(X) - cP(Y)$ irreducible sporadic cases	126

CHAPTER I

Introduction

1.1 Main theorem

In this thesis we address the following problem:

Problem I.1. *Determine all rational functions $f(X) \in \mathbb{C}(X)$ for which the numerator of $\frac{f(X) - f(Y)}{X - Y}$ has an irreducible factor whose normalization is a curve of genus zero or one.*

In the following sections we will discuss the applications of Problem I.1 to several questions in complex dynamics, number theory, and complex analysis.

We will solve the problem when $f(X)$ is a Laurent polynomial, or in other words, an element of $\mathbb{C}[X, X^{-1}]$. There are three types of nonconstant Laurent polynomials $f(X)$, depending on whether $f^{-1}(\infty)$ is $\{\infty\}$, $\{0\}$, or $\{0, \infty\}$. The first two types consist of $f(X) = g(X)$ and $f(X) = g(1/X)$ where $g(X)$ is a polynomial. In these cases, Problem I.1 was solved recently in [2]. Therefore in this thesis we focus on the third type of Laurent polynomials, which we will call genuine Laurent polynomials.

Definition I.2. A *genuine Laurent polynomial* is an element $f(X)$ in $\mathbb{C}[X, X^{-1}]$ such that $f^{-1}(\infty) = \{0, \infty\}$.

For ease of expression, we define

Definition I.3. For any $f(X) \in \mathbb{C}(X) \setminus \mathbb{C}$, define $F_f(X, Y)$ to be the numerator of $\frac{f(X) - f(Y)}{X - Y}$. Define $F_{f,c}(X, Y)$ to be the numerator of $f(X) - cf(Y)$ for $c \in \mathbb{C}^* \setminus \{1\}$.

Definition I.4. For any $n \geq 2$ define $T_n(X) \in \mathbb{C}[X]$ to be the unique polynomial satisfying $T_n(X + 1/X) = X^n + 1/X^n$.

Our main results are as follows.

Theorem I.5. For a genuine Laurent polynomial $f(X) \in \mathbb{C}[X, X^{-1}]$ and a bivariate polynomial $H(X, Y) \in \mathbb{C}[X, Y]$, the following are equivalent:

- $H(X, Y)$ is an irreducible factor of $F_f(X, Y)$ which defines a curve whose normalization has genus 0 or 1.
- $f = g \circ h \circ \mu$ for some $g \in \mathbb{C}[X]$ and some $\mu(X) = eX^p$ with $e \in \mathbb{C}^*$ and $p \in \{1, -1\}$, where the numerator $\hat{H}(X, Y)$ of $H(\mu^{-1}(X), \mu^{-1}(Y))$ divides $F_h(X, Y)$ and in addition \hat{H} (up to multiplication by a nonzero constant in \mathbb{C}) and h satisfy at least one of the following:

1. $h = \frac{(X+1)^n}{X^k}$, where $n > k$ are coprime positive integers; here $\hat{H}(X, Y) = F_h(X, Y)$ has genus zero.
2. $h = h_1 \circ X^n$ where $n > 1$ and h_1 is a genuine Laurent polynomial, with $\hat{H}(X, Y) = X - cY$ for some $c \neq 1$ such that $c^n = 1$; here $\hat{H}(X, Y) = 0$ has genus 0.
3. $h = T_n \circ L$ where $n \geq 3$ and $\deg(L) \leq 3$ and $(L, \hat{H}(X, Y))$ is listed in Table 1.3.
4. $h = X^n \circ h_1$ where $n \geq 2$ and h_1 is a genuine Laurent polynomial and $F_{h_1,c}(X, Y)$ has an irreducible factor of genus 0 or 1 for some $c \neq 1$ such that $c^n = 1$. This case is solved in Theorem I.6. Here $\hat{H}(X, Y)$ is this irreducible factor.

5. h is a genuine Laurent polynomial of degree at most 10. The pairs $(h, \hat{H}(X, Y))$ are listed in Table 1.1 and Table 1.2.

Theorem I.6. *Pick any $d \in \mathbb{C}^* \setminus \{1\}$, any genuine Laurent polynomial $f(X) \in \mathbb{C}[X, X^{-1}]$, and any $H(X, Y) \in \mathbb{C}[X, Y]$. Then the following are equivalent:*

- $H(X, Y)$ is an irreducible factor of $F_{f,d}(X, Y)$ which defines a curve of genus 0 or 1
- $f = g \circ h \circ \mu$ for some $g \in \mathbb{C}[X]$, some genuine Laurent polynomial $h \in \mathbb{C}[X, X^{-1}]$, some $\mu(X) = eX^p$ with $e \in \mathbb{C}^*$ and $p \in \{-1, 1\}$ and some $c \in \mathbb{C}^*$ for which the pair (h, c) is described in the following list, where the numerator $\hat{H}(X, Y)$ of $H(\mu^{-1}(X), \mu^{-1}(Y))$ divides $F_{h,c}(X, Y)$ and $d \in \langle c \rangle$, and if $m \in \mathbb{Z}$ satisfies $c^m = d$ then all terms of $g(X)$ have degree congruent to m modulo the order of c (where congruence $(\text{mod } \infty)$ is interpreted to mean equality).

1. $h(X) = \frac{(X+1)^n}{X^k}$ where $n > k$ are coprime positive integers. Here $\hat{H}(X, Y) = F_{h,c}(X, Y)$ has genus 0.
2. $h(X) = h_1(X^m)$ where m is any positive integer, $c = -1$, and h_1 is a genuine Laurent polynomial such that $h_1(X) = -h_1(a/X)$ for some $a \in \mathbb{C}^*$. Here $\hat{H}(X, Y) = XY - \beta$ has genus 0 where $\beta^m = a$.
3. $h(X) = h_1(X^m)$ where m is any positive integer, c is a root of unity, and h_1 is a genuine Laurent polynomial satisfying $h_1(aX) = ch_1(X)$ for some $a \in \mathbb{C}^*$ such that $c \in \langle a \rangle$. Here $\hat{H}(X, Y) = X - \beta Y$ has genus 0 where $\beta^m = a$.
4. $h(X) = T_m \circ L$ where $m \geq 2$ and $c = -1$, with $(L, \hat{H}(X, Y))$ being an entry in Table 1.3 for values n and r where $n = 2m$ and r is odd.

5. h has degree at most 8, and $(h, c, \hat{H}(X, Y))$ occurs in Table 1.4 or Table 1.5.

Table 1.1: $F_h(X, Y)$ has a genus 0 or 1 irreducible factor: sporadic cases part I

For case (1) to (24) $\hat{H}(X, Y) = F_h(X, Y)$, which has genus 0 in case (1), (5), (7), (11), (14) and (15), and genus 1 in all the other cases.

(1) $X + 1/X$
(2.1) $(X^3 + 1)/X$
(2.2) $(X^3 + X^2 + a)/X$ where $a \in \mathbb{K} \setminus \{0, 1/27\}$
(3) $(X^2 + aX + 1)^2/X$ where $a^2 \in \mathbb{K} \setminus \{4, -12\}$
(4) $(X - 1)^3(X + a)/X^2$ where $a \in \mathbb{K} \setminus \{0, -1, 7 \pm 4\sqrt{3}\}$
(5) $(X^4 + 4X^3 + 2X - 1/4)/X^2$
(6) $(X^4 - 6X^2 - 3)/X$
(7) $(X - 1)^3(X - 9)/X$
(8.1) $(X - 1)^4(X - 4(i + 1))/X$ where $i^2 = -1$
(8.2) $(X - 1)^4(X - 27/2)/X^2$
(9) $(X - 1)^5(X + (3s + 7)/2)/X^3$ where $s^2 = 5$
(10) $(X - 1)^5(X - (3s + 11)/2)/X^2$ where $s^2 = -15$
(11) $(X - 1)^5(X + 4s - 9)/X^3$ where $s^2 = 5$
(12.1) $(X^3 + 9X + 2)^2/X^3$
(12.2) $(X^3 + 3X^2 + (9w^2 - 1)X + 2w^3 + w^2 - 1/27)^2/X^3$ where $w \in \mathbb{K} \setminus \{0, 1/6, -1/3, 2/3\}$ and $w^2 + 8/21w - 8/63 \neq 0$
(13) $(X - 1)^4(X + (3s - 11)/2)^2/X$ where $s^2 = -15$
(14) $(X^2 + 8X - 2)^3/X^2$
(15) $(X^2 + 10X + 5)^3/X$
(16) $(X^2 + 5X - 5)^3/X$
(17) $(X - 1)^3(X - 16)^2(X - 25)/X$
(18) $(X - 1)^4(X^2 - 6X + 25)/X$
(19.1) $(X + 9)(X^2 + (2w + 7)X + w + 2)^3/X$ where $w \in \mathbb{K}$ has order 3
(19.2) $(X + 25)(X^2 + X - 256/5)^3/X^2$
(19.3) $(X + 1)(X^2 + 5/27X - 1/48)^3/X^3$
(20) $(X^2 + 13X + 49)(X^2 + 5X + 1)^3/X$
(21.1) $(X^2 + 2X + (s + 3)/14)^4/X$ where $s^2 = -7$
(21.2) $(X^2 + X - 27/20)^4/X^3$
(22.1) $(X^3 + 12X^2 + 3(s + 11)X + s + 5)^3/X$ where $s^2 = -2$
(22.2) $(X^3/21 + X^2 + X/4 - 32/3)^3/X^2$
(22.3) $(X^3 + 3/2X^2 + 24/5X - 10)^3/X^4$
(23.1) $(X^2 + X + (i + 1)/32)^5/X^2$ where $i^2 = -1$
(23.2) $(X^2 + 3X - 4)^5/X^4$
(24) $(X + 1/4)^8(X + a(a + 1)^2 - 1/4)^2/X^5$ where $a^4 - 2a^2 + 2 = 0$

For case (25) to (28) $F_h(X, Y)$ is reducible.

(25) $h(X) = (X + 2)(2X^2 - X - 1)^4/X^3$ and $F_h(X, Y)$ has two irreducible factors. The factor $\hat{H}(X, Y) = X^2Y^4 - X^3Y^3 + X(X^3 - 9X/4 + 1/2)Y^2 + X^2Y/2 + 1/4$ has genus 1.
(26) $h(X) = (X + s - 2)(X^3 - X^2 + (s + 1)X/2 + (s + 1)/2)^3/X^5$ where $s^2 = 5$, and $\hat{H}(X, Y)$ has genus 0 and it is either of the two irreducible factors of $F_h(X, Y)$.
(27) $h(X) = (X + (11 - 5s)/2)^2(X^2 + X - 1)^4/X^5$ where $s^2 = 5$, and $\hat{H}(X, Y)$ is either of the two irreducible factors of $F_h(X, Y)$.
(27.1) $\hat{H}(X, Y)$ has genus 0 and it is the degree-30 factor.
(27.2) $\hat{H}(X, Y)$ has genus 1 and it is the degree-60 factor.
(28) $h(X) = (X + 2)^6(X - s - 3)^3(X + 3s + 7)/X^5$ where $s^2 = 5$, and $\hat{H}(X, Y) = X^3Y + (s + 1)X^2Y^2/2 + (s + 5)X^2Y + (2s + 6)X^2 + XY^3 + (s + 5)XY^2 - (2s + 2)XY + (2s + 6)Y^2$ which has genus 1.

Table 1.2: $F_h(X, Y)$ has a genus 0 or 1 irreducible factor: sporadic cases part II

(1) $h = L(X^2)$ where $L = (X - 1)^3(X - 9)/X$. $\hat{H}(X, Y)$ has genus 1 and is either of the two irreducible factors of $F_L(X^2, Y^2)$.

(2) $h = L(X^m)$ where $L(X) = \frac{(X+1)^n}{X^k}$ and

(2.1) $(m, n, k) = (2, 4, 1)$. $\hat{H}(X, Y)$ has genus 1 and is either of the two irreducible factors of $F_L(X^m, Y^m)$.

(2.2) $(m, n, k) = (3, 3, 1)$. $\hat{H}(X, Y)$ is either of the two irreducible factors of $F_L(X^m, Y^m)$: the factor $X^2Y + XY^2 - 1$ has genus 0 and $X^4Y^2 - X^3Y^3 + X^2Y^4 + X^2Y + XY^2 + 1$ has genus 1.

(2.3) $(m, n, k) = (2, 3, 1)$ and $\hat{H}(X, Y) = F_L(X^3, Y^3)$ has genus 0.

(3) $h = P \circ L$ where $P(X) = X^3(X^2 + 5X + 40)$ and L is a deg-2 genuine Laurent polynomial for which $\Lambda(L) = \{\frac{1}{2}(-5 + 3i\sqrt{15}) \text{ or } \frac{1}{2}(-5 - 3i\sqrt{15}), 3\}$. Here $\hat{H}(X, Y)$ is the numerator of $F_P(L(X), L(Y))$ and has genus 1

(4) $h = P \circ L$ where $P = X^r(X - 1)^s$ with $\gcd(r, s) = 1$ and $r + s > 3$, and L is a degree-2 genuine Laurent polynomial. Let $\Lambda(L) = \{\alpha_1, \alpha_2\}$, and let λ_1, λ_2 be the two simple roots of $L(X) - \frac{r^r(-s)^s}{(r+s)^{r+s}}$, then

(4.1) $P = (X - a)(X - b)^3$ where $\{a, b\} = \{0, 1\}$, and $\alpha_1 = \lambda_1, \alpha_2 = \lambda_2$. Here $\hat{H}(X, Y)$ has genus 0 and is either of the two irreducible factors of the numerator of $F_P(L(X), L(Y))$

(4.2) $P = (X - a)(X - b)^3$ where $\{a, b\} = \{0, 1\}$, and $\alpha_1 = a, \alpha_2 = \lambda_1$. Here $\hat{H}(X, Y)$ has genus 1 and is the numerator of $F_P(L(X), L(Y))$

(4.3) $P = (X - a)(X - b)^3$ where $\{a, b\} = \{0, 1\}$ and $L = (X + \frac{1}{16X} + \frac{1}{2})$. Here $\hat{H}(X, Y)$ has genus 1 and is any irreducible factor of the numerator of $F_P(L(X), L(Y))$

(4.4) $P = (X - a)(X - b)^4$ where $\{a, b\} = \{0, 1\}$, $\alpha_1 = a$ and $\alpha_2 = \lambda_1$. Here $\hat{H}(X, Y)$ has genus 1 and is the numerator of $F_P(L(X), L(Y))$

Table 1.3: $F_h(X, Y)$ has a genus 0 or 1 irreducible factor: $h = T_n \circ L$

In this table L is a genuine Laurent polynomial and define $T(X, Y, r)$ to be the numerator of $L(X)^2 + L(Y)^2 - 2L(X)L(Y)\cos(2\pi r/n) - 4\sin^2(2\pi r/n)$ where $0 < r < n/2$.

(1) L has branch points $\{-2, 2, \alpha, \infty\}$ where each has type $(1^1 2^1)$ and $\alpha^2 = 2(1 + \cos(2\pi r/n))$ for some $0 < r < n/2$. Here $\hat{H}(X, Y)$ has genus 1 and is an irreducible factor of $T(X, Y, r)$.

(2) $L(X) = aX + b/X + c$ where $a, b, c \in \mathbb{C}^*$ and let $\{\beta_1, \beta_2\} := \{2\sqrt{ab} + c, -2\sqrt{ab} + c\}$ be the finite branch points of L . Then $\beta_1 = 2$ or -2 . If $\beta_2^2 \neq 2(1 + \cos(2\pi r/n))$ then $\hat{H}(X, Y) = T(X, Y, r)$ has genus 1; otherwise $\hat{H}(X, Y)$ has genus 0 and it is any irreducible factor of $T(X, Y, r)$.

Table 1.4: $F_{h,c}$ sporadic cases part I

(1) $h = X + 1/X$ and $c = -1$ and $\mu(X) = -X$ or $-1/X$

(2) $h = (X^3 + 1)/X$ and $c = w$ ($w^3 = 1$ and $w \neq 1$) and $\mu(X) = w^2X$

(3) $h = (X^2 + 1)^2/X$ and $c = -1$ and $\mu(X) = 1/X$

(4) $h = (X - 1)^3(X + 1)/X^2$ and $c = -1$ and $\mu(X) = 1/X$

(5) $h = (X^4 + 4X^3 + 2X - 1/4)/X^2$ and $c = -1$ and $\mu(X) = -1/(2X)$

(6) $h = (X^4 - 6X^2 - 3)/X$ and $c = -1$ and $\mu(X) = -X$

For case (1) to (6) $\hat{H}(X, Y)$ is the numerator of $F_h(X, \mu(Y))$ and the genus is 0 in case (1) and (5), and is 1 in all other cases.

(7) $h = P \circ L$ where $P = X^4 + 4X^3 + 3(a + 3)X^2$ with $a^2 = 3$, and $c = -1$, and $\deg(L) = 2$. Let λ be a nonzero finite branch point of P then the two simple roots of $P(X) - \lambda$ are all the finite branch points of L . Here $\hat{H}(X, Y)$ has genus 1 and it is either of the two irreducible factors of $F_{h,-1}(X, Y)$.

(8) $h = L(X^2)$ where L is any genuine Laurent polynomial of degree 2 and $c \in \mathbb{C}^* \setminus \{1\}$. Here $\hat{H}(X, Y)$ has genus 0 or 1 and it is any irreducible factor of $F_{L,c}(X^2, Y^2)$.

Table 1.5: $F_{h,c}$ sporadic cases part II

item	n	k	\mathfrak{g}	order of c	reduced sequences ramification types
(1)	2	1	0	≥ 3	$(1^2) \rightarrow (2^1) \rightarrow (2^1) \rightarrow (1^2)$
(2)	2	1	1	≥ 2 ≥ 5	$(1^2) \leftrightarrow (2^1), (1^2) \leftrightarrow (2^1)$ or $(1^2) \rightarrow (2^1) \rightarrow (1^2) \rightarrow (2^1) \rightarrow (1^2)$
(3)	3	1, 2	0	4	$(1^1 2^1) \rightarrow (1^1 2^1) \rightarrow (1^1 2^1) \rightarrow (1^1 2^1)$
(4)	3	1, 2	1	≥ 5 ≥ 4 2	$(1^3) \rightarrow (1^1 2^1) \rightarrow (1^1 2^1) \rightarrow (1^1 2^1) \rightarrow (1^3)$ or $(1^3) \rightarrow (1^1 2^1) \rightarrow (1^1 2^1) \rightarrow (1^3), (1^1 2^1)$ or $(1^3) \leftrightarrow (1^1 2^1), (1^1 2^1) \leftrightarrow (1^1 2^1)$
(5)	4	1, 3	0	2	$(1^2 2^1) \leftrightarrow (1^2 2^1), (2^2)$
(6)	4	1, 3	1	≥ 2	$P_1 = P_2 = (1^2 2^1), P_3 = (2^2)$, any matching pattern
(7)	4	1, 3	1	≥ 4	$(1^4) \rightarrow (1^2 2^1) \rightarrow (1^2 2^1) \rightarrow (1^4), (2^2)$
(8)	4	1, 3	1	2	$(1^2 2^1) \leftrightarrow (1^2 2^1), (1^1 3^1)$
(9)	4	2	0	2	$(1^2 2^1) \leftrightarrow (1^2 2^1), (1^1 3^1)$
(10)	4	2	0	≥ 4	$(1^2 2^1) \rightarrow (1^2 2^1) \rightarrow (2^2) \rightarrow (1^2 2^1)$
(11)	4	2	1	2	$(1^2 2^1) \leftrightarrow (4^1)$
(12)	4	2	1	2	$(1^1 3^1) \leftrightarrow (2^2)$
(13)	4	2	1	≥ 2	four $(1^2 2^1)$, any matching pattern
(14)	4	2	1	2 ≥ 5	$(1^4) \leftrightarrow (1^2 2^1), (1^2 2^1) \leftrightarrow (2^2)$ or $(1^4) \rightarrow (1^2 2^1) \rightarrow (2^2) \rightarrow (1^2 2^1) \rightarrow (1^4)$
(15)	4	2	1	≥ 4	$(1^4) \rightarrow (1^2 2^1) \rightarrow (1^2 2^1) \rightarrow (1^4), (1^1 3^1)$
(16)	6	1, 5	1	2	$(3^2), (1^4 2^1) \leftrightarrow (1^4 2^1)$
(17)	6	2, 4	0	2	$(3^2), (1^4 2^1) \leftrightarrow (1^4 2^1)$
(18)	6	2, 4	1	2	$(1^4 2^1), (2^3) \leftrightarrow (1^2 2^2)$
(19)	6	3	0	2	$(2^1 4^1), (1^4 2^1) \leftrightarrow (1^4 2^1)$
(20)	6	3	1	2	$(1^1 5^1), (1^4 2^1) \leftrightarrow (1^4 2^1)$
(21)	6	3	1	4	$(1^4 2^1) \rightarrow (1^4 2^1) \rightarrow (1^4 2^1) \rightarrow (1^4 2^1), (2^3)$
(22)	6	3	1	≥ 2	three $(1^2 2^2)$, any matching pattern
(23)	6	3	1	≥ 4	$(1^n) \rightarrow (1^{n-2} 2^1) \rightarrow (1^{n-2} 2^1) \rightarrow (1^n), (2^1 4^1)$

In this table $h(X)$ is a genuine Laurent polynomial of degree n with denominator X^k and $h(X)$ satisfies the reduced sequence condition. For the definition and motivation of reduced sequence we refer the reader to Definition IX.3. Here $\tilde{H}(X, Y) = F_{h,c}(X, Y)$ with genus \mathfrak{g} as described in the table.

1.2 Application I: Complex functional equations

The functional equation

$$(1.1) \quad f \circ P = f \circ Q$$

plays an important role in many contexts, where f is a complex rational function and P, Q are distinct nonconstant meromorphic functions on the complex plane. Picard [15] showed that an irreducible algebraic curve admits a parametrization by meromorphic functions if and only if it has genus 0 or 1. Therefore, for a given

nonconstant $f(X) \in \mathbb{C}(X)$, Equation (1.1) has a solution if and only if $F_f(X, Y)$ has a component of genus zero or one. Thus Theorem I.5 implies the following result.

Theorem I.7. *For any genuine Laurent polynomial $f(X) \in \mathbb{C}[X, X^{-1}]$, the equation $f \circ P = f \circ Q$ has a solution in distinct nonconstant meromorphic functions P, Q on \mathbb{C} if and only if f is one of the Laurent polynomials described in Theorem I.5.*

In addition to determining the Laurent polynomial $f(X)$ for which Equation (1.1) has a solution, we can also use our results to describe all possibilities for the meromorphic functions P and Q . This is because we determine all irreducible components of $F_f(X, Y) = 0$ having genus 0 or 1, so that with some work we can determine a “minimal” parametrization of each such component via rational or elliptic functions, and then use the known description [2] of how all meromorphic parametrizations can be obtained from a minimal parametrization. We note that an analogue of Theorem I.5 in the case of polynomials was proved in [2] (building on earlier work from [1]), and yields a solution of Equation (1.1) when $f(X)$ is a polynomial.

The classification result in this thesis has several applications in complex dynamics and complex analysis, as follows:

1. Lyubich and Minsky [9] used hyperbolic orbifold 3-laminations to study backward orbits of a rational function, as well as other dynamical questions. In item 10 on page 83 they asked several questions about solutions to Equation (1.1), as such solutions play an important role in their theory. Specifically, they asked if all solutions to the Equation (1.1) have a specific form. Theorem I.7 provides many classes of solutions to Equation (1.1) and gives a negative answer to their most ambitious question.
2. Nevanlinna’s Five-Values Theorem ([14], [6, Theorem 2.6]) says that a noncon-

stant meromorphic function is completely determined by its preimages at five complex numbers. More precisely, if P, Q are nonconstant meromorphic functions such that $P^{-1}(a_i) = Q^{-1}(a_i)$ for each of five distinct complex numbers a_i , then $P = Q$. This result inspired a great deal of subsequent work, with the ultimate goal being to move from preimages of points to preimages of finite sets. Many authors studied the analogous question: when can distinct meromorphic functions P, Q satisfy $P^{-1}(S_i) = Q^{-1}(S_i)$ for several finite subsets $S_i \subset \mathbb{C}$? If the finite sets S_i satisfy certain conditions, then one can use Nevanlinna's second main theorem to show that there exists a rational function f such that $f \circ P = f \circ Q$. In the opposite direction, if $f \circ P = f \circ Q$, then for any complex number b , the set $f^{-1}(b)$ has the same preimage under P as it does under Q , in other words, $f^{-1}(b)$ plays the role of the finite sets S_i .

Our Theorem I.7 provides several new classes of meromorphic functions P and Q for which there are infinitely many finite sets S_i such that $P^{-1}(S_i) = Q^{-1}(S_i)$. In addition, Theorem I.7 can be combined with results from Nevanlinna theory in order to classify all P, Q with this property if in addition the sets S_i satisfy certain further conditions.

3. In complex dynamics, two important invariants of a rational function are its Julia set and its measure of maximal entropy. Many authors have studied the extent to which these invariants determine a rational function, or in other words, when two distinct rational functions can have the same Julia set or the same measure of maximal entropy. In the work of Levin-Przytycki [7, 8] and Ye [19], the authors reduce these two questions to the solution of Equation (1.1), where f, P, Q are all rational functions. The work of [2] gives the complete list of solutions when f is a polynomial, and this thesis gives the complete list when

f is a Laurent polynomial.

1.3 Application II: Diophantine equations and near-injectivity of rational functions

Theorem I.5 has the following number-theoretic consequence.

Theorem I.8. *Let $f(X) \in \bar{\mathbb{Q}}[X, X^{-1}]$ be a genuine Laurent polynomial. Then f is listed in Theorem I.5 if and only if there is a number field K which contains infinitely many elements c for which the equation $f(X) = c$ has at least two solutions in K .*

Proof. We first prove the “if” direction of the theorem. The condition on f says that there is number field K for which the equation the equation $f(X) = f(Y)$ has infinitely many solutions in $K \times K$ which do not satisfy $X = Y$ (since only finitely many solutions satisfy $X = Y$). It follows that $F_f(X, Y) = 0$ has infinitely many K -rational points, so also some irreducible component of $F_f(X, Y)$ has infinitely many K -rational points. Such a component must be geometrically irreducible, and hence by Faltings’ theorem [4] must have genus zero or one, so that f is described in Theorem I.5.

We then prove the “only if” direction of the theorem. Note that any smooth projective geometrically irreducible curve of genus 0 or 1 has infinitely many points over some number field, more precisely for genus 0, the number field could be any number field over which the curve has one point; and for genus 1, the number field could be any number field over which the curve has two points whose difference in the Jacobian has infinite order. If a genuine Laurent polynomial f satisfies that $F_f(X, Y)$ has a factor whose normalization has genus zero or one, then $F_f(X, Y)$ has infinitely many K -rational points for some number field K , and this implies that there are infinitely many elements $c \in K$ for which the equation $f(X) = c$ has at

least two solutions in K . □

The version of Theorem I.8 when f is any polynomial is proved by Carney, Hortsch and Zieve in [2]. Using the theorem, they proved the following unexpected result:

Theorem I.9 (Carney–Hortsch–Zieve [2]). *For any $f(X) \in \mathbb{Q}[X]$, the polynomial map $\mathbb{Q} \rightarrow \mathbb{Q}$ defined by $c \mapsto f(c)$ is at most 6-to-1 over all but finitely many values.*

They also proved the following more general result for number fields.

Theorem I.10 (Carney–Hortsch–Zieve [2]). *Let K be a number field, and let N be the largest positive integer for which some primitive N -th root of unity ξ satisfies $\xi + \xi^{-1} \in K$. Then, for any $f(X) \in K[X]$, the function $K \rightarrow K$ defined by $c \mapsto f(c)$ is $(\leq N)$ -to-1 over all but finitely many values. Moreover, there are polynomials $f(X) \in K[X]$ which induce functions $K \rightarrow K$ that are N -to-1 over infinitely many values.*

In the very near future we hope to prove analogues of these results for Laurent polynomials, using Theorem I.8 and its polynomial analogue from [2]. We will explain the method at the end of this section. If there is an analogue of Theorem I.10 for Laurent polynomials, then this would be evidence in support of the following conjectures.

Conjecture I.11 (Carney–Hortsch–Zieve [2]). *Let K be a number field, and let $f(X) \in K(X)$ be any rational function. Then the map $K \rightarrow K$ defined by $c \mapsto f(c)$ is at most N -to-1 over all but finitely many values, where N is a constant depending only on $[K : \mathbb{Q}]$.*

Conjecture I.12 (Carney–Hortsch–Zieve [2]). *For any positive integers d and D , there is an integer $C(d, D)$ with the following property: for any degree- d number field*

K , and any morphism $f : V_1 \rightarrow V_2$ between D -dimensional varieties defined over K , the induced map $f : V_1(K) \rightarrow V_2(K)$ is $(\leq C(d, D))$ -to-1 over all elements of $V_2(K)$ which are not contained in some proper Zariski-closed subset of $V_2(\bar{K})$.

These conjectures are related to Mazur and Merel's results about rational torsion on elliptic curves. Their result will be a direct consequence of Conjecture I.11.

Theorem I.13 (Mazur [10], Merel [11]). *For any positive integer d , there is an integer $C(d)$ with the following property: for any degree- d number field K , every elliptic curve E over K has at most $C(d)$ torsion points defined over K . Moreover, one may take $C(1)$ to be 16.*

In just a few lines, one can deduce Theorem I.13 from the special case of Conjecture I.12 in which V_1 and V_2 are genus-1 curves, and conversely. Moreover, it is shown in [2] that Theorem I.13 also follows quickly from Conjecture I.11.

We now outline the envisioned strategy for proving a the Laurent polynomial analogue of Theorem I.10.

The first step is to use Faltings' theorem to translate the arithmetic question into geometry. In particular, if a Laurent polynomial $f(X) \in K(X) \setminus K$ induces a function $K \rightarrow K$ which is $(\geq r)$ -to-1 over infinitely many values, then the algebraic set V defined by $f(X_1) = f(X_2) = \dots = f(X_r)$ contains infinitely many K -rational points with distinct coordinates. Since every component is a curve, by Faltings' theorem at least one component has genus 0 or 1. Theorem I.8 and its polynomial analogue in [2] solve the problem when $r = 2$, and yield the set of Laurent polynomials. We will then continue the following process inductively on r . Suppose we have the list of Laurent polynomials for r , then for $r + 1$, we can relate each component of $f(X_1) = f(X_2) = \dots = f(X_{r+1})$ with a component of $f(X_1) = f(X_2) = \dots = f(X_r)$,

and the component from $r + 1$ is expected to have a larger genus, unless some specific ramification constraints are satisfied. Since we only want components of genus zero or one, from r to $r + 1$, the set of Laurent polynomials satisfying the genus condition shrinks. Let r be the smallest value for which this set of Laurent polynomials is empty; then the Laurent polynomial analogue of Theorem I.10 will be true for $N = r - 1$.

CHAPTER II

Proof of Theorem I.5 and Theorem I.6

In this chapter we prove Theorem I.5 and Theorem I.6, using results whose proofs appear in subsequent chapters. We begin with an outline of the thesis.

2.1 Notation and terminology

Let \mathbb{K} be an algebraically closed field of characteristic 0. We will work over such a field \mathbb{K} throughout this thesis. We use capital letters X, Y, U, V for rational function variables, and lower case letters x, y, u, v, t for elements which are transcendental over \mathbb{K} (but which might be algebraically dependent over \mathbb{K}).

For any $f(X) \in \mathbb{K}(X)$ we define $F_f(X, Y)$ to be the numerator of $\frac{f(X)-f(Y)}{X-Y}$ and define $F_{f,c}(X, Y)$ to be the numerator of $f(X) - cf(Y)$ for any $c \in \mathbb{K}^* \setminus \{1\}$.

The goal of this thesis is to classify the genuine Laurent polynomials $f(X) \in \mathbb{K}[X, X^{-1}]$ for which $F_f(X, Y)$ has an irreducible factor of genus zero or one. Here by “genus” we mean the genus of the normalization of the irreducible factor. Since the polynomial case is already solved in [2], we will assume f is a genuine Laurent polynomial in this thesis.

We say that a rational function $f(X) \in \mathbb{K}(X)$ of degree at least 2 is *indecomposable* if it cannot be written as the composition of two lower-degree rational functions in $\mathbb{K}(X)$; otherwise, we say that $f(X)$ is *decomposable*.

2.2 Outline of the thesis

In section 2.3 we will show how the results proved in subsequent chapters can be combined to prove Theorem I.5 and Theorem I.6. The bulk of the work in this thesis occurs in the subsequent chapters, where Theorem I.5 and Theorem I.6 are proved when $f(X)$ is restricted to certain classes of Laurent polynomials. We begin in Chapter III with preliminary results and background material. In particular, we show in Lemma III.3 that any genuine Laurent polynomial has a decomposition $f = f_1 \circ f_2 \circ f_3$, where $P := f_1$ is a polynomial, $L := f_2$ is an indecomposable genuine Laurent polynomial, and $f_3 = X^n$ for some positive integer n . We will use different types of arguments depending on the nature of this decomposition of f .

The following chapters solve the classification of genuine Laurent polynomials f for which $F_f(X, Y)$ has an irreducible factor of genus 0 or 1.

- In Chapter IV we classify indecomposable genuine Laurent polynomials $f = L$ for which $F_f(X, Y)$ is irreducible with genus 0 or 1. The classification is Theorem IV.1.
- In Chapter V we classify indecomposable genuine Laurent polynomials $f = L$ for which $F_f(X, Y)$ is reducible with an irreducible factor of genus 0 or 1. The classification is Theorem V.1.
- In Chapter VI we solve the decomposable case that $f = L \circ X^n$ (where $n > 1$). The classification is Theorem VI.1.
- In Chapter VII we solve the decomposable case that $f = P \circ L$. The classification is Theorem VII.1.
- In Chapter VIII we solve the decomposable case that $f = P \circ L \circ X^n$ (where

$n > 1$). The classification is Theorem VIII.1.

Some cases in Theorem VII.1 and Theorem VIII.1 are reduced to the problem of classifying genuine Laurent polynomials f and $c \in \mathbb{K}^* \setminus \{1\}$ for which $F_{f,c}(X, Y)$ has an irreducible factor of genus 0 or 1, and we solve this problem in Chapter IX and Chapter X. The following is the outline of Chapter IX and Chapter X.

- In Chapter IX we solve the case when $F_{f,c}(X, Y)$ is irreducible with genus 0 or 1.
 1. The classification is Theorem IX.6.
- In Chapter X we solve the case when $F_{f,c}(X, Y)$ is reducible with an irreducible factor of genus 0 or 1. Each section of Chapter X solves the problem for one type of f .
 1. We solve the case when $f = L$ is indecomposable. The classification is Proposition X.3 and Proposition X.4.
 2. We solve the case when $f = P \circ L$. The classification is Proposition X.13.
 3. We solve the case when $f = L \circ X^n$ or $f = P \circ L \circ X^n$ (where $n > 1$). The classification is Proposition X.14 and Proposition X.15.

2.3 Proof of Theorem I.5

Pick an irreducible factor $H(X, Y)$ of $F_f(X, Y)$ such that $H(X, Y) = 0$ has genus 0 or 1. Let x be transcendental over \mathbb{K} , and let y satisfy $H(x, y) = 0$. Then let $t := f(x) = f(y)$, and let h be a genuine Laurent polynomial which has the minimal degree such that $f = g \circ h \circ \mu$ for some polynomial g , and $\mu(X) = eX^p$ with some $e \in \mathbb{K}^*$ and $p \in \{-1, 1\}$, and $h(\mu(x)) = h(\mu(y))$. Now $H(X, Y)$ is an irreducible factor of $F_{h \circ \mu}(X, Y)$. By Remark III.26 there is a genus-preserving bijection between the irreducible factors $H(X, Y)$ of $F_{h \circ \mu}(X, Y)$ and the irreducible factors $\hat{H}(X, Y)$

of $F_h(X, Y)$ up to multiplication by some nonzero element in \mathbb{K}^* , where $\hat{H}(X, Y)$ is the numerator of $H(\mu^{-1}(X), \mu^{-1}(Y))$. Therefore it suffices to solve the problem in case $\mu(X) = X$, which we will assume in what follows.

In the following proof we assume that $f = h$.

Put $r := f_3(x) = x^n$, $s := f_3(y) = y^n$, $u := f_2(r)$, $v := f_2(s)$, and $t := f_1(u)$. Note that $t = f(x) = f(y) = f_1(v)$ and that $[\mathbb{K}(x) : \mathbb{K}(r)] = n = [\mathbb{K}(y) : \mathbb{K}(s)]$ and $[\mathbb{K}(r) : \mathbb{K}(u)] = \deg(f_2) = [\mathbb{K}(s) : \mathbb{K}(v)]$ and $[\mathbb{K}(u) : \mathbb{K}(t)] = \deg(f_1) = [\mathbb{K}(v) : \mathbb{K}(t)]$. By Riemann–Hurwitz, every subfield of $\mathbb{K}(x, y)$ which properly contains \mathbb{K} will have genus at most equal to the genus of $\mathbb{K}(x, y)$; the latter genus equals the genus of $\hat{H}(X, Y)$, and hence is 0 or 1.

There are three cases we need to consider.

1. $\mathbb{K}(r) = \mathbb{K}(s)$.
2. $\mathbb{K}(r) \neq \mathbb{K}(s)$, but $\mathbb{K}(u) = \mathbb{K}(v)$.
3. $\mathbb{K}(u) \neq \mathbb{K}(v)$.

2.3.1 Case 1: $\mathbb{K}(r) = \mathbb{K}(s)$

In this case there must be a linear fractional $\mu(X) \in \mathbb{K}(X)$ such that $s = \mu(r)$, so $f_1 \circ f_2 \circ \mu(r) = f_1 \circ f_2(r)$. Since r is transcendental over \mathbb{K} , this means $f_1 \circ f_2 \circ \mu(X) = f_1 \circ f_2(X)$. Now consider the preimage of ∞ on the both sides: on the right it is $\{0, \infty\}$, and on the left it is $\{\mu^{-1}(0), \mu^{-1}(\infty)\}$. Since μ preserves $\{0, \infty\}$, $\mu(X)$ must be either cX or c/X for some $c \in \mathbb{K}^*$. Since $f_3 = X^n$, this implies that either $y = ax$ or $y = a/x$, where $a^n = c$.

- (1) If $y = ax$ then $f(ax) = f(x)$, so that $f(x)$ is in the subfield of $\mathbb{K}(x)$ fixed by the automorphism $x \mapsto ax$. Denoting this order by m , we see that a is a primitive m -th root of unity, and the fixed field of $x \mapsto ax$ is $\mathbb{K}(x^m)$. Therefore

$f = g \circ X^m$ for some genuine Laurent polynomial g , and $\hat{H}(X, Y) = X - aY$ which has genus 0.

- (2) If $y = a/x$ then $f(a/x) = f(x)$, so that $f(x)$ is in the subfield of $\mathbb{K}(x)$ fixed by the automorphism $x \mapsto a/x$, namely the field $\mathbb{K}(x+a/x)$. Hence $f(X) = g(X+a/X)$ for some rational function g , but since $f^{-1}(\infty) = \{0, \infty\} = (X + a/X)^{-1}(\infty)$, it follows that $g^{-1}(\infty) = \{\infty\}$, whence g is a polynomial. Then the minimality of f implies that g is a constant which can be chosen to be 1, so $f = X + a/X$. Now since $f = (\sqrt{a}X) \circ (X + 1/X) \circ (X/\sqrt{a})$ we can choose $f = X + 1/X$. Thus in this case: $f = X + 1/X$ where $\hat{H}(X, Y) = XY - 1$.

2.3.2 Case 2: $\mathbb{K}(r) \neq \mathbb{K}(s)$, but $\mathbb{K}(u) = \mathbb{K}(v)$

Since $\mathbb{K}(u) = \mathbb{K}(v)$, we have $v = \mu(u)$ for some linear fractional $\mu \in \mathbb{K}(X)$, so $f_1(\mu(u)) = f(y) = f(x) = f_1(u)$. Since f_1 is a polynomial, this equality shows $f^{-1}(\infty) = \{\infty\} = \mu^{-1}(\infty)$, so μ must be a linear polynomial. Likewise, μ permutes $f_1^{-1}(S)$ for any finite subset S of \mathbb{K} , so by taking S large enough we see that μ permutes a finite set of size at least 3, which forces μ to have finite order. Let c be the unique fixed point of μ in \mathbb{K} , so that $(X - c) \circ \mu \circ (X + c)$ has finite order and fixed point 0, and hence equals aX for some root of unity a , so $\mu = (X + c) \circ aX \circ (X - c)$.

If $a \neq 1$, put $F_1 := f_1 \circ (X + c)$ and $F_2 := (X - c) \circ f_2$. Note that $f_1 \circ (X + c) \circ aX \circ (X - c) = f_1$, so $F_1(aX) = F_1(X)$, whence $F_1(X) = g(X^m)$ where m is the order of a . Moreover, $F_1 \circ F_2 = f_1 \circ f_2$. Note that F_1 and F_2 satisfy all the properties required of f_1 and f_2 , namely that $\mathbb{K}(F_2(r)) = \mathbb{K}(F_2(s))$ and F_2 is a genuine Laurent polynomial which is indecomposable, and F_1 is a polynomial. Therefore we lose no generality by replacing f_1 and f_2 by F_1 and F_2 , while also replacing u and v by $u - c$ and $v - c$ (note that these replacements do not change f , x , y , or H). After these

replacements, we may assume that either

(2a) $u = v$ or

(2b) $v = au$ where a is a primitive m -th root of unity for some $m > 1$, and $F_1(X) = g(X^m)$ for some polynomial g . The minimality of f implies that g is a nonzero constant so we can assume $F_1(X) = X^m$.

Case 2a: $u = v$

The minimality of f implies f_1 is a nonzero constant so we can assume $f = f_2 \circ f_3 = L \circ X^n$. In this case r, s are distinct transcendentals over \mathbb{K} such that $f_2(r) = f_2(s)$, and $\mathbb{K}(r, s)$ has genus 0 or 1. Now we have the function field tower in Figure 2.1.

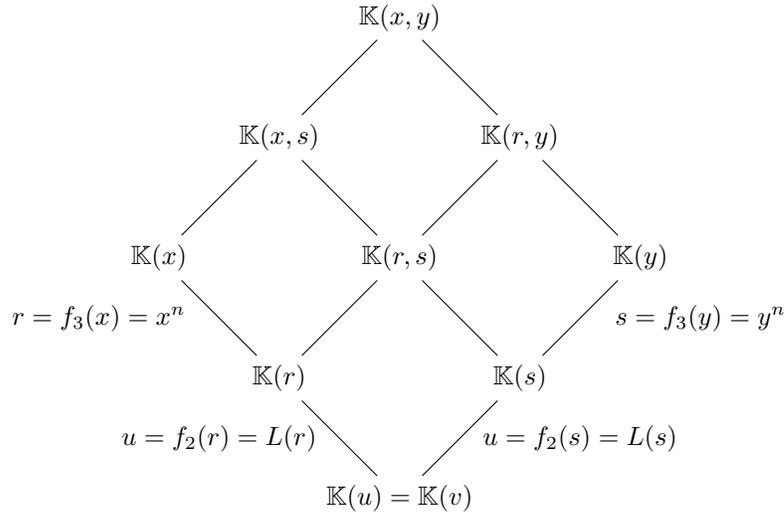


Figure 2.1: Tower of function fields

Here $\mathbb{K}(r, s)$ is the function field of some irreducible factor of $F_L(X, Y)$, where all possibilities for L are classified in Theorem IV.1 (when $F_L(X, Y)$ is irreducible) and Theorem V.1 (when $F_L(X, Y)$ is reducible). If $n > 1$, we also require $\mathbb{K}(x, y)$ to have genus zero or one. For each such L , the possibilities for n are classified in Theorem VI.1.

Case 2b: $v = au$ for some primitive m -th root of unity a and $f_1(X) = X^m$ where $a \neq 1$ and $m > 1$

This case $\hat{H}(X, Y)$ is an irreducible factor of $F_{h_1, a}(X, Y)$ where $h_1 = f_2 \circ f_3 = L \circ X^n$. This is case (4) of the theorem.

2.3.3 Case 3: $\mathbb{K}(u) \neq \mathbb{K}(v)$

In this case, $\mathbb{K}(u, v)$ is the function field of an irreducible factor $H_1(X, Y)$ of $F_{f_1}(X, Y)$ and $\mathbb{K}(u, v)$ has genus zero or one. If $f = f_1 \circ f_2 = P \circ L$, then $\hat{H}(X, Y)$ is an irreducible factor of $F_P(L(X), L(Y))$ and this is solved in Theorem VII.1. Case (3) in Theorem VII.1 is the case (3) in this theorem; case (1) and (2) in Theorem VII.1 are cases (3) and (4) in Table 1.2. Case (4) in Theorem VII.1 is a special case of case (4) in this theorem.

If $f_3 := X^n$ with $n > 1$, then $f = P \circ L \circ X^n$ and $\frac{f(X)-f(Y)}{X-Y} = \frac{P \circ L(X^n) - P \circ L(Y^n)}{X^n - Y^n} \frac{X^n - Y^n}{X - Y}$, so $\hat{H}(X, Y)$ is an irreducible factor of $F_{P \circ L}(X^n, Y^n)$ and this is solved in Proposition VIII.1. The case in Proposition VIII.1 is case (4) in this theorem.

2.4 Proof of Theorem I.6

There exists a pair (h, c) where h is a genuine Laurent polynomial of minimal degree such that $c \in \mathbb{K}^* \setminus \{1\}$ and $f = g \circ h$ for some polynomial g and $h(X) - ch(Y)$ divides $f(X) - df(Y)$. First we show that $d \in \langle c \rangle$ and for any $m \in \mathbb{Z}$ such that $c^m = d$, all terms of $g(X)$ have degree congruent to m (mod the order of c). From the congruences $h(X) \equiv ch(Y) \pmod{H(X, Y)}$ and $g(h(x)) = dg(h(Y)) \pmod{H(X, Y)}$, we find that $dg(h(Y)) \equiv g(h(X)) \equiv g(ch(Y)) \pmod{H(X, Y)}$. It follows that $dg(h(Y)) = g(ch(Y))$, since otherwise $H(X, Y)$ would divide a nonzero polynomial in $\mathbb{K}[Y]$, so that $H(X, Y)$ would be an element of $\mathbb{K}[Y]$, contradicting the fact that $H(X, Y)$ is an irreducible factor of $h(X) - ch(Y)$. Next the equality

$dg(h(Y)) = g(ch(Y))$ implies that $dg(Y) = g(cY)$, so if $g(Y)$ has a term of degree j then $d = c^j$. Therefore indeed $d \in \langle c \rangle$, and if $d = c^m$ then all terms of $g(X)$ have degree congruent to $m \pmod{\text{the order of } c}$.

Now since $H(X, Y)$ is an irreducible factor of $F_{h,c}(X, Y)$ then we only need to work on the pair (h, c) . In fact for the set of pairs $(f \circ \mu^{-1}, d)$ where $\mu(X) = eX^p$ with $e \in \mathbb{K}^*$ and $p \in \{-1, 1\}$, we only need to work on the pair (h, c) since $(h \circ \mu^{-1}, c)$ is a minimal pair of $(f \circ \mu^{-1}, d)$, and any $H(X, Y)$ of $F_{h,c}(X, Y)$ will yield an irreducible factor $\hat{H}(X, Y)$ of $F_{h \circ \mu^{-1}, c}(X, Y)$ of genus at most 1 where $\hat{H}(X, Y)$ is the numerator of $H(\mu^{-1}(X), \mu^{-1}(Y))$.

The case when $F_{h,c}(X, Y)$ is irreducible with genus 0 or 1 is solved in Theorem IX.6. When $F_{h,c}(X, Y)$ is decomposable, we consider the four types of h . The case h is indecomposable is solved in Proposition X.3 and Proposition X.4; the case when $h = P \circ L$ is solved in Proposition X.13; the case when $h = L \circ X^n$ or $h = P \circ L \circ X^n$ (where $n > 1$) is solved in Proposition X.14 and Proposition X.15. This concludes the proof.

CHAPTER III

Preliminaries

In this chapter we present the notation, terminology, and background results that will be used in this thesis. We firstly define what indecomposable and decomposable rational functions are, and state how genuine Laurent polynomials decompose. After that we define curves, function fields, places, and monodromy groups, and how to build function field towers. Then we give the Riemann–Hurwitz formula to compute the genus, and list some tools to analyze the degree of the composite of two extensions of a function field. At the end we give the factorizations of some special polynomials, and some inequalities related to the genus formula.

Throughout this thesis, we work over an arbitrary algebraically closed field \mathbb{K} of characteristic zero, instead of the complex field \mathbb{C} . We use capital letters X, Y, U, V for rational function variables, and lower case letters x, y, u, v, t for elements which are transcendental over \mathbb{K} (but which might be algebraically dependent over \mathbb{K}).

The irreducible factors of the numerator of a rational function we come across in this thesis always define irreducible algebraic curves, and by the *genus* of a factor, we always mean the genus of the normalization of the curve defined by the irreducible factor.

3.1 Decomposability

Definition III.1. We say that a rational function $f(X) \in \mathbb{K}(X)$ of degree at least 2 is *indecomposable* if it cannot be written as the composition of two lower-degree rational functions in $\mathbb{K}(X)$; otherwise, we say that $f(X)$ is *decomposable*.

Lemma III.2. *If $f_1, f_2 \in \mathbb{K}(X)$ are nonconstant rational functions such that $f_1 \circ f_2 \in \mathbb{K}[X]$, then there is a linear fractional $\mu \in \mathbb{K}(X)$ so that $f_1 \circ \mu \in \mathbb{K}[X]$ and $\mu^{-1} \circ f_2 \in \mathbb{K}[X]$.*

If $g_1, g_2 \in \mathbb{K}(X)$ are nonconstant rational functions such that $g_1 \circ g_2$ is a genuine Laurent polynomial in $\mathbb{K}[X, X^{-1}]$, then there is a linear fractional $\mu \in \mathbb{K}(X)$ so that one of the following holds

- (1) $g_1 \circ \mu \in \mathbb{K}[X]$ and $\mu^{-1} \circ g_2$ is a genuine Laurent polynomial in $\mathbb{K}[X, X^{-1}]$
- (2) $g_1 \circ \mu$ is a genuine Laurent polynomial in $\mathbb{K}[X, X^{-1}]$ and $\mu^{-1} \circ g_2 = X^n$ for some $n > 0$

Proof. For the first half, since $f_1 \circ f_2$ is a polynomial which is totally ramified at ∞ , we have $f_1^{-1}(\infty) = a$ and $f_2^{-1}(a) = \infty$ for some $a \in \mathbb{K} \cup \{\infty\}$. Let $\mu \in \mathbb{K}(X)$ be a linear fractional such that $\mu(\infty) = a$, then $f_1 \circ \mu$ and $\mu^{-1} \circ f_2$ are both totally ramified at ∞ with preimage ∞ , so they are both polynomials.

For the second half, $g_2^{-1} \circ g_1^{-1}(\infty) = (g_1 \circ g_2)^{-1}(\infty) = \{0, \infty\}$. Then there are two cases:

- (1) $g_1^{-1}(\infty)$ has one element. Let μ be a linear fractional such that μ^{-1} moves that element to ∞ , then $(g_1 \circ \mu)^{-1}(\infty) = \infty$, so $g_1 \circ \mu$ is a polynomial. Now $(\mu^{-1} \circ g_2)^{-1}(\infty) = \{0, \infty\}$, so $\mu^{-1} \circ g_2$ is a genuine Laurent polynomial.
- (2) $g_1^{-1}(\infty)$ has two elements. Let μ be a linear fractional such that μ^{-1} moves the

two elements to $\{0, \infty\}$, then $(g_1 \circ \mu)^{-1}(\infty) = \{0, \infty\}$, so $g_1 \circ \mu$ is a genuine Laurent polynomial. Now $(\mu^{-1} \circ g_2)^{-1}(\{0, \infty\}) = \{0, \infty\}$, so $\mu^{-1} \circ g_2 = X^n$ for some nonzero integer n . We can assume $n > 0$ since otherwise we can replace μ with $\mu \circ 1/X$ and then $(\mu \circ 1/X)^{-1} \circ g_2 = X^{-n}$ with the exponent $-n > 0$.

This concludes the proof. \square

Lemma III.3. *Any genuine Laurent polynomial $f \in \mathbb{K}[X, X^{-1}]$ can be written as $f = f_1 \circ f_2 \circ f_3$ where $f_1 \in \mathbb{K}[X]$ is a polynomial, $f_2 \in \mathbb{K}[X, X^{-1}]$ is an indecomposable genuine Laurent polynomial, and $f_3 = X^n$ for some positive integer n .*

Proof. If f is indecomposable, then take $f_1 = X$, $f_2 = f$ and $n = 1$. If f is decomposable, suppose $f = g \circ h$ where g and h are both rational functions of degree at least 2. Since $f^{-1}(\infty) = \{0, \infty\}$, $g^{-1}(\infty)$ could have one point or two points. In either case, we can find an appropriate linear fractional $\mu(X) \in \mathbb{K}(X)$ such that $(g \circ \mu)^{-1}(\infty) = \{\infty\}$ in the first case, and $\{0, \infty\}$ in the second case. We will then replace g, h with $g \circ \mu$ and $\mu^{-1} \circ h$. In the first case, g is a polynomial and since $h^{-1}\{\infty\} = \{0, \infty\}$, h is a genuine Laurent polynomial. In the second case, g is a genuine Laurent polynomial, and since $h^{-1}\{0, \infty\} = \{0, \infty\}$, we have $h = aX^n$ where $n \neq 0$ is an integer, and we can assume $n > 0$ since otherwise we can replace g with $g \circ (1/X)$. Therefore, there are two cases, either g is a polynomial and h is a genuine Laurent polynomial, or g is a genuine Laurent polynomial and $h = X^n$ with $n > 0$.

If f is decomposable, we can decompose it until we see an indecomposable genuine Laurent polynomial L . Each time either we have a polynomial P_i on the left, or a X^j on the right, so $f = P_1 \circ P_2 \circ \dots \circ P_k \circ L \circ X^{n_1} \circ X^{n_2} \circ \dots \circ X^{n_l}$, let $f_1 = P_1 \circ P_2 \circ \dots \circ P_k$, $f_2 = L$ and $f_3 = X^{n_1} \circ X^{n_2} \circ \dots \circ X^{n_l}$. This concludes the proof. \square

3.2 Curves and function fields

By a *curve* we always mean a non-singular projective geometrically irreducible curve. In this thesis, we usually represent curves by affine equations which might have singularities, but this curve is always birationally equivalent to the unique non-singular projective curve corresponding to its function field. When we refer to genus of a curve defined by equations, this genus is always the genus of this unique non-singular projective curve, or equivalently, the genus of the function field.

By a *function field over a field K* , we mean a finitely-generated extension L/K of transcendental degree 1, and we require that K is the full constant field of L .

3.3 Function field tower

Let $f(X), g(X) \in \mathbb{K}(X) \setminus \mathbb{K}$ be any rational functions, let t be a transcendental element over \mathbb{K} , and let x, y be roots of $f(X) - t$ and $g(X) - t$ respectively. Then we can build the following function fields tower in Figure 3.1.

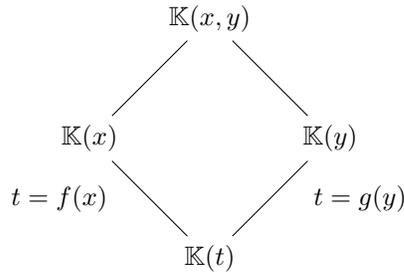


Figure 3.1: Function field tower

In this tower, $\mathbb{K}(x, y)$ is the function field of an irreducible factor of $f(X) - g(Y)$, and in fact, for every irreducible factor of $f(X) - g(Y)$, we can choose appropriate x, y , such that the function field $\mathbb{K}(x, y)$ is the function field of the factor. We will work with function fields directly, instead of working on the irreducible factors of $f(X) - g(Y)$. Besides the stated correspondence between the irreducible factors and

the function fields, there are more reasons why we choose to work with function fields:

1. The genus of a factor is in fact the genus of the normalization of the factor (as a curve), which equals the genus of the function field, so we do not need to know what the normalization of the factor looks like.
2. There are a lot of tools in terms of function fields (Galois theory, Abyhankar's lemma, Riemman-Hurwitz formula) to analyze reducibility and calculate genus.

The goal of this thesis may be restated as determining all genuine Laurent polynomials f for which there is a corresponding function field $\mathbb{K}(x, y)$ of genus at most 1.

Definition III.4. Let L be a function field over \mathbb{K} , let M_1 and M_2 be finite extensions of L , and let $M = M_1M_2$. Then we refer to the diagram in Figure 3.2 as a *square*. We say the square is *irreducible* if $[M : M_1] = [M_2 : L]$ or equivalently, $[M : L] =$

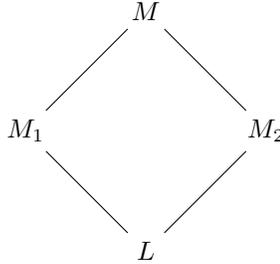


Figure 3.2: Function field tower

$[M_1 : L][M_2 : L]$; otherwise, we say the square is *reducible*.

For example, in the tower in Figure 3.1, if the square is irreducible, then $f(X) - g(Y)$ must be irreducible; and otherwise, $\mathbb{K}(x, y)$ corresponds to an irreducible factor of $f(X) - g(Y)$.

We use the following two towers very often in this paper:

1. In Figure 3.1, choose $g = f$ and $y \neq x$. Then $\mathbb{K}(x, y)$ is the function field of an irreducible factor of $F_f(X, Y) = \frac{f(X)-f(Y)}{X-Y}$.
2. In Figure 3.1, choose $g = cf$ where $c \in \mathbb{K} \setminus \{1\}$ is a root of unity. Then $\mathbb{K}(x, y)$ is the function field of an irreducible factor of $f(X) - cf(Y)$.

The tower above is for single functions f, g . We will often study function field towers in which f and g are given as compositions of lower-degree functions, namely $f = f_1 \circ f_2$ and $g = g_1 \circ g_2$ where $f_1, f_2, g_1, g_2 \in \mathbb{K}(X) \setminus \mathbb{K}$. In this setting we build the following more complicated function field tower, as in Figure 3.3.

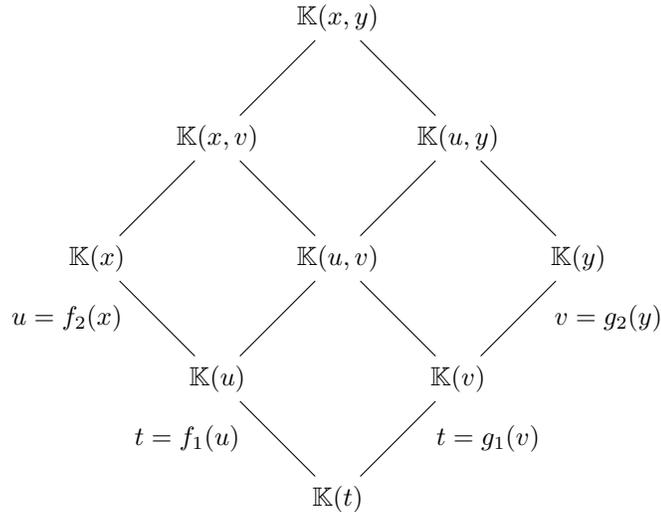


Figure 3.3: Tower of function fields

In Figure 3.3, x is transcendental over \mathbb{K} , y satisfies $f(x) = g(y)$, and we define $u := f_2(x)$ and $v := g_2(y)$ and $t := f_1(u)$. It follows that $t = g_1(v)$.

Definition III.5 (top/bottom/left/right square). In Figure 3.3, from top to bottom, from left to right, we call the four squares the *top square*, *left square*, *right square*, and *bottom square*.

In this paper, most times we choose $f = g$ to be the same genuine Laurent polynomial. A genuine Laurent polynomial has two possible decompositions, either

a polynomial composed with a genuine Laurent polynomial, or a genuine Laurent polynomial composed with a cyclic polynomial (in other words, X^n), and we choose $f_1 = g_1, f_2 = g_2$ according to which decomposition we are working on.

In the following sections, we will discuss the tools that can be applied to the function field tower. With the tools, we will be able to determine the degrees of the field extensions in a square, and compute the genus of a given function field in the tower.

3.4 Ramification and genus

3.4.1 Places and ramification

Each place in $\mathbb{K}(t)$ corresponds to a value $\alpha \in \mathbb{K} \cup \{\infty\}$, in fact, the maximal ideal of the place is generated by $(t - \alpha)$ if $\alpha \in \mathbb{K}$ and $1/t$ if $\alpha = \infty$, and we write α_t to represent the corresponding place in $\mathbb{K}(t)$. We use similar notation for other rational function fields such as $\mathbb{K}(u)$. We note that more complicated function fields such as $\mathbb{K}(u, v)$ do not necessarily contain exactly one place having a given value of u and v ; in subsequent sections we will describe how many such places exist in terms of ramification indices. The same thing is not true for $\mathbb{K}(u, v), \mathbb{K}(x, v)$, etc, since there may be more than one place in $\mathbb{K}(u, v)$ for a given value of u and v , to find exactly how many places, we will use Abyhankar's lemma stated in the following sections.

Let $f(X) \in \mathbb{K}(X)$ be a genuine Laurent polynomial, and let $\Lambda(f)$ be the set of values $\lambda \in \mathbb{K}$ such that $f(X) - \lambda$ has at least one multiple root. For any $\lambda_0 \in \Lambda(f)$, if the set of multiplicities of $f(X) - \lambda_0$ has a_i many b_i 's, $i \in \{1, \dots, d\}$, then we say λ_0 has *ramification type* $(b_1^{a_1} \dots b_d^{a_d})$. For example, for $f(X) = X + \frac{1}{X}$, $\Lambda(f) = \{\pm 2\}$, and ± 2 both have ramification type (2^1) , and ∞ will have ramification type (1^2) .

Definition III.6. Let $f(X) \in \mathbb{K}(X)$ be a rational function, and $\lambda \in \mathbb{K} \cup \{\infty\}$. If

$X = a$ (where $a \in \mathbb{K} \cup \{\infty\}$) is a solution to $f(X) = \lambda$, then we define $e_f(a)$ to be the multiplicity of the root $X = a$.

The ramification of f determines the ramification of $\mathbb{K}(x)/\mathbb{K}(t)$, where $f(x) = t$. For example, for $f(X) = X + \frac{1}{X}$, ∞_t is unramified with $0_x, \infty_x$ lying over it, and 2_t is totally ramified with 1_x lying over it.

Generally, let L/M be an extension of function fields over \mathbb{K} , let P be a place of M , and let Q_1, \dots, Q_d be the places of L lying over P . We write $e(Q_i|P)$ for the *ramification index* of Q_i/P , and we refer to the multiset of values $e(Q_1|P), \dots, e(Q_d|P)$ as the *ramification multiset* over P in L/M , which denote by $Ram_l(P)$. If we collect the multiplicity of the values in the multiset, we will get the *ramification type* as mentioned before.

Note that the sum of the elements of $Ram_l(P)$ equals $[L : M]$. We say that P is a *branch point* of L/M if the ramification multiset over P includes an integer larger than 1, and the *branch locus* $Br(L/M)$ of L/M is the set of all branch points of L/M .

If $L = \mathbb{K}(x)$ and $M = \mathbb{K}(t)$, and if ∞ is a branch point of f , then $Br(f) := Br(L/M) = \Lambda(f) \cup \{\infty\}$; if not, then $Br(f) := Br(L/M) = \Lambda(f)$. Note that here we use values to represent places.

3.4.2 Monodromy groups, Riemann's existence theorem and ramification

Definition III.7. Let $f(X) \in \mathbb{K}(X) \setminus \mathbb{K}$ be any rational function, let t be a transcendental element over $\mathbb{K}(X)$, and let x be a root of $f(X) - t$. We define the *monodromy group* of $f(X)$ to be the Galois group of the Galois closure of $\mathbb{K}(x)/\mathbb{K}(t)$, viewed as a group of permutations of the set of conjugates of x over $\mathbb{K}(t)$; in other words, it is the Galois group of $f(X) - t$ over $\mathbb{K}(t)$.

Throughout the thesis \mathbb{K} is fixed, since the monodromy group does not depend on the choice of t , once \mathbb{K} is fixed then the monodromy group only depends on f , so we can write the monodromy group as $\text{Mon}(f)$.

The monodromy group is very useful for the following reasons.

1. Müller [12] has determined all permutation groups which occur as monodromy groups of indecomposable genuine Laurent polynomials, see Theorem V.2.
2. $F_f(X, Y)$ is irreducible if and only if $\text{Mon}(f)$ is doubly transitive. If $\text{Mon}(f)$ is not doubly transitive, we can use it to compute the degree and genus of each irreducible factor of $F_f(X, Y)$.
3. Lemma III.9 states the relationship between the ramification of f and the monodromy group. Given the monodromy group, we are able to get some information on the ramification of f . Given a collection of ramification types, we can also determine whether there exists a corresponding rational function.

Definition III.8. For any $\sigma \in S_n$, define $O(\sigma)$ to be the number of cycles in σ .

We will use the following consequence of Riemann's existence theorem.

Lemma III.9. *For any $f(X) \in \mathbb{K}(X) \setminus \mathbb{K}$ with $Br(f) = \{t_1, \dots, t_d\}$, there exist $\tau_1, \dots, \tau_d \in \text{Mon}(f)$ satisfying all of the following:*

- $\text{Mon}(f) = \langle \tau_1, \dots, \tau_d \rangle$.
- $\prod_{i=1}^d \tau_i = 1$.
- For each τ_i , the multiset of cycle lengths of τ_i equals the multiset of ramification indices of t_i .
- $\sum_{i=1}^d (n - O(\tau_i)) = 2n - 2$.

Pick any nontrivial elements $\tau_1, \dots, \tau_d \in S_n$ such that $\sum_{i=1}^d (n - O(\tau_i)) = 2n - 2$, the group $\langle \tau_1, \dots, \tau_d \rangle$ is transitive, and $\prod_{i=1}^d \tau_i = 1$. Then, for any pairwise distinct elements $t_1, \dots, t_d \in \mathbb{K} \cup \{\infty\}$, there exists a rational function $f(X) \in \mathbb{K}(X)$ such that

- $\text{Mon}(f) = \langle \tau_1, \dots, \tau_d \rangle$.
- $\text{Br}(f) = \{t_1, \dots, t_d\}$, and for each t_i , the multiset of cycle lengths of τ_i equals the multiset of ramification indices of t_i .

Proof. It suffices to prove the result in case $\mathbb{K} = \mathbb{C}$. The first part is proved in [18, Theorem 2.13]. That result also shows that, for any τ_i 's as in the second part, there exists an extension $F/\mathbb{K}(t)$ and pairwise distinct places P_1, \dots, P_d of $\mathbb{C}(t)$ such that

- $[F : \mathbb{K}(t)] = n$
- Every place of $\mathbb{K}(t)$ other than the P_i 's is unramified in $F/\mathbb{K}(t)$
- The multiset of cycle lengths of τ_i equals the multiset of ramification indices in $F/\mathbb{K}(t)$ of all the places of F which lie over P_i .

Applying the Riemann–Hurwitz formula to $F/\mathbb{K}(t)$ shows that

$$2\mathbf{g}(F) - 2 = -2n + \sum_{i=1}^d (n - O(\tau_i)),$$

so that $2\mathbf{g}(F) - 2 = -2$ and thus F has genus zero. Therefore there is some $x \in F$ for which $F = \mathbb{K}(x)$, whence $t = f(x)$ for some rational function $f(X) \in \mathbb{K}(X)$. It follows that f has the required properties. \square

3.4.3 Abhyankar's lemma, genus and Riemann-Hurwitz formula

We will often need to determine the ramification in the compositum of two extensions of a function field. The first tool for this is known as Abhyankar's lemma.

Lemma III.10 (Abhyankar's lemma, Theorem 3.9.1 in [17]). *Let M_1/L and M_2/L be extensions of function fields over \mathbb{K} . For any place R of M_1M_2 , let $Q_i := R \cap M_i$ for $i \in \{1, 2\}$, and let $P := R \cap L$. Then $e(R|P)$ is the least common multiple of $e(Q_1|P)$ and $e(Q_2|P)$.*

The second tool describes the number of places R which correspond to prescribed places Q_1 , and Q_2 . This number is the greatest common divisor of $e(Q_1|P)$ and $e(Q_2|P)$ if $[M_1M_2 : M_2] = [M_1 : L]$; when this condition does not hold, we still get this number of places if we sum over the fields whose product is $M_1 \otimes_L M_2$. It is more convenient to state this result in the language of curves, where a modern reference is [3].

Lemma III.11 (Lemma 7.1 in [3]). *Let $\phi_1 : C_1 \rightarrow D$, and $\phi_2 : C_2 \rightarrow D$ be non constant morphisms of curves over \mathbb{K} , and let B_1, \dots, B_d be the curves which are components of the fibered product $C_1 \times_D C_2$. Let $Q_i \in C_i(\mathbb{K})$ for $i \in \{1, 2\}$, and assume that $\phi_1(Q_1)$ and $\phi_2(Q_2)$ both equal the same point $P \in D(\mathbb{K})$. For each $j \in \{1, \dots, r\}$, let m_j be the number of points in $B_j(\mathbb{K})$ whose image in $C_i(\mathbb{K})$ is Q_i for each $i \in \{1, 2\}$. Then $\sum_{j=1}^l m_j = \gcd(e(Q_1|P), e(Q_2|P))$.*

Combining the above two lemma with the Riemann-Hurwitz genus formula for M_1M_2/M_1 yields the following useful formulas, which we will refer to as Riemann-Hurwitz.

Lemma III.12 (Riemann-Hurwitz). *Let M_1/L and M_2/L be extensions of function fields over \mathbb{K} , and write $n_i := [M_i : L]$. Let \mathfrak{g}_i be the genus of M_i , and let \mathfrak{g} be the genus of M_1M_2 . If $[M_1M_2 : M_2] = n_1$ then*

$$2\mathfrak{g} - 2 = n_1(2\mathfrak{g}_1 - 2) + \sum_{P \in \text{Br}(M_1/L)} \sum_{e_i \in \text{Ram}_{M_i}(P)} (e_1 - \gcd(e_1, e_2)).$$

If M_1/L and M_2/L are isomorphic extensions and $[M_1M_2 : M_2] = n_1 - 1$ then

$$2\mathbf{g} - 2 = (n_1 - 1)(2\mathbf{g}_1 - 2) + \sum_{P \in \text{Br}(M_1/L)} \sum_{e_i \in \text{Ram}_{M_i}(P)} (e_1 - \gcd(e_1, e_2)).$$

Proof. Apply Riemann–Hurwitz genus formula on M_1M_2/M_2 , we have

$$2\mathbf{g} - 2 = [M_1M_2 : M_2](2\mathbf{g}_1 - 2) + \sum_{P \in \text{Br}(M_1/L)} \sum_{Q/R/P} (e(Q|R) - 1).$$

where Q, R are places in M_1M_2 and M_2 lying over P , and Q lies over R . Suppose R_1, \dots, R_d be the places over P with ramification indices e_1, \dots, e_d . Pick any R_i in M_2 and R_j in M_1 , then there are $\gcd(e_i, e_j)$ many places in M_1M_2 lying over both R_i and R_j , and by Abhyankar’s lemma, each place has ramification index $\text{lcm}(e_i, e_j)/e_i$, which equals $e_j/\gcd(e_i, e_j)$. Therefore, $\sum_{Q/R_j} (e(Q|R_j) - 1) = e_j - \gcd(e_i, e_j)$. We get the desired result by summing over all R_j ’s. This proves the first formula. For the second formula, for each R_j , there are $e_j - 1$ places in M_1M_2 lying over R_j in M_1 and R_j in M_1 instead of e_j many. However, this does not matter since all such places are unramified over R_j , the same formula still holds. This proves the second formula. \square

Definition III.13. We use $\mathbf{g}_{xy}, \mathbf{g}_{xv}$, etc., to represent the genus of the function field $\mathbb{K}(x, y), \mathbb{K}(x, v)$, etc.

The two Riemann–Hurwitz formulas give us information on the ramification in function field extensions. In particular, we will apply Riemann–Hurwitz to the tower in Figure 3.3, where the condition \mathbf{g}_{xy} imposes severe constraints on the ramification in the various field extensions in the diagram. We often apply the following special case of Lemma III.12.

Lemma III.14 (Riemann–Hurwitz). *Let $f, g \in \mathbb{K}(X) \setminus \mathbb{K}$ be two rational functions.*

If $f(X) - g(Y)$ is irreducible, then the genus \mathfrak{g} of the curve $f(X) - g(Y) = 0$ is given by

$$2\mathfrak{g} - 2 = -2 \deg(f) + \sum_{\lambda \in \text{Br}(f) \cup \text{Br}(g)} \sum_{f(a)=g(b)=\lambda} (e_f(a) - \gcd(e_f(a), e_g(b))).$$

If $F_f(X, Y)$ is irreducible, then the genus \mathfrak{g} of the curve $F_f(X, Y) = 0$ is given by

$$2\mathfrak{g} - 2 = -2(\deg(f) - 1) + \sum_{\lambda \in \text{Br}(f)} \sum_{f(a)=f(b)=\lambda} (e_f(a) - \gcd(e_f(a), e_f(b))).$$

Proof. Let $K = \mathbb{K}$, $M_1 = \mathbb{K}(x)$ and $M_2 = \mathbb{K}(y)$ where x is a root of $f(X) - t$ and y is a root of $g(Y) - t$. The two formulas follow directly from Lemma III.12. \square

In this paper, we will apply the first formula to $f(X) - cf(Y)$, where $c \in \mathbb{K} \setminus \{1\}$, $f(X)$ is a genuine Laurent polynomial, and $f(X) - cf(Y)$ is irreducible.

3.5 Degree of the composite of two extensions of a function field

Recall in Definition III.4, we call the function field tower formed by a function field, two extension fields, and the composite of the two extensions a square. Most of the time, we cannot apply the Riemann–Hurwitz formula to a square directly, unless we know the square is irreducible, or reducible in the specific way stated in Lemma III.12. So irreducibility is the first thing we need to check before applying the Riemann–Hurwitz formula.

However, it is not always true that a square is irreducible or reducible in the way we want. The good news is we can divide the square into tower of squares, by adding intermediate fields, and after that the left, right, top squares in this tower will be

irreducible, as stated in Theorem III.15, and Theorem III.16 gives more constraints on the ramification in the bottom square.

Theorem III.15 (Fried–Müller–Zieve). *Let K be a function field over \mathbb{K} , and let L and M be finite extensions of K . Then there are fields L' and M' satisfying all of the following:*

- (1) $K \subseteq L' \subseteq L$ and $K \subseteq M' \subseteq M$.
- (2) L'/K and M'/K have the same Galois closure.
- (3) $[L : L'] = [L.M : L' : M]$ and $[M : M'] = [L.M : L.M']$.

Condition (3) says that the top, left, and right squares are irreducible, while condition (2) gives a strong constraint on the bottom square (which might be reducible).

Proof. A weaker version is proved in [5, Proposition 2]. The general version stated in this theorem is proved by Müller and Zieve in [13]. \square

If L'/K and M'/K have the same Galois closure, as in the above theorem, we have more constraints, as shown in the following theorem. These constraints will enable us to analyze the conditions for the bottom square to be reducible.

Theorem III.16. *If L'/K and M'/K have the same Galois closure N , then for any place P of K , the ramification index in N/K of any place lying over P equals the lcm of the ramification indices in L'/K of all the places lying over P , and likewise equals the lcm of the ramification indices in M'/K of all places lying over P . In particular, $Br(L'/K) = Br(M'/K)$.*

Proof. We use the fact that, if L'/K is an extension of function fields over \mathbb{K} , and N is its Galois closure, and we pick a place Q of N having inertia group I in N/K , then the orbits of I on the set $Hom_K(L', N)$ are in bijection with the places of L'

which lie over the place $Q \cap K$, and moreover this bijection can be chosen so that the size of the I -orbit equals the ramification index in L'/K of the corresponding place of L' . Next, since N is the Galois closure of L'/K , no nonidentity element of $Gal(N/K)$ fixes every element of $Hom_K(L', N)$. It follows that $Gal(N/K)$ (and hence I) embeds into the group of permutations of $Hom_K(L', N)$. Since I is cyclic, this means that the order of I is cyclic, it follows that the order of I is the lcm of the lengths of its orbits on $Hom_K(L', N)$, and hence is the lcm of the ramification indices in L'/K of the places over $Q \cap K$. \square

3.6 Facts on the factorization of certain polynomials

One case we will study in this thesis is when a genuine Laurent polynomial is the composition of a polynomial and an indecomposable genuine Laurent polynomial. In this case, in Figure 3.3, $f_1 = g_1$ will be the polynomial. There are two important classes of polynomials we use very often in this thesis: the cyclic polynomial X^n and the Chebyshev polynomial T_n . We list some facts about their factorizations in this section.

Definition III.17. The Chebyshev polynomial T_n is the unique polynomial which satisfies the equation $T_n(X + \frac{1}{X}) = X^n + \frac{1}{X^n}$.

If $n = 2$ then $T_2(X) = X^2 - 2$ which has branch points $\{-2, \infty\}$, both of which are totally ramified. Now we study the ramification and branch points of T_n for $n > 2$. Let y be transcendental over \mathbb{K} , then the field extension $\mathbb{K}(y)/\mathbb{K}(y^n + 1/y^n)$ has an intermediate field $\mathbb{K}(y + 1/y)$. The branch points of $\mathbb{K}(y)/\mathbb{K}(y^n + 1/y^n)$ are $\{-2, 2, \infty\}$ where ∞ has type (n^2) and ± 2 both have type (2^n) . For the branch point ∞ , note that $y = 0$ and $y = \infty$ both lie over $y + 1/y = \infty$ so ∞ is a totally ramified branch point of $\mathbb{K}(y + 1/y)/\mathbb{K}(y^n + 1/y^n)$. All the places in $\mathbb{K}(y)$ lying over

$y^n + 1/y^n = \pm 2$ have ramification index 2 over $\mathbb{K}(y^n + 1/y^n)$ but are unramified over $\mathbb{K}(y + 1/y)$ unless $y = \pm 1$, therefore all the places in $\mathbb{K}(y + 1/y)$ lying over $y^n + 1/y^n = \pm 2$ has ramification index 2 except the place $y + 1/y = \pm 1$ which is unramified. The analysis above shows that:

If $n > 2$, then the branch locus of $T_n(X)$ is $\{2, -2, \infty\}$; the infinite place of $\mathbb{K}(T_n(x))$ is totally ramified in $\mathbb{K}(x)/\mathbb{K}(T_n(x))$; all places of $\mathbb{K}(x)$ which lie over the places $T_n(x) = \pm 2$ have ramification index 1 or 2 in $\mathbb{K}(x)/\mathbb{K}(T_n(x))$, and the only such places of $\mathbb{K}(x)$ which have ramification index 1 are the places $x = \pm 2$.

In the following lemma, we define μ_n to be the set of all n -th root of unity.

Lemma III.18. *For any positive integer n and any $c \in \mathbb{K}^*$, we have*

$$X^n - cY^n = \prod_{\xi^n=c} (X - \xi Y)$$

Moreover, $T_n(X) - cT_n(Y)$ is irreducible if $c \neq \pm 1$. Finally, if $e \in \{0, 1\}$ satisfies $e \equiv n \pmod{2}$, then

$$F_{T_n}(X, Y) = (X + Y)^{1-e} \prod_{\substack{\xi \in \mu_n \setminus \{\pm 1\} \\ \xi \sim \xi^{-1}}} (X^2 - XY(\xi + \xi^{-1}) + Y^2 + (\xi - \xi^{-1})^2).$$

$$T_n(X) + T_n(Y) = (X + Y)^e \prod_{\substack{\xi \in \mu_{2n} \setminus \{\mu_n \cup \mu_2\} \\ \xi \sim \xi^{-1}}} (X^2 - XY(\xi + \xi^{-1}) + Y^2 + (\xi - \xi^{-1})^2).$$

where each product is taken over a system of representatives of the relevant set of ξ 's modulo the equivalence relation $\xi \sim \xi^{-1}$, and each quadratic polynomial occurring in each product is irreducible.

Proof. We refer the reader to Lemma 1 on page 52 of [16]. □

3.7 Ramification and decomposability

Lemma III.19 and Lemma III.20 say that genuine Laurent polynomials of certain ramification types are decomposable.

Lemma III.19. *Let $f(X) \in \mathbb{K}(X) \setminus \mathbb{K}$ be any rational function which has at least three branch points. If there is an integer $N > 1$ such that at least two branch points of f have all their ramification indices being multiples of N , then $f(X)$ is decomposable.*

Proof. We can assume the two branch points of f whose ramification indices are all divisible by N are 0 and ∞ , since otherwise we can compose f to the right with a linear fractional which maps 0 and ∞ to the two branch points. This new function and f have the same decomposability, so we lose no generality.

Let g, h be the numerator and denominator of f , then the fact that all ramification indices over 0 and ∞ are divisible by N implies that $g = g_1^N$ and $h = h_1^N$ for some polynomials g_1 and h_1 . Thus $f = (g_1/h_1)^N$, so if f is decomposable then g_1/h_1 has degree 1, but then f has only two branch points whereas our hypothesis required it to have at least three. □

Lemma III.20. *Let $f(X) \in \mathbb{K}[X, X^{-1}]$ be a genuine Laurent polynomial of degree n , where n is even and $n > 2$. If the denominator of f is $X^{n/2}$, and f has three finite branch points with ramification types $\{(2^{\frac{n}{2}}), (1^2 2^{\frac{n-2}{2}}), (1^{n-2} 2^1)\}$, then $f(X)$ is decomposable.*

Proof. Let a, d, b, c be the corresponding branch cycles (see Lemma III.9). Thus, writing $n = 2m$, a, b, c, d are elements of S_n with cycle structures $a : m, m$, $d : 2, 1^{n-2}$, $b : 2^m$, and $c : 2^{m-1}, 1^2$, such that $adbc = 1$ and $G = \langle a, b, c, d \rangle$ is transitive. To prove the result, we show that there is a G -invariant partition of $\{1, 2, \dots, n\}$ into m two-element sets.

Since b, c have order 2, we get $ad = (bc)^{-1} = c^{-1}b^{-1} = cb$.

Assume for the moment that d connects the two cycles of a . Then without loss

we may assume that $a = (1, 2, \dots, m)(m + 1, \dots, n)$ and $d = (m, n)$, so that $ad = (1, 2, \dots, n)$. Now let B be the partition of $\{1, 2, \dots, n\}$ into $n/2$ 2-element sets, defined by $B = \{\{i, i + m\} : i = 1, 2, \dots, m\}$. Clearly a and d permute the sets in B . But since b, c have order 2, each of them conjugates cb to its inverse: $b(cb)b = bc = c(cb)c$. Since we already know that $ad = cb$, it follows that b, c conjugate ad to its inverse. This lets us write down b, c : say $b(k) = r$, then $b(ad)b$ maps $k \mapsto b(r + 1)$, but we know that $b(ad)b$ is the inverse of ad , and hence maps $k \mapsto k - 1$. So $b(r + 1) = k - 1$, and since b has order 2, we also get $b(k - 1) = r + 1$. Now repeat this to get $b(k - 2) = r + 2$, $b(k - 3) = r + 3, \dots$, and in general $b(i) = -i + \text{constant}$. But this clearly permutes the sets in B , since those sets are simply the cosets mod m . Hence a, d, b (and similarly c) permute the sets in B , so also $G = \langle a, b, c, d \rangle$ permutes these sets, as desired.

We now prove that d must connect the two cycles of a . Suppose otherwise. Suppose without loss that $d = (1, k)$ for some $k \leq m$. Then $ad = (1, k + 1, k + 2, \dots, m)(2, 3, \dots, k)(m + 1, m + 2, \dots, n)$. We claim that in this case it is not possible that $\langle a, b, c, d \rangle$ was transitive, since a, b, c, d will map $\{m + 1, m + 2, \dots, n\}$ to itself. This is clear for a and d . As before, b conjugates $da = bc$ to its inverse, so b normalizes the group $\langle da \rangle$, which implies that b permutes the $\langle da \rangle$ -orbits (because $b\langle da \rangle = \langle da \rangle b$ so $b\langle da \rangle(i) = \langle da \rangle b(i)$ which means that the b -image of the $\langle da \rangle$ -orbit containing i equals the $\langle da \rangle$ -orbit containing $b(i)$). But $\{m + 1, \dots, n\}$ is strictly bigger than the other two $\langle da \rangle$ -orbits, so b must map it to itself. Likewise for c . Hence $\langle a, b, c, d \rangle$ is not transitive, contradiction. \square

3.8 Inequalities connected with the Riemann-Hurwitz formula

In this paper, we will apply the first formula in Lemma III.14 to $f(X) - cf(Y)$, where $f(X) \in \mathbb{K}[X, X^{-1}]$ is a genuine Laurent polynomial, $c \in \mathbb{K}^* \setminus \{1\}$, and $f(X) - cf(Y)$ is irreducible. The Riemann-Hurwitz formula looks like this:

$$0 \geq 2g - 2 = -2 \deg(f) + \sum_{\lambda \in \text{Br}(f) \cup \text{Br}(cf)} \sum_{f(a)=cf(b)=\lambda} (e_f(a) - \gcd(e_f(a), e_{cf}(b))).$$

By switching the roles of f and cf , we get, we get

$$0 \geq 2g - 2 = -2 \deg(f) + \sum_{\lambda \in \text{Br}(f) \cup \text{Br}(cf)} \sum_{f(a)=cf(b)=\lambda} (e_{cf}(b) - \gcd(e_f(a), e_{cf}(b))).$$

Then we add the two equations together to get

$$4 \deg(f) \geq \sum_{\lambda \in \text{Br}(f) \cup \text{Br}(cf)} \sum_{f(a)=cf(b)=\lambda} (e_f(a) + e_{cf}(b) - 2 \gcd(e_f(a), e_{cf}(b))).$$

We would like to get a lower bound for $\sum_{f(a)=cf(b)=\lambda} (e_f(a) + e_{cf}(b) - 2 \gcd(e_f(a), e_{cf}(b)))$, which will be useful for determining how many branch points f and cf have in total in Chapter IX. In this section, we just work on the lower bound.

Note that $\sum_{f(a)=\lambda} e_f(a) = \deg(f)$ and $\sum_{cf(b)=\lambda} e_{cf}(b) = \deg(f)$, so we reduce it to the following problem.

Problem III.21. *Let $n, a_1, a_2, \dots, a_d, b_1, b_2, \dots, b_l$ be positive integers such that $\sum_{i=1}^d a_i = \sum_{j=1}^l b_j = n$. What is a good lower bound for $\sum_{i=1}^d \sum_{j=1}^l (a_i + b_j - 2 \gcd(a_i, b_j))$ which depends only on n ?*

In the following three lemmas we give lower bounds in case the a_i 's and b_j 's satisfy any of three sets of additional conditions.

Lemma III.22 (Carney–Hortsch–Zieve [2]). *Let a_1, \dots, a_d and b_1, \dots, b_l be positive integers such that $\sum_{i=1}^d a_i = \sum_{j=1}^l b_j = n$ and $\gcd(a_1, \dots, a_d) = \gcd(b_1, \dots, b_l) = 1$.*

Then

$$\sum_{i=1}^d \sum_{j=1}^l (a_i + b_j - 2 \gcd(a_i, b_j)) \geq n - 1$$

unless every a_i and every b_j is 1. Moreover, equality holds exactly when both the a_i 's and b_j 's are 1, 2, 2, \dots , 2, and the sum equals n if and only if either

- both the a_i 's and b_j 's are 3, 1 (so $n = 4$)
- both the a_i 's and b_j 's are 2, 1, 1 (so $n = 4$) or
- the a_i 's are 1, 1, \dots , 1 and the b_j 's are 2, 1, 1, \dots , 1, or vice-versa.

Lemma III.23. Let a_1, \dots, a_d be positive integers such that $\sum_{i=1}^d a_i = n$ and $\gcd(a_1, \dots, a_d) > 1$.

1. Then

$$\sum_{i=1}^d \sum_{j=1}^d (a_i + a_j - 2 \gcd(a_i, a_j)) \geq \frac{2n}{3}$$

unless all a_i 's are equal.

Proof. By applying the previous lemma to $a_1/a, \dots, a_d/a$, where $a := \gcd(a_1, \dots, a_d)$,

we see that

$$\begin{aligned} & \sum_{i=1}^d \sum_{j=1}^d (a_i + a_j - 2 \gcd(a_i, a_j)) \\ &= a \sum_{i=1}^d \sum_{j=1}^d \left(\frac{a_i}{a} + \frac{a_j}{a} - 2 \gcd\left(\frac{a_i}{a}, \frac{a_j}{a}\right) \right) \\ &\geq a \left(\frac{n}{a} - 1 \right) = n - a \end{aligned}$$

unless all a_i 's are equal. If $a = n$ or $a = \frac{n}{2}$, then all a_i 's are the same, and

$\sum_{i=1}^d \sum_{j=1}^d (a_i + a_j - 2 \gcd(a_i, a_j)) = 0$; if not, then $a \leq \frac{n}{3}$, so the result follows. \square

Lemma III.24. Let a_1, \dots, a_d and b_1, \dots, b_l be positive integers such that $\sum_{i=1}^d a_i = \sum_{j=1}^l b_j = n$ and $\gcd(a_1, \dots, a_d) > 1$ but $\gcd(b_1, \dots, b_l) = 1$. Then

$$\sum_{i=1}^d \sum_{j=1}^l (a_i + b_j - 2 \gcd(a_i, b_j)) \geq n$$

where equality holds if and only if the a_i 's are $2, 2, \dots, 2$, and the b_j 's are $1, 1, 2, 2, \dots, 2$ or vice-versa.

Proof. It suffices to show that $\sum_{j=1}^l (a_i + b_j - 2 \gcd(a_i, b_j)) \geq a_i$ for every i , and to find the conditions when the equality holds. Since if this is true, then $\sum_{i=1}^d \sum_{j=1}^l (a_i + b_j - 2 \gcd(a_i, b_j)) \geq \sum_{i=1}^d a_i = n$, and the equality holds if and only if $\sum_{j=1}^l (a_i + b_j - 2 \gcd(a_i, b_j)) = a_i$ for every i .

From now on, we fix one i , prove $\sum_{j=1}^l (a_i + b_j - 2 \gcd(a_i, b_j)) \geq a_i$ and find the condition when the equality holds.

If some b_j satisfies $\gcd(a_i, b_j) < b_j$, say b_1 , then $\gcd(a_i, b_1) \leq \frac{b_1}{2}$ and $a_i + b_1 - 2 \gcd(a_i, b_1) \geq a_i$. However, in fact this cannot be equality. If equality holds then $\gcd(a_i, b_1) = \frac{b_1}{2}$ and $a_i + b_j - 2 \gcd(a_i, b_j) = 0$ for all $j \neq 1$. Let $b_1 = 2b$, then $a_i = bc$ where c is odd, and $b_j = a_i = bc$ for $j \neq 1$. Now $1 = \gcd(b_1, \dots, b_d) = b$, so the b_j 's are $1, c, c, \dots, c$ and $a_i = c$. However, in this case, $\gcd(a_i, n) = \gcd(c, 1 + c(l-1)) = 1$, which violates the condition that $\gcd(a_1, \dots, a_s) > 1$.

If all b_j satisfy $\gcd(a_i, b_j) = b_j$, then $b_j \mid a_i$ for every j . We show there are j_1, j_2 such that $b_{j_1} < a_i$ and $b_{j_2} < a_i$, so $\sum_{j=1}^l (a_i + b_j - 2 \gcd(a_i, b_j)) = \sum_{j=1}^l (a_i - b_j) \geq \sum_{j=j_1, j_2} (a_i - \frac{a_i}{2}) = a_i$. Suppose instead that there is at most one $j = j_1$ for which $b_j < a_i$. Since the b_j 's are coprime and they all divide a_i , we must have $b_{j_1} = 1$. Now $n = \sum_{j=1}^l b_j = 1 + (l-1)a_i$, so $\gcd(n, a_i) = 1$, which violates the non-trivial gcd condition of a_i 's.

Therefore we have the desired inequality.

It becomes equality if and only if for all i , $\sum_{j=1}^l (a_i + b_j - 2 \gcd(a_i, b_j)) = a_i$. According to the above arguments, it only can happen in the second case. In that case $\sum_{j=1}^l (a_i + b_j - 2 \gcd(a_i, b_j)) = \sum_{j=1}^l (a_i - b_j) \geq \sum_{j=j_1, j_2} (a_i - \frac{a_i}{2}) = a_i$ implies $b_{j_1} = b_{j_2} = \frac{a_i}{2}$ and the rest of the b_j 's equal a_i . Now $\gcd(b_1, \dots, b_d) = \frac{a_i}{2} = 1$ implies

$a_i = 2$, $b_{j_1} = b_{j_2} = 1$, and the rest of the b_j 's equal $a_i = 2$. □

3.9 Equivalent and strongly equivalent functions

Definition III.25. For polynomials $f, g \in \mathbb{K}[X] \setminus \mathbb{K}$, we say they are *equivalent* if $f = \nu \circ g \circ \mu$ for some degree-one $\mu, \nu \in \mathbb{K}[X]$; we say they are *strongly equivalent* if $f = (aX) \circ g \circ \mu$ for some $a \in \mathbb{K}^*$ and some degree-one $\mu \in \mathbb{K}[X]$.

For genuine Laurent polynomials $f, g \in \mathbb{K}[X, X^{-1}] \setminus \mathbb{K}$, we say they are *equivalent* if $f = \nu \circ g \circ \mu$ for some degree-one $\nu \in \mathbb{K}[X]$ and $\mu(X) = eX^p$ for some $e \in \mathbb{K}^*$ and $p \in \{-1, 1\}$; we say they are *strongly equivalent* if $f = (aX) \circ g \circ \mu$ for some $a \in \mathbb{K}^*$ and $\mu(X) = eX^p$ for some $e \in \mathbb{K}^*$ and $p \in \{-1, 1\}$.

Remark III.26. Let f, g be two polynomials or two genuine Laurent polynomials. If they are equivalent then there is a genus-preserving bijection between the irreducible factors of $F_f(X, Y)$ and those of $F_g(X, Y)$. If they are strongly equivalent then, for every $c \in \mathbb{K}^*$, there is a genus-preserving bijection between the irreducible factors of $F_{f,c}(X, Y)$ and those of $F_{g,c}(X, Y)$ up to multiplication by some nonzero element in \mathbb{K}^* . More precisely if $H(X, Y)$ is an irreducible factor of $F_g(X, Y)$ (respectively $F_{g,c}(X, Y)$) then the numerator $\hat{H}(X, Y)$ of $H(\mu(X), \mu(Y))$ is an irreducible factor of $F_f(X, Y)$ (respectively $F_{f,c}(X, Y)$) and they have the same genus.

CHAPTER IV

Indecomposable genuine Laurent polynomial case: Part I

In this chapter and the next chapter, we classify the indecomposable genuine Laurent polynomials such that $F_f(X, Y)$ has a factor of genus at most 1. The main result in this chapter is Theorem IV.1, which gives the classification of the genuine Laurent polynomials for which $F_f(X, Y)$ is irreducible with genus 0 or 1. We prove this theorem by firstly showing that when $\deg(f) \geq 26$ there is only one equivalence class (see Definition III.25) of Laurent polynomials; we use a computer to determine the small degree cases (up to 26) and get the small degree cases (up to the equivalence relation defined in Definition III.25) in Table 4.1.

Theorem IV.1. *Let $f(X) \in \mathbb{K}[X, X^{-1}]$ be a genuine Laurent polynomial with denominator X^k . If $F_f(X, Y)$ is irreducible and its genus \mathfrak{g} is in $\{0, 1\}$, then up to the equivalence relation one of the following holds:*

1. $f(X) = \frac{(X+1)^n}{X^k}$ where $\gcd(n, k) = 1$ and $n > k$. Here $F_f(X, Y)$ has genus 0.
2. $f(X)$ has degree at most 10 and is one of the Laurent polynomials in Table 4.1.

The values of k and \mathfrak{g} , the value of $n := \deg(f)$, and the ramification type of f are listed in Table 4.2.

Table 4.1: Indecomposable genuine Laurent polynomials f where $F_f(X, Y)$ has genus 0 or 1

(1) $X + 1/X$
(2.1) $(X^3 + 1)/X$
(2.2) $(X^3 + X^2 + a)/X$ where $a \in \mathbb{K} \setminus \{0, 1/27\}$
(3) $(X^2 + aX + 1)^2/X$ where $a^2 \in \mathbb{K} \setminus \{4, -12\}$
(4) $(X - 1)^3(X + a)/X^2$ where $a \in \mathbb{K} \setminus \{0, -1, 7 \pm 4\sqrt{3}\}$
(5) $(X^4 + 4X^3 + 2X - 1/4)/X^2$
(6) $(X^4 - 6X^2 - 3)/X$
(7) $(X - 1)^3(X - 9)/X$
(8.1) $(X - 1)^4(X - 4(i + 1))/X$ where $i^2 = -1$
(8.2) $(X - 1)^4(X - 27/2)/X^2$
(9) $(X - 1)^5(X + (3s + 7)/2)/X^3$ where $s^2 = 5$
(10) $(X - 1)^5(X - (3s + 11)/2)/X^2$ where $s^2 = -15$
(11) $(X - 1)^5(X + 4s - 9)/X^3$ where $s^2 = 5$
(12.1) $(X^3 + 9X + 2)^2/X^3$
(12.2) $(X^3 + 3X^2 + (9w^2 - 1)X + 2w^3 + w^2 - 1/27)^2/X^3$ where $w \in \mathbb{K} \setminus \{0, 1/6, -1/3, 2/3\}$ and $w^2 + 8/21w - 8/63 \neq 0$
(13) $(X - 1)^4(X + (3s - 11)/2)^2/X$ where $s^2 = -15$
(14) $(X^2 + 8X - 2)^3/X^2$
(15) $(X^2 + 10X + 5)^3/X$
(16) $(X^2 + 5X - 5)^3/X$
(17) $(X - 1)^3(X - 16)^2(X - 25)/X$
(18) $(X - 1)^4(X^2 - 6X + 25)/X$
(19.1) $(X + 9)(X^2 + (2w + 7)X + w + 2)^3/X$ where $w \in \mathbb{K}$ has order 3
(19.2) $(X + 25)(X^2 + X - 256/5)^3/X^2$
(19.3) $(X + 1)(X^2 + 5/27X - 1/48)^3/X^3$
(20) $(X^2 + 13X + 49)(X^2 + 5X + 1)^3/X$
(21.1) $(X^2 + 2X + (s + 3)/14)^4/X$ where $s^2 = -7$
(21.2) $(X^2 + X - 27/20)^4/X^3$
(22.1) $(X^3 + 12X^2 + 3(s + 11)X + s + 5)^3/X$ where $s^2 = -2$
(22.2) $(X^3/21 + X^2 + X/4 - 32/3)^3/X^2$
(22.3) $(X^3 + 3/2X^2 + 24/5X - 10)^3/X^4$
(23.1) $(X^2 + X + (i + 1)/32)^5/X^2$ where $i^2 = -1$
(23.2) $(X^2 + 3X - 4)^5/X^4$
(24) $(X + 1/4)^8(X + a(a + 1)^2 - 1/4)^2/X^5$ where $a^4 - 2a^2 + 2 = 0$

4.1 Setup and some inequalities

In Lemma III.14, the second formula is the genus formula for $F_f(X, Y)$, where $F_f(X, Y)$ is irreducible.

$$2\mathfrak{g}_{xy} - 2 = -2(\deg(f) - 1) + \sum_{\lambda \in \text{Br}(f)} \sum_{f(a)=f(b)=\lambda} (e_f(a) - \gcd(e_f(a), e_f(b)))$$

Our goal is to use this formula to find all the possible ramification types of $f(X)$, subject to the genus constraint $\mathfrak{g}_{xy} \leq 1$. We expect a result as stated in Theorem IV.1.

Table 4.2: Ramification types of Laurent polynomials f from Table 4.1

case	$\text{Mon}(f)$	\mathfrak{g}	k	ramification indices (∞ not counted)
(1)	S_2	0	1	$(2^1), (2^1)$
(2)	S_3	1	1	$(1^1 2^1), (1^1 2^1), (1^1 2^1)$
(3)	S_4	1	1	$(2^2), (1^2 2^1), (1^2 2^1)$
(4)	S_4	1	2	$(1^1 3^1), (1^2 2^1), (1^2 2^1)$
(5)	A_4	0	2	$(1^1 3^1), (1^1 3^1)$
(6)	A_4	1	1	$(1^1 3^1), (1^1 3^1)$
(7)	A_4	0	1	$(2^2), (1^1 3^1)$
(8.1)	$AGL_1(5)$	1	1	$(1^1 2^2), (1^1 4^1)$
(8.2)	S_5	1	2	$(1^1 2^2), (1^1 4^1)$
(9)	A_6	1	3	$(1^1 5^1), (1^3 3^1)$
(10)	A_6	1	2	$(1^1 5^1), (1^2 2^2)$
(11)	A_5	0	3	$(1^1 5^1), (1^2 2^2)$
(12)	S_6	1	3	$(1^3 3^1), (2^3), (1^4 2^1)$
(13)	A_6	1	1	$(2^1 4^1), (1^2 2^2)$
(14)	A_6	0	2	$(1^3 3^1), (3^2)$
(15)	A_5	0	1	$(1^2 2^2), (3^2)$
(16)	A_6	1	1	$(1^3 3^1), (3^2)$
(17)	S_6	1	1	$(2^3), (1^1 2^1 3^1)$
(18)	S_5	1	1	$(2^3), (1^2 4^1)$
(19.1)	$AGL_1(7)$	1	1	$(1^1 2^3), (1^1 3^2)$
(19.2) & (19.3)	S_7	1	2 or 3	$(1^1 3^2), (1^1 2^3)$
(20)	$PSL_2(7)$	1	1	$(2^4), (1^2 3^2)$
(21.1)	$ASL_3(2)$	1	1	$(1^4 2^2), (4^2)$
(21.2)	A_8	1	3	$(1^4 2^2), (4^2)$
(22.1)	$AGL_2(3)$	1	1	$(1^3 2^3), (3^3)$
(22.2) & (22.3)	S_9	1	2 or 4	$(1^3 2^3), (3^3)$
(23)	A_{10}	1	2 or 4	$(1^6 2^2), (5^2)$
(24)	A_{10}	1	5	$(2^1 8^1), (1^6 2^2)$

Let $n = \deg(f)$, and suppose $Br(f) = \{\lambda_1, \dots, \lambda_r, \infty\}$. For each λ_i , let $c_i = \sum_{f(a)=f(b)=\lambda_i} (e_f(a) - \gcd(e_f(a), e_f(b)))$. The key to solving the genus equation is to get a lower bound for c_i in terms of n , and to show that if n is large enough ($n \geq 26$), the lower bound is very large, so f has only a few branch points. This will solve the large degree cases, namely, $n \geq 26$ cases; for the small degree cases, we can use a computer program.

For each λ_i , let $a_i = n - \#(\text{distinct roots of } f(X) = \lambda_i)$, and let $b_i = \#(\text{simple roots of } f(X) = \lambda_i)$. Then $\sum_{i=1}^r a_i = n$, by the Riemann-Hurwitz formula on $\mathbb{K}(X)/\mathbb{K}(t)$; and $a_i \geq \frac{n-b_i}{2}$ by the definition of a_i and b_i .

If $\lambda = \infty$, $c_\infty = \sum_{f(a)=f(b)=\lambda} (e_f(a) - \gcd(e_f(a), e_f(b))) = n - 2 \gcd(n, k)$. If $\lambda = \lambda_i$,

we only sum those terms where $e_f(b) = 1$ (in total there are b_i many such b 's), so $c_i \geq b_i \sum_{f(a)=\lambda} (e_f(a) - 1) = b_i a_i$. By combining this information with the fact that $\mathfrak{g}_{xy} \leq 1$, we obtain

$$n + 2 \gcd(n, k) - 2 \geq 2\mathfrak{g}_{xy} - 4 + n + 2 \gcd(n, k) \geq \sum a_i b_i$$

If $k = n/2$, then $2n - 2 \geq \sum a_i b_i$; if $k \neq n/2$, $\gcd(n, k) \leq \frac{n}{3}$, so it follows that $\frac{5}{3}n - 2 \geq \sum a_i b_i$.

The following results provide constraints on a_i , b_i , c_i in the large degree cases, namely, when $n \geq 26$.

Lemma IV.2. *If $n \geq 26$, then for all i , either $b_i \leq 4$ or $b_i \geq n - 4$. If $b_i \geq n - 4$, then $a_i \leq 2$.*

Proof. Note that if $5 \leq b_i \leq n - 5$, then $a_i b_i \geq b_i \frac{n-b_i}{2} \geq 2.5(n - 5) > 2n - 2$, which violates the genus formula. If $b_i \geq n - 4$, and $a_i \geq 3$, then $a_i b_i \geq 3(n - 4) > 2n - 2$, which also violates the genus formula. \square

Lemma IV.3. *If $n \geq 26$, then if $b_i = 0$ and $c_i > 0$, then $c_i \geq \min(\frac{n-1}{2}, \frac{n}{3}) = \frac{n}{3}$.*

Proof. Consider the ramification indices of one such point. If their gcd is 1, then by Lemma III.22, $c_i \geq \frac{n-1}{2}$; if their gcd > 1 but they are not all equal, then by Lemma III.23 $c_i \geq \frac{n}{3}$. \square

Lemma IV.4. *If $n \geq 26$ and $b_i \geq n - 4$, we have the following table. And since $a_i \leq 2$, $f(X) = \lambda_i$ has at least $n - 2$ many distinct roots.*

b_i	a_i	ramification type	c_i
$n - 4$	2	$(1^{n-4}2^2)$	$2n - 8$
$n - 3$	2	$(1^{n-3}3^1)$	$2n - 6$
$n - 2$	1	$(1^{n-2}2^1)$	$n - 2$

Proof. Subject to $a_i \geq \frac{n-b_i}{2}$, the table lists all the possible values of a_i and b_i . The ramification indices and c_i can then be easily calculated. \square

Lemma IV.5. *If $n \geq 26$ and $1 \leq b_i \leq 4$, then a_i , b_i , c_i and the ramification type are as in some row of the following table, unless either $b_i = 1$ and $a_i \geq \frac{n+3}{2}$ or $b_i = 2$ and $a_i \geq \frac{n+2}{2}$.*

b_i	a_i	ramification type	c_i
1	$\frac{n-1}{2}$	$(1^1 2^{\frac{n-1}{2}})$	$\frac{n-1}{2}$
1	$\frac{n}{2}$	$(1^1 3^1 2^{\frac{n-4}{2}})$	$2n - 6$
1	$\frac{n+1}{2}$	$(1^1 4^1 2^{\frac{n-5}{2}})$	$\frac{3}{2}(n - 3)$
2	$\frac{n-2}{2}$	$(1^2 2^{\frac{n-2}{2}})$	$n - 2$
2	$\frac{n}{2}$	$(1^2 4^1 2^{\frac{n-6}{2}})$	$2n - 6$

Proof. Firstly when $b_i = 1$, if $a_i = \frac{n-1}{2}$ or $\frac{n}{2}$, the table contains all possible ramification types: if $a_i = \frac{n+1}{2}$, then ramification type could also be $(1^1 3^1 2^{\frac{n-7}{2}})$, whose $c_i = 3.5n - 20.5 > 2n - 2$; if $a_i = \frac{n+2}{2}$, then ramification type could be $(1^1 5^1 2^{\frac{n-6}{2}})$, $(1^1 3^1 4^1 2^{\frac{n-8}{2}})$, $(1^1 3^3 2^{\frac{n-10}{2}})$, whose $c_i = 3n - 14, 3n - 14, 5n - 44$ respectively, all bigger than $2n - 2$.

When $b_i = 2$, if $a_i = \frac{n-2}{2}$, the table contains all possible ramification types; if $a_i = \frac{n-1}{2}$, then ramification type is $(1^2 3^1 2^{\frac{n-5}{2}})$, whose $c_i = 2.5n - 8.5 > 2n - 2$; if $a_i = \frac{n}{2}$, then ramification type could also be $(1^2 3^2 2^{\frac{n-8}{2}})$, whose $c_i = 4n - 24 > 2n - 2$. If

$a_i = \frac{n+1}{2}$, then ramification type could be $(1^2 2^{\frac{n-11}{2}} 3^3)$, $(1^2 2^{\frac{n-9}{2}} 3^1 4^1)$, and $(1^2 2^{\frac{n-7}{2}} 5^1)$, whose c_i are $\frac{11n-97}{2}$, $\frac{7n-33}{2}$ and $\frac{7n-33}{2}$ respectively, and they are all bigger than $2n-2$ when $n \geq 26$. \square

4.2 Large degree cases: when $n = \deg(f) \geq 26$

Proposition IV.6. *Let $f(x) \in \mathbb{K}(X)$ be a genuine Laurent polynomial of degree $n \geq 26$ with denominator X^k . If $F_f(X, Y)$ is irreducible with genus zero or one, then $n > k$, $\gcd(n, k) = 1$, $\mathfrak{g} = 0$, and $\Lambda(f)$ must have ramification type $\{(1^{n-2} 2^1), (n^1)\}$. In other words, $f(X) = (m_1 + m_0 X) \circ \frac{(X+1)^n}{X^k} \circ (m_2 X^a)$, where $m_1, m_2 \in \mathbb{K}^*$, $m_0 \in \mathbb{K}$, $a = \pm 1$.*

Proof. As always, let $n := \deg(f)$. We determine all plausible ramification types of f which are consistent with the genus of $F_f(X, Y)$ being zero or one. Note that the ramification types we find might not correspond to an indecomposable genuine Laurent polynomial, and even if they did, the corresponding Laurent polynomial might have $F_f(X, Y)$ being reducible.

We firstly deal with the case when f has a finite branch point λ_0 such that $f(X) = \lambda_0$ has a unique root. In this case, it is easy to check that $\Lambda(f)$ has ramification type $\{(1^{n-2} 2^1), (n^1)\}$. At ∞ , the ramification type is $(k^1(n-k)^1)$. Since all ramification indices of f over ∞ and λ_0 are divisible by $\gcd(k, n)$, the fact that f is indecomposable (which follows from our hypothesis that $F_f(X, Y)$ is irreducible) implies that $\gcd(k, n) = 1$, by Lemma III.19.

Now we can use the Riemann-Hurwitz formula to calculate the genus, and easily find $\mathfrak{g} = 0$. In fact, we can find this Laurent polynomial. Writing δ for the unique root of $f(X) = \lambda_0$, we obtain $f(X) = \lambda_0 + d \frac{(X-\delta)^n}{X^k}$ for some $d \in \mathbb{K}^*$, which can be rewritten in the form stated in the proposition.

From now on, we will assume f has no finite branch whose ramification type is (n^1) . We have the following equation from the Riemann–Hurwitz formula:

$$2n - 2 \geq \sum_{b_i \leq 4} a_i b_i + \sum_{b_i \geq n-4} c_i \geq \frac{n-4}{2} \sum_{1 \leq b_i \leq 4} b_i + (n-2) \#\{i : b_i \geq n-4\}$$

It follows that there are at most two values i for which $b_i \geq n-4$.

Case 1: If $b_1, b_2 \geq n-4$ then we must have $b_1 = b_2 = n-2$, $a_1 = a_2 = 1$ and both points have ramification type $(1^{n-2}2^1)$. The above inequality says $2n-2 \geq \frac{n-4}{2} \sum_{1 \leq b_i \leq 4} b_i + 2(n-2)$, this implies for all $i \geq 3$, we must have $b_i = 0$, $\sum_{i \geq 3} c_i = 2$, and $\sum_{i \geq 3} a_i = n-2$.

By Lemma IV.3, if $b_i = 0$, and $c_i > 0$, then $c_i \geq \frac{n}{3} > 2$, so we should have $c_i = 0$. Thus each one has $((\frac{n}{s})^s)$, $a_i = n-s \geq n/2$, so there is only one such point, now $n-s = n-2$ implies $s = 2$, so this point is $((\frac{n}{2})^2)$. Moreover, we have the same thing for ∞ , so the ramification indices are

$$k = n/2, ((\frac{n}{2})^2), (1^{n-2}2^1), (1^{n-2}2^1)$$

in which case $\mathfrak{g} = 0$.

When $n > 2$, $f(X)$ is decomposable by Lemma III.19, so this case cannot occur.

Case 2: suppose that $b_1 \geq n-4$ but $b_i < n-4$ for $i > 1$. If $b_1 \neq n-2$, then $\sum_{i \geq 2} c_i \leq 6$, so $b_i = 0$ for all $i \geq 2$, however any nonzero c_i satisfies $c_i \geq \min(\frac{n-1}{2}, \frac{n}{3}) \geq \frac{26}{3} > 6$, which is a contradiction.

If $b_1 = n-2$ (so $a_1 = 1$, $c_1 = n-2$), then $n \geq \frac{n-4}{2} \sum_{1 \leq b_i \leq 4} b_i$, so $\sum_{1 \leq b_i \leq 4} b_i \leq 2$. Thus for the set $\{1 \leq b_i \leq 4\}$, there are a few possibilities:

1. A single 2, say $b_2 = 2$, then $\frac{n-2}{2} \leq a_2 \leq \frac{n}{2}$ (since $n \geq c_2 \geq a_2 b_2$). By Lemma IV.5, $a_2 = \frac{n-2}{2}$, ramification type is $(1^2 2^{\frac{n-2}{2}})$, and $c_2 = n-2$. Now $\sum_{i \geq 3} a_i = \frac{n}{2}$, $b_i = 0$ for $i \geq 3$, and $\sum_{i \geq 3} c_i = 0$ (if $\mathfrak{g} = 0$) or 2 (if $\mathfrak{g} = 1$). Note when $b_i = 0$ a

nonzero c_i is at least $\frac{26}{3}$, the only chance is $\sum_{i \geq 3} c_i = 0$ with $\mathbf{g} = 0$. Since $c_i = 0$ implies $a_i \geq \frac{n}{2}$, so $\{b_i = 0\}$ has a single point, say b_3 , then $b_3 = 0$ and $a_3 = \frac{n}{2}$, so the ramification type is $(2^{\frac{n}{2}})$.

$$k = n/2, (2^{\frac{n}{2}}), (1^2 2^{\frac{n-2}{2}}), (1^{n-2} 2^1), \mathbf{g} = 0$$

When $n > 2$, $f(X)$ is decomposable, see Lemma III.20.

2. Two 1's, say $b_2 = b_3 = 1$. Then $\frac{n-1}{2} \leq a_2, a_3 \leq \frac{n+1}{2}$. By Lemma IV.5, we must have $a_2 = a_3 = \frac{n-1}{2}$ and both have type $(1^1 2^{\frac{n-1}{2}})$, $c_2 + c_3 = n - 1$. Since n is odd, then $k \neq \frac{n}{2}$, but now $\frac{5}{3}n - 2 \geq c_1 + c_2 + c_3 = 2n - 3$ cannot happen.

3. A single 1, say $b_2 = 1$. Then $a_2 \geq \frac{n-1}{2}$, $c_2 \geq \frac{n-1}{2}$. Now $\sum_{i \geq 3} a_i \leq \frac{n-1}{2}$, $b_i = 0$ for all $i \geq 3$, and $\sum_{i \geq 3} c_i \leq \frac{n+1}{2}$. Since each $a_i < \frac{n}{2}$ for $i \geq 3$, it follows that $c_i > 0$ (so $c_i \geq \frac{n}{3}$) for $i \geq 3$, so there is exactly one such point.

If $k \neq n/2$, then $\frac{5}{3}n - 2 \geq c_1 + c_2 + c_3 \geq (n-2) + \frac{n-1}{2} + \frac{n}{3}$, which is impossible.

So $k = n/2$, and now $a_2 + a_3 = n - 1$, $b_2 = 1$, $b_3 = 0$. However, now $n - 1 = a_2 + a_3 \geq \sum_{i=2,3} \frac{n-b_i}{2} = n - 0.5$, contradiction.

4. No point. Then $\sum_{i \geq 2} a_i = n - 1$ (so at least two points), $b_i = 0$ for all $i \geq 2$.

However, now $\sum_{i \geq 2} a_i \geq 2 \frac{n-b_i}{2} = n$, impossible.

Case 3: when $\#\{b_i \geq n-4\} = 0$. So all $b_i \leq 4$. Since $n = \sum a_i \geq \sum \frac{n-b_i}{2}$, so there are exactly two points, and assume $b_1 \leq b_2 \leq 4$. Now $2n-2 \geq c_1 + c_2 \geq \sum_{i=1,2} b_i \frac{n-b_i}{2}$, rewrite we have $n \leq \frac{b_1^2 + b_2^2 - 2}{b_1 + b_2 - 4}$, we can then easily check that all the cases satisfying $b_1 + b_2 > 4$ violate $n \geq 26$, so $b_1 + b_2 \leq 4$.

Moreover, we have $2n - 2 \geq 2b_1 \frac{n-b_1}{2}$, so $b_1 \leq 2$.

Also, we can get a bound for a_1 . $\frac{n+b_2}{2} = n - \frac{n-b_2}{2} \geq n - a_2 = a_1 \geq \frac{n-b_1}{2}$

1. If $b_1 = 2$, then $b_2 = 2$, and one of a_i must be at most $\frac{n}{2}$, say it is a_1 , by Lemma IV.5, $a_1 = \frac{n-2}{2}$, $c_1 = n - 2$. Now $a_2 = \frac{n+2}{2}$, and $c_2 \geq b_2 a_2 = n + 2$, then $c_1 + c_2 = 2n > 2n - 2$, impossible.

2. If $b_1 = 1$, then $1 \leq b_2 \leq 3$, and $\frac{n+b_2}{2} \geq a_1 \geq \frac{n-1}{2}$.

If $b_2 = 1$, then $\frac{n+1}{2} \geq a_1, a_2 \geq \frac{n-1}{2}$. By lemma IV.5, the only possibility is $a_1 = \frac{n-1}{2}$, $a_2 = \frac{n+1}{2}$, and $c_1 + c_2 = \frac{n-1}{2} + \frac{3}{2}(n-3) = 2n - 5$. Since now n is odd, $k \neq \frac{n}{2}$, we should have $\frac{5}{3}n - 2 \geq 2n - 5$, which is impossible for $n \geq 26$.

If $b_2 = 2$, then $c_2 \geq a_2 b_2 \geq n - 2$, so $c_1 \leq n$. Now since $\frac{n+2}{2} \geq a_1 \geq \frac{n-1}{2}$, by Lemma IV.5, we must have $a_1 = \frac{n-1}{2}$ where $c_1 = \frac{n-1}{2}$. Now $a_2 = \frac{n+1}{2}$, by lemma, $c_2 > 2n - 2$, so this case is impossible.

If $b_2 = 3$, then $c_2 \geq a_2 b_2 \geq \frac{3n-9}{2}$, so $c_1 \leq \frac{n+5}{2}$. Now since $\frac{n+3}{2} \geq a_1 \geq \frac{n-1}{2}$, by Lemma IV.5, we must have $a_1 = \frac{n-1}{2}$ or $\frac{n+3}{2}$, and anyway n is odd and $k \neq n/2$. So $\frac{5}{3}n - 2 \geq c_1 + c_2 \geq \frac{3n-9}{2} + \frac{n-1}{2} = 2n - 5$, which is impossible for $n \geq 26$.

3. If $b_1 = 0$, then $b_2 > 0$, since otherwise $a_1 = a_2 = \frac{n}{2}$ and $c_1 = c_2 = 0$, but we need $c_1 + c_2 > 0$ for the genus formula.

First consider the case when $c_1 > 0$, note that this implies $a_1 > \frac{n}{2}$ and $c_1 \geq \frac{n}{3}$.

If n is odd, and $b_2 \geq 3$, then $\frac{5}{3}n - 2 \geq \frac{n}{3} + 3\frac{n-3}{2}$, which is impossible for $n \geq 26$.

Thus if n is odd, we must have $b_2 \leq 2$.

If $b_2 = 1$, then $\frac{n+b_2}{2} \geq a_1 > \frac{n}{2}$ says $a_1 = \frac{n+1}{2}$, n is odd, and now its ramification type is $(2^{\frac{n-3}{2}} 3^1)$, so $c_1 = \frac{3}{2}(n-3)$. We also have $a_2 = \frac{n-1}{2}$, so $\frac{5}{3}n - 2 \geq c_1 + c_2 \geq \frac{3}{2}(n-3) + \frac{n-1}{2} = 2n - 5$, impossible.

If $b_2 = 2$, then $\frac{n+2}{2} \geq a_1 > \frac{n}{2}$. Since $c_2 \geq a_2 b_2 \geq n - 2$, we need $c_1 \leq n$. By the argument above, a_1 can only be $\frac{n+2}{2}$, now its ramification type is $(2^{\frac{n-6}{2}} 3^2)$ or $(2^{\frac{n-4}{2}} 4^1)$, whose c_1 is $3n - 18$ and $n - 4$ respectively, so the ramification type

should be the latter one. Now $a_2 = \frac{n-2}{2}$, by Lemma IV.5, $c_2 = n - 2$. Now the genus formula becomes $2n + 2\mathbf{g} - 4 = n - 4 + n - 2$, and $\mathbf{g} = -1$, impossible.

If $b_2 = 3$, then n is even and $\frac{n+3}{2} \geq a_1 > \frac{n}{2}$, so $a_1 = \frac{n+2}{2}$. By the argument above, $c_1 \geq n - 4$, so $2n - 2 \geq c_1 + c_2 \geq n - 4 + 3\frac{n-3}{2}$, this is impossible for $n \geq 26$.

If $b_2 = 4$, then $c_2 \geq 2n - 8$, so $c_1 \leq 6$, which is impossible since we assume $c_1 > 0$.

Second consider the case when $c_1 = 0$. Note this point must have the form $((\frac{n}{s})^s)$, and $a_1 = n - s$. Note $n - s = a_1 \leq \frac{n+b_2}{2} \leq \frac{n+4}{2}$. If $s \neq \frac{n}{2}$, then $s \leq \frac{n}{3}$, so $\frac{2n}{3} \leq \frac{n+4}{2}$, which is impossible. Thus $s = a_1 = a_2 = \frac{n}{2}$. Now the genus formula $2n + 2\mathbf{g} - 4 = c_2$ says c_2 is either $2n - 2$ or $2n - 4$. By Lemma IV.5, this is impossible for $b_2 = 1, 2$. If $b_2 = 3$, then the ramification type could be $(1^3 2^{\frac{n-12}{2}} 3^3)$, $(1^3 2^{\frac{n-10}{2}} 3^1 4^1)$ or $(1^3 2^{\frac{n-8}{2}} 5^1)$, and their c_2 are $6n - 54$, $4n - 20$, $4n - 20$ respectively, but none of them could be $2n - 2$ or $2n - 4$ given $n \geq 26$.

□

4.3 Proof of Theorem IV.1

Proof. When $n \geq 26$, we get the first case from Proposition IV.6.

When $n < 26$, it is a finite computation. We can assume that no points in $\Lambda(f)$ has ramification type (n^1) . For each n , there are only finitely many choices for the ramification types of $\Lambda(f)$, for each choice we can use a computer program to check if they satisfy the Riemann–Hurwitz formula. The ramification types of f which make the Riemann–Hurwitz are those listed in Table 4.2 and the following:

1. $(n, k) = (6, 3)$ with ramification types $\{(2^3), (1^2 2^2), (1^4 2^1)\}$ at the three finite branch points. However this case f is decomposable.

2. $(n, k) = (8, 3)$ with ramification types $\{(2^4), (1^2 3^2)\}$ at the two finite branch points. However no rational function satisfies this condition.
3. $n = 9$ and $k = 3, 6$ with ramification types $\{(1^1 2^4), (1^1 2^2 4^1)\}$ at the two finite branch points. However this case f is decomposable.

The cases in Table 4.2 do happen, and in this table we compute the monodromy group and the genus of $F_f(X, Y)$. We list all the corresponding indecomposable Laurent polynomials in Table 4.1. □

CHAPTER V

Indecomposable genuine Laurent polynomial case: Part II

In this chapter we show Theorem V.1, which gives all the indecomposable genuine Laurent polynomials f (up to the equivalent relation defined in Definition III.25) for which $F_f(X, Y)$ is reducible with at least one genus 0 or 1 component.

Our strategy is as follows: $F_f(X, Y)$ is reducible if and only if the monodromy group of $f(X)$ is not doubly-transitive. In [12], Müller gave all the groups which could occur as the monodromy group of an indecomposable genuine Laurent polynomial (we restate the result in Theorem V.2). These groups are S_n , A_n , $S_m \wr S_2$ and a few finite groups of size at most 40, where $n := \deg(f)$ and $m^2 = n$. Among them the groups which are not doubly-transitive are $S_m \wr S_2$ and a few finite groups of small size. The genus of the components of $F_f(X, Y)$ is easy to compute when the monodromy group has small size. The hard case is when the group is $S_m \wr S_2$, and we deal with this case by explicitly finding the ramification type of the corresponding Laurent polynomial and then use this to compute the genus of each component of $F_f(X, Y)$.

Theorem V.1. *Let $f(X) \in \mathbb{K}[X, X^{-1}]$ be an indecomposable genuine Laurent polynomial for which $F_f(X, Y)$ is reducible with an irreducible factor $H(X, Y)$ of genus 0 or 1. Then $f = (c_1X + c_0) \circ h \circ \mu(X)$ for some $\mu(X) = eX^p$ with $c_1, e \in \mathbb{K}^*$*

and $p \in \{1, -1\}$ and $c_0 \in \mathbb{K}$, where the numerator $\hat{H}(X, Y)$ of $H(\mu^{-1}(X), \mu^{-1}(Y))$ divides $F_h(X, Y)$ and in addition \hat{H} (up to multiplication by a nonzero constant in \mathbb{K}^*) and h satisfy one of the following conditions in Table 5.1. The ramification information of the irreducible factors are given in Table 5.2.

Table 5.1: $F_h(X, Y)$ is reducible with a genus 0 or 1 irreducible factor (indecomposable case)

(1) $h(X) = (X + 2)(2X^2 - X - 1)^4/X^3$ and $F_h(X, Y)$ has two irreducible factors. The factor $\hat{H}(X, Y) = X^2Y^4 - X^3Y^3 + X(X^3 - 9X/4 + 1/2)Y^2 + X^2Y/2 + 1/4$ has genus 1.
(2) $h(X) = (X + s - 2)(X^3 - X^2 + (s + 1)X/2 + (s + 1)/2)^3/X^5$ where $s^2 = 5$, and $\hat{H}(X, Y)$ has genus 0 and it is either of the two irreducible factors of $F_h(X, Y)$.
(3) $h(X) = (X + (11 - 5s)/2)^2(X^2 + X - 1)^4/X^5$ where $s^2 = 5$, and $\hat{H}(X, Y)$ is either of the two irreducible factors of $F_h(X, Y)$.
(3.1) $\hat{H}(X, Y)$ has genus 0 and it is the degree-30 factor.
(3.2) $\hat{H}(X, Y)$ has genus 1 and it is the degree-60 factor.
(4) $h(X) = (X + 2)^6(X - s - 3)^3(X + 3s + 7)/X^5$ where $s^2 = 5$, and $\hat{H}(X, Y) = X^3Y + (s + 1)X^2Y^2/2 + (s + 5)X^2Y + (2s + 6)X^2 + XY^3 + (s + 5)XY^2 - (2s + 2)XY + (2s + 6)Y^2$ which has genus 1.

Table 5.2: Ramification information of factors of $F_h(X, Y)$ in Table 5.1

Case	Mon(h)	d	\mathbf{g}	at ∞	first branch point	second branch point
(1)	$S_3 \wr S_2$	4	1	$3[2^2], 6[1^4]$	$1[4], 4^2[\text{each } 1^4]$	$1^3[\text{each } 1^2, 2], 2^3[\text{each } 1^4]$
(2.1)	A_5	3	0	$5^2[\text{each } 1^3]$	$1[3], 3^3[\text{each } 1^3]$	$1^2[\text{each } 1, 2], 2^4[\text{each } 1^3]$
(2.2)	A_5	6	0	$5^2[\text{each } 1^6]$	$1[3^2], 3^3[\text{each } 1^6]$	$1^2[\text{each } 2^3], 2^4[\text{each } 1^6]$
(3.1)	S_5	3	0	$5^2[\text{each } 1^3]$	$2[1, 2], 4^2[\text{each } 1^3]$	$1^4[\text{one } 1^3, \text{three } 1, 2], 2^3[\text{each } 1^3]$
(3.2)	S_5	6	1	$5^2[\text{each } 1^6]$	$2[2^3], 4^2[\text{each } 1^6]$	$1^4[\text{three } 1^2, 2^2, \text{one } 2^3], 2^3[\text{each } 1^6]$
(4)	S_5	3	1	$5^2[\text{each } 1^3]$	$1[3], 3[1, 2], 6[1^3]$	$1^4[\text{three } 1, 2, \text{one } 1^3], 2^3[\text{each } 1^3]$

Here x, y are distinct roots of $h(X) - t$ for which $\mathbb{K}(x, y)$ is the function field of the irreducible factor of $F_h(X, Y)$ stated in Table 4.1, and $d = [\mathbb{K}(x, y) : \mathbb{K}(x)]$. The numbers (not in bracket) in the last three columns are the ramification indices of places in $\mathbb{K}(x)$ over the branch point in $\mathbb{K}(t)$, while the numbers in the bracket are the ramification type of these places in $\mathbb{K}(x, y)/\mathbb{K}(x)$.

5.1 Monodromy groups of indecomposable genuine Laurent polynomials

Theorem V.2 (Müller [12]). *If $f(X) \in \mathbb{K}[X, X^{-1}]$ is an indecomposable genuine Laurent polynomial, then the monodromy group G of f satisfies $G = A_n$, or $G = S_n$, or $G = S_m \wr S_2$ (where $m^2 = n$), or G has size at most 40 and G is one of the groups in Table 5.3 or Table 5.4.*

n	G	n	G
5	$AGL_1(5)$	7	$AGL_1(7)$
8	$A\Gamma L_1(8)$	8	$AGL_3(2)$
9	$A\Gamma L_1(9)$	9	$AGL_2(3)$
16	$C_2^4 \rtimes (C_5 \times C_4)$	16	index 2 in $(S_4 \times S_4) \times C_2$
16	$C_2^4 \rtimes S_5$	16	$A\Gamma L_2(4)$
16	$C_2^4 \rtimes A_7$	16	$A\Gamma L_4(2)$
32	$A\Gamma L_5(2)$		

Table 5.3: Affine group cases

n	G	n	G
6	$PSL_2(5)$	6	$PGL_2(5)$
8	$PSL_2(7)$	8	$PGL_2(7)$
10	A_5	10	S_5
10	$PSL_2(9)$	10	$P\Sigma L_2(9)$
10	M_{10}	10	$P\Gamma L_2(9)$
12	M_{11}	12	M_{12}
14	$PSL_2(13)$	21	$P\Sigma L_3(4)$
21	$P\Gamma L_3(4)$	22	M_{22}
22	$M_{22} \times C_2$	24	M_{24}
40	$PSL_4(3)$	40	$PGL_4(3)$

Table 5.4: Almost simple group cases

Proposition V.3. *If $f(X) \in \mathbb{K}[X, X^{-1}]$ is an indecomposable genuine Laurent polynomial for which $F_f(X, Y)$ is reducible, then the monodromy group of f is one of the following:*

1. $S_m \wr S_2$ (in degree m^2)
2. $C_2^4 \rtimes A_7$ (in degree 16)
3. index 2 in $(S_4 \times S_4) \times C_2$ (in degree 16)
4. A_5 and S_5 (in degree 10)

Proof. A_n and S_n are both doubly transitive. $G = S_m \wr S_2$ acting on $\{(a; b) | a, b \in \{1, \dots, m\}\}$ is not doubly transitive, where by $(a; b)$ we mean an ordered pair with entries a and b . One can easily check that G acting on 2-pairs, in other words $\{(a; b)(c; d) | a, b, c, d \in \{1, \dots, m\}\}$ has two orbits, the first orbit is $\{(a; b)(a; c)\} \cup \{(b; a)(c; a)\}$ with $b \neq c$, the second orbit is $\{(a; b)(c; d)\}$ with $a \neq c$ and $b \neq d$.

We used Magma to check which of the remaining groups are doubly transitive. \square

5.2 Wreath products as monodromy groups

In this section, we prove the following result for the $S_m \wr S_2$ case.

Proposition V.4. *If $f(X) \in \mathbb{K}[X, X^{-1}]$ is an indecomposable genuine Laurent polynomial of degree m^2 with monodromy group $G = S_m \wr S_2$ for some $m \geq 4$, then every irreducible factor of $F_f(X, Y)$ has genus at least 2.*

We will prove the proposition by the following method.

Let $N = S_m \times S_m$ which acting on the set of pairs $\{(a; b) | a, b \in \{1, \dots, m\}\}$, $G = S_m \wr S_2 = \langle \tau_1, \dots, \tau_r \rangle$, $\tau_1 \dots \tau_r = 1$ (see Lemma III.9), and let $E := \{\tau_1, \dots, \tau_r\}$. Note that each τ_i is corresponding to a branch point of f .

Let $\xi \in G$ be a group element which swaps the coordinates of all the pairs, then $G = \langle N, \xi \rangle$, and $[G : N] = 2$. Applying Riemann–Hurwitz to $\mathbb{K}(x)/\mathbb{K}(t)$ gives some constraints on the τ_i 's, which when combined with the above properties of the τ 's force the ramification types of the τ_i 's to be one of a handful of possibilities.

The group G has two orbits on the collection of two-point sets, corresponding to the two irreducible factors of $F_f(X, Y)$. Now since we know the type of all τ_i 's and the two irreducible factors, we can explicitly compute the genus of the two irreducible factors.

5.2.1 The structure of τ_i 's

We will show the following lemma, which gives the structure of τ_i 's.

Lemma V.5. *Besides $(m^1) \times (k^1(m-k)^1)$ corresponding to the branch point ∞ , all the remaining τ_i are exactly*

- (1) one τ from the conjugacy class of ξ , and the other τ from the conjugacy class of $(1^{m-2}2^1 \times 1^m)\xi$
- (2) two τ 's from the conjugacy class of ξ , and one τ of type $(2^1 1^{m-2}) \times (1^m)$ or $(1^m) \times (2^1 1^{m-2})$

We will need a few additional lemmas to prove this lemma.

Lemma V.6. *at least two τ 's are in $G \setminus N$. The τ at ∞ has type $(k^1(m-k)^1) \times m^1 \in N$, where $(k, m) = 1$.*

Proof. Since G is generated by the τ 's, at least one τ is in $G \setminus N$. Since the product of the τ 's is 1, there must be at least two such τ 's. The second claim is from [12, Lemma 3.15]. \square

Let $\Omega_1 = \{(a; b) | a, b \in \{1, \dots, m\}\}$, $\Omega_2 = \{(a; b)(a; c)\} \cup \{(b; a)(c; a)\}$ with $b \neq c$, and $\Omega_3 = \{(a; b)(c; d)\}$ with $a \neq c$ and $b \neq d$. By $(a; b)$ we mean an ordered pair with entries a and b . Let K_i be the fixed field by the stabilizer of Ω_i , and \mathfrak{g}_i be the genus of K_i . The degree (as extension of $\mathbb{K}(t)$) of K_1, K_2, K_3 is the size of corresponding Ω_i 's, which is $n_1 = m^2$, $n_2 = 2m^2(m-1)$ and $n_3 = m^2(m-1)^2$ respectively.

Let \mathfrak{g}_i be the genus of K_i , then $\mathfrak{g}_1 = 0$ because $K_1 = \mathbb{K}(x, t)/(f(x) - t)$. Let $O_i(\tau)$ be the number of orbits of τ acting on Ω_i . By applying the Riemann–Hurwitz formula to $K_i/\mathbb{K}(t)$, we get the following genus formula

Lemma V.7. *Let $E = \{\tau_1, \dots, \tau_r\}$, then*

$$2m^2 - 2 = \sum_{\tau \in E} (m^2 - O_1(\tau))$$

$$m^2 = \sum_{\tau \in E \setminus \{\infty\}} (m^2 - O_1(\tau))$$

Proof. The first comes from $2\mathbf{g}_1 - 2 = n_1(-2) + \sum_{\tau \in E} (m^2 - O_1(\tau))$, and $\mathbf{g}_1 = 0$, $n_1 = m^2$. The second is because, at ∞ , τ has type $(k^1(m-k)^1) \times (m^1)$ where $(m, k) = 1$, and $O_1(\tau) = \sum_{i,j} (i, j) a_i b_j = 2$. \square

Lemma V.8. *For any nontrivial $\tau \in G$, $m^2 - O_1(\tau) \geq m$, and equality holds if and only if $\tau \in N$, with type $(2^1 1^{m-2}) \times (1^m)$ or $(1^m) \times (2^1 1^{m-2})$.*

Proof. Firstly consider $\tau \in N$ with type $(1^{a_1} \cdots m^{a_m}) \times (1^{b_1} \cdots m^{b_m})$, where at least one of a_1, b_1 is less than $m - 2$. Acting on Ω_1 , τ has $a_1 b_1$ fixed points, and all other orbits have length at least two, so $\Omega_1(\tau) \leq a_1 b_1 + \frac{m^2 - a_1 b_1}{2} = \frac{m^2 + a_1 b_1}{2} \leq \frac{m^2 + m(m-2)}{2} = m^2 - m$. Equality holds if and only if $\{a_1, b_1\} = \{m, m-2\}$, which gives us the desired type. Thus the lemma is true for $\tau \in N$.

For $\tau \in G \setminus N$, note $\tau^2 \in N$, and $O_1(\tau) \leq O_1(\tau^2) \leq m^2 - m$. Equality holds if and only if τ^2 has the type $(2^1 1^{m-2}) \times (1^m)$ or $(1^m) \times (2^1 1^{m-2})$. However, this is impossible. Suppose $\tau = (t_1 \times t_2)\xi \in G$ where $t_1, t_2 \in S_m$, then $\tau^2 = t_1 t_2 \times t_2 t_1 \in N$. Since $t_1 t_2 = t_2^{-1} (t_2 t_1) t_2$, $t_1 t_2$ and $t_2 t_1$ are in the same conjugacy class, so they must have the same type, whence it cannot be that one has type $2^1 1^{m-2}$ and the other has 1^m . \square

Lemma V.9. *For any $\tau \in G \setminus N$, $m^2 - O_1(\tau) > \frac{m(m+1)}{2}$ unless τ belongs to one of the following conjugacy classes*

(1) class of ξ , in this case, $m^2 - O_1(\tau) = \frac{m(m-1)}{2}$

(2) class of type $(1^{m-2} 2^1 \times 1^m)\xi$, in this case, $m^2 - O_1(\tau) = \frac{m(m+1)}{2}$

Proof. Say $\tau = (t_1 \times t_2)\xi$. We have $(t_3^{-1} \times t_4^{-1}) \cdot (t_1 \times t_2)\xi \cdot (t_3 \times t_4) = (t_3^{-1} t_1 t_4 \times t_4^{-1} t_2 t_3)\xi$, choose $t_4 = t_2 t_3$, and use \sim to represent conjugacy, this shows $(t_1 \times t_2)\xi \sim (t_3^{-1} t_1 t_2 t_3 \times 1)\xi$. Note that as t_3 runs over all elements in S_m , $t_3^{-1} t_1 t_2 t_3$ runs over all elements in

S_m of the same type as $t_1 t_2$, so it makes sense to say class of a certain type as stated in (2).

Since $O_1(\tau)$ is the same for the conjugacy class of τ , we just need to pay attention to the elements in $(S_m \times 1)\xi$. Pick any element $(t \times 1)\xi$, where (say) t has type $(1^{a_1} \cdots m^{a_m})$, we want to calculate its O_1 . Let $(a; b)$ be an ordered pair, then under the iterated action of $(t \times 1)\xi$, the orbit is

$$(a; b) \mapsto (tb; a) \mapsto (ta; tb) \mapsto (t^2 b; ta) \mapsto (t^2 a; t^2 b) \mapsto \cdots$$

The orbit length is 1 if and only if $a = b$ is fixed by t , so there are a_1 many 1-orbits. The orbit length is 2 if and only if $a \neq b$ are both fixed by t , so there are $\frac{a_1(a_1-1)}{2}$ many 2-orbits. All the remaining orbits have orbit length at least 3, so there are at most $\frac{m^2 - a_1 - a_1(a_1-1)}{3} = \frac{m^2 - a_1^2}{3}$ orbits remaining.

Therefore, $m^2 - O_1((t \times 1)\xi) \geq m^2 - (a_1 + \frac{a_1(a_1-1)}{2} + \frac{m^2 - a_1^2}{3}) = \frac{4m^2 - 3a_1 - a_1^2}{6}$. When $a_1 \leq m - 4$, the right hand side is at least $\frac{4m^2 - 3(m-4) - (m-4)^2}{6} = \frac{3m^2 + 5m - 4}{6} > \frac{3m^2 + 3m}{6} = \frac{m(m+1)}{2}$. Now the remaining cases,

If $a_1 = m - 3$, then $(t \times 1)\xi$ has type $((1^{m-3} 3^1) \times 1^m)\xi$, and its action on the set of ordered pairs has type $(1^{m-3} 2^{\frac{(m-3)(m-4)}{2}} 3^1 6^{m-2})$. Here the number of 1-orbits and 2-orbits comes from $a_1 = m - 3$. All other orbits have length either 3 or 6, where 3-orbit requires $b = ta$, so there are 3 such pairs and they form one 3-orbit. The remaining $6m - 12$ pairs form $m - 2$ many 6-orbits. In this case, $m^2 - O_1 = \frac{m^2 + 3m - 4}{2} > \frac{m^2 + m}{2}$.

If $a_1 = m - 2$, then $(t \times 1)\xi$ has type $((1^{m-2} 2^1) \times 1^m)\xi$. Its action on the set of ordered pairs only has orbit length 1, 2, 4, so the type is $(1^{m-2} 2^{\frac{(m-2)(m-3)}{2}} 4^{m-1})$, and $m^2 - O_1 = \frac{m(m+1)}{2}$.

If $a_1 = m$, then $(t \times 1)\xi = \xi$, its action on the set of ordered pairs has type $(1^m 2^{\frac{m(m-1)}{2}})$, so $m^2 - O_1 = \frac{m(m-1)}{2}$. □

Now we can prove Lemma V.5.

Proof of Lemma V.5. Consider the formula

$$(5.1) \quad m^2 = \sum_{\tau \in E \setminus \{\infty\}} (m^2 - O_1(\tau))$$

from Lemma V.7. By Lemma V.6, at least two τ 's are in $G \setminus N$, then by Lemma V.9, there are exactly two, and their $m^2 - O_1(\tau)$ are either $\frac{m(m-1)}{2}$ and $\frac{m(m+1)}{2}$, or both $\frac{m(m-1)}{2}$. The first choice is case (1); for the second choice, the right side of Equation (5.1) has m left, by Lemma V.8, this space only fits one τ , and τ must have type $(2^1 1^{m-2}) \times (1^m)$ or $(1^m) \times (2^1 1^{m-2})$, this is case (2). \square

5.2.2 Genus of the two components

Lemma V.10. *For the elements involved in E , the following table gives the number of their orbits, when acting on Ω_2 and Ω_3 .*

	$(m^1) \times (k^1(m-k)^1)$	ξ	$(2^1 1^{m-2} \times 1^m)$	$(2^1 1^{m-2} \times 1^m)\xi$
$O_2(\tau)$	$3m - 4$	$m^3 - m^2$	$2m^3 - 5m^2 + 4m$	$m^3 - 4m^2 + 8m - 6$
$O_3(\tau)$	$m(m-1)$	$\frac{m^4 - 2m^3 + 2m^2 - m}{2}$	$m^4 - 4m^3 + 6m^2 - 3m$	$\frac{m^4 - 6m^3 + 20m^2 - 35m + 24}{2}$

Proof. For $(m^1) \times (k^1(m-k)^1)$, acting on $\{(a; b)(a; c) | b \neq c\}$ it has $\frac{mk(k-1)}{[m, k]} + \frac{m(m-k)(m-k-1)}{[m, m-k]} = (k-1) + (m-k-1) = m-2$ orbits, acting on $\{(b; a)(c; a) | b \neq c\}$ it has $\frac{m(m-1)k}{[m, k]} + \frac{m(m-1)(m-k)}{[m, m-k]} = 2m-2$, so $O_2(\tau) = 3m-4$. Now acting on $\Omega_3 = \{(a; b)(c; d) | a \neq c, b \neq d\}$, $O_3(\tau) = \frac{m(m-1)k(k-1)}{[m, k]} + 2\frac{m(m-1)k(m-k)}{[m, k, m-k]} + \frac{m(m-1)(m-k)(m-k-1)}{[m, m-k]} = m(m-1)$.

For the remaining τ , we use Burnside's lemma, which says $\#orbit(\tau) = \frac{1}{|\tau|} \sum_{i=0}^{|\tau|-1} \#Fix(\tau^i)$, where $|\tau|$ is the order of τ .

For $\tau = \xi$, $O_2(\tau) = \frac{1}{2}(2m^2(m-1) + 0) = m^2(m-1)$; $O_3(\tau) = \frac{1}{2}((m(m-1))^2 + m(m-1))$ since $Fix(\xi) = \{(a; a)(c; c) | a \neq c\}$.

For τ with type $(2^1 1^{m-2} \times 1^m)$, choose any element of that type, say $\tau = (12) \times 1$, then $O_2(\tau) = \frac{1}{2}(2m^2(m-1) + (m-2)m(m-1) + (m-2)(m-3)m)$, since $Fix(\tau) = \{(a; b)(a; c) | b \neq c, a \neq 1, 2\} \cup \{(b; a)(c; a) | b \neq c \text{ and both } \neq 1, 2\}$. $O_3(\tau) = \frac{1}{2}((m(m-1))^2 + (m-2)(m-3)m(m-1))$ since $Fix(\tau) = \{(a; b)(c; d) | a \neq c \text{ and both } \neq 1, 2, b \neq d\}$.

For τ with type $(2^1 1^{m-2} \times 1^m)\xi$, choose $\tau = ((12) \times 1)\xi$, now $\tau^2 = (12) \times (12)$, $\tau^3 = (1 \times (12))\xi$, $\tau^4 = 1$. On Ω_2 , τ and τ^3 has no fixed points, $\#Fix(\tau^2) = 2 \cdot (m-2)(m-2)(m-3)$, so $O_2(\tau) = \frac{1}{4}(2m^2(m-1) + 2(m-2)(m-2)(m-3))$. On Ω_3 , $Fix(\tau) = Fix(\tau^3) = \{(a; a)(c; c) | a \neq c \text{ and both } \neq 1, 2\}$, so $\#Fix(\tau) = \#Fix(\tau^3) = (m-2)(m-3)$; $Fix(\tau^2) = \{(a; b)(c; d) | a \neq c, b \neq d \text{ and all } \neq 1, 2\}$, so $\#Fix(\tau^2) = (m-2)^2(m-3)^3$. Therefore $O_3(\tau) = \frac{1}{4}((m(m-1))^2 + 2(m-2)(m-3) + (m-2)^2(m-3)^2)$.

By simplifying the expressions for O_2 and O_3 , we get the desired expressions in the table. □

Now we can prove Proposition V.4.

Proof of Proposition V.4. We have the following formula for $\mathfrak{g}_2, \mathfrak{g}_3$

$$2\mathfrak{g}_i - 2 = (-2)n_i + \sum_{\tau \in E} (n_i - O_i(\tau))$$

where $i = 2, 3$, $n_2 = \#\Omega_2 = 2m^2(m-1)$, $n_3 = \#\Omega_3 = (m(m-1))^2$.

Lemma V.5 gives us the possible configurations of E , and Lemma V.10 gives us the O_i values.

In case (1) of Lemma V.5, one can easily find

$$\begin{aligned} \mathfrak{g}_2 &= \frac{3m^2 - 11m + 12}{2} \\ \mathfrak{g}_3 &= \frac{(m-1)(m-2)(2m-5)}{2} \end{aligned}$$

In case (2) of Lemma V.5, one can easily find

$$\begin{aligned} \mathfrak{g}_2 &= \frac{3m^2 - 7m + 6}{2} \\ \mathfrak{g}_3 &= \frac{(m-2)(2m^2 - 3m - 1)}{2} \end{aligned}$$

It is easy to check that when $m \geq 4$, $\mathfrak{g}_2, \mathfrak{g}_3$ are both > 1 . □

5.3 Proof of Theorem V.1

Proof of Theorem V.1. In Proposition V.3, there are two finite groups, and $S_m \wr S_2$. In Proposition V.4, we showed that when $m \geq 4$, and $G = S_m \wr S_2$, all factors of $F_f(X, Y)$ have genus greater than 1, so we only need to consider $S_2 \wr S_2, S_3 \wr S_2$ and the two finite groups in Proposition V.3. By a computer program, we can get the desired result. □

CHAPTER VI

Decomposable case: indecomposable genuine Laurent polynomial composed with cyclic polynomial

In this chapter, we study the case when the genuine Laurent polynomial f has decomposition $L \circ X^m$, where L is an indecomposable Laurent polynomial of degree at least 3 and $m \geq 2$. We do not consider the $\deg(L) = 2$ case here since in this case all the irreducible factors of $F_L(X^m, Y^m)$ has the form $aXY - b$ where $a, b \in \mathbb{K}^*$ and then $\mathbb{K}(x) = \mathbb{K}(y)$; this case is already covered in case 1 of the proof of Theorem I.5.

In this case, $\frac{f(X)-f(Y)}{X-Y} = \frac{L(X^m)-L(Y^m)}{X^m-Y^m} \frac{X^m-Y^m}{X-Y}$. Each factor in the second part has genus 0, so we just consider when $F_L(X^m, Y^m)$ has an irreducible factor of genus 0 or 1. Note that in this case $F_L(X, Y)$ must have an irreducible factor of genus 0 or 1, so such L must come from Theorem IV.1 or Theorem V.1.

Theorem VI.1. *Let $L \in \mathbb{K}[X, X^{-1}]$ be an indecomposable degree- n ($n \geq 3$) genuine Laurent polynomial having denominator X^k , and let m be an integer with $m \geq 2$. If $F_L(X^m, Y^m)$ has an irreducible factor whose genus $\mathfrak{g}_{x,y}$ satisfies $\mathfrak{g}_{x,y} \leq 1$, then the pair (L, m) is one of these in Table 6.1.*

Proof. First we show that the left square is irreducible. Note that $u = 0$ and $u = \infty$ are both totally ramified in $\mathbb{K}(x)$, and in any case one of $u = 0$ and $u = \infty$ must have an unramified place in $\mathbb{K}(u, v)$ lying over it, so this place will be totally ramified in

Table 6.1: $F_L(X^m, Y^m)$ where L is indecomposable genuine Laurent polynomial

(1) $L = (X - 1)^3(X - 9)/X$ and $m = 2$. This case $F_L(X^2, Y^2)$ has two irreducible factors and each has genus 1.
(2) $L(X) = (c_1X + c_0) \circ \frac{(X+1)^n}{X^k} \circ (c_2X^a)$, where $c_1, c_2 \in \mathbb{K}^*$, $c_0 \in \mathbb{K}$ and $a = \pm 1$.
(2.1) $(m, n, k) = (2, 4, 1)$. This case $F_L(X^m, Y^m)$ has two irreducible factors and each has genus 1.
(2.2) $(m, n, k) = (3, 3, 1)$. $\hat{H}(X, Y)$ is either of the two irreducible factors of $F_L(X^m, Y^m)$: the factor $X^2Y + XY^2 - 1$ has genus 0 and $X^4Y^2 - X^3Y^3 + X^2Y^4 + X^2Y + XY^2 + 1$ has genus 1.
(2.3) $(m, n, k) = (2, 3, 1)$. This case $F_L(X^m, Y^m)$ is irreducible of genus 0.

$\mathbb{K}(x, v)/\mathbb{K}(u, v)$. This implies the left square is irreducible, and the same argument shows the right square is irreducible too.

Now we split into two cases, the case $F_L(X, Y)$ is irreducible and the case $F_L(X, Y)$ is reducible. In either case we will consider the possible m values for which $\mathfrak{g}_{xv} \leq 1$, and then deal with the reducibility of the top square and consider when $\mathfrak{g}_{xy} \leq 1$.

Case 1: $F_L(X, Y)$ is irreducible

In this case, L are the Laurent polynomials from Theorem IV.1. Again we will build a tower of function fields. Let $u = x^m \neq v = y^m$, and $L(u) = L(v) = t$.

First of all \mathfrak{g}_{uv} must be 0. Note that in any case ($k > 1$ or $n - k > 1$ or $k = n - k = 1$), one of 0_u and ∞_u must have an unramified preimage in $\mathbb{K}(u, v)$, then since both of them are totally ramified in $\mathbb{K}(u)$, so there is ramification in $\mathbb{K}(x, v)/\mathbb{K}(u, v)$. If $\mathfrak{g}_{uv} = 1$, then \mathfrak{g}_{xv} will be > 1 , contradiction. The argument above shows that $\mathbb{K}(x, v)/\mathbb{K}(u, v)$ has a totally ramified branch point of index equal to m , so we also know the left square (similarly the right square) must be irreducible. Now we apply Riemann-Hurwitz formula to $\mathbb{K}(x, v)/\mathbb{K}(u, v)$, see when \mathfrak{g}_{xv} could be at most 1.

We firstly look at the cases when $k = \frac{n}{2}$. This case ∞_u and 0_u are all unramified in $\mathbb{K}(u, v)$, so we have $2\mathfrak{g}_{xv} - 2 = (-2)m + 2(n - 1)(m - 1) = 2(n - 2)m - 2(n - 1)$, so $2 \leq m \leq \frac{n-1}{n-2} = 1 + \frac{1}{n-2}$ and the only possibility is $n = 2$ (since n is even), and $\mathfrak{g}_{xv} = 0$. However in our assumption $n > 3$ so we have $k \neq \frac{n}{2}$.

We then look at the cases when $\gcd(k, n - k) = 1$ but $k \neq \frac{n}{2}$. These cases are the $(n, k) = (4, 1)$ and $(n, k) = (6, 1)$ cases from Table 4.1 and the first case in Theorem IV.1 where $n > 2$.

For the cases from Table 4.1, the genus formula is $2\mathfrak{g}_{xv} - 2 = (-2)m + (n - 1)(m - 1) + (m - \gcd(m, n - 1))$. If $n = 6$, then the formula becomes $2\mathfrak{g}_{xv} = 4m - 3 - \gcd(m, 5) \geq 3m - 3 \geq 3$, so $n = 6$ cannot happen. If $n = 4$, this becomes $2m - 3 - \gcd(m, 3) = 0$ or -2 , so $\mathfrak{g}_{xv} = 1$ and $m = 2$ or 3 . If $m = 3$, let P_{uv} be the place over 0_u and ∞_v , then P_{uv} is unramified in $\mathbb{K}(x, v)$ but ramified in $\mathbb{K}(u, y)$, so $\mathfrak{g}_{xy} > \mathfrak{g}_{xv} = 1$. If $m = 2$, then every place in $\mathbb{K}(u, v)$ is either totally ramified or unramified in both $\mathbb{K}(x, v)$ and $\mathbb{K}(u, y)$, so $\mathbb{K}(x, y)$ has genus 1 no matter the top square is reducible or not. This case L is case 7 in Table 4.1.

For the first case in Theorem IV.1 where $n > 2$, the genus formula is $2\mathfrak{g}_{xv} - 2 = (-2)m + (n - 2)(m - 1) + (2m - \gcd(m, k) - \gcd(m, n - k)) = (n - 2)(m - 1) - \gcd(m, k) - \gcd(m, n - k)$. Since $\gcd(k, n - k) = 1$, then at least one of $\gcd(m, k)$ and $\gcd(m, n - k)$ is 1, and the other is at most m , so $0 \geq (n - 2)(m - 1) - (m + 1)$. Then $n \leq \frac{m+1}{m-1} + 2 = 3 + \frac{2}{m-1}$. The possibility are $(m, n) = (2, \leq 5), (3, \leq 4), (\geq 4, \leq 3)$. For the first two possibilities of (m, n) , we get the following solutions: $(m, n, k, \mathfrak{g}_{xv}) = (2, 3, 1, 0), (2, 4, 1, 1), (2, 5, 1, 1), (2, 5, 2, 1), (3, 3, 1, 1), (3, 4, 1, 1)$. For the third possibility of (m, n) , $n = 3$ and $(m, \mathfrak{g}_{xv}) = (4, 1)$.

Among these cases where $\mathfrak{g}_{xv} = 1$ and $m \leq 3$, we require any place in $\mathbb{K}(u, v)$ to be totally ramified or unramified in both $\mathbb{K}(x, v)$ and $\mathbb{K}(u, y)$ no matter the top square is reducible or not. Therefore we need $\frac{[m, n-k]}{n-k} = \frac{[m, k]}{k}$, and the satisfying genus 1 cases are $(m, n, k, \mathfrak{g}_{xv}) = (2, 4, 1, 1), (3, 3, 1, 1)$ and these two cases $\mathfrak{g}_{xy} = 1$ no matter the top square is reducible or not. The remaining $\mathfrak{g}_{xv} = 1$ case is when $(m, n, k) = (4, 3, 1)$. This case the place in $\mathbb{K}(u, v)$ lying over $u = \infty$ and $v = 0$ has

type (2^2) in $\mathbb{K}(x, v)$ but has type (4^1) in $\mathbb{K}(u, y)$, so there is ramification between $\mathbb{K}(x, y)$ and $\mathbb{K}(x, v)$, so $\mathfrak{g}_{xy} > 1$.

Among these cases the only $\mathfrak{g}_{xv} = 0$ case is $(m, n, k, \mathfrak{g}_{xv}) = (2, 3, 1, 0)$. In this case the place in $\mathbb{K}(u, v)$ lying over $u = 0$ and $v = \infty$ is unramified in $\mathbb{K}(x, v)$ but totally ramified in $\mathbb{K}(y, u)$, so the top square must be irreducible and Riemann–Hurwitz shows that $\mathfrak{g}_{xy} = 0$.

Finally we look at the cases when $\gcd(k, n - k) > 1$ and $k \neq \frac{n}{2}$. The only case is case 16 in Table 4.1, where $n = 6$, k is even. Without loss of generality, we can assume $k = 2$. Now the ramification indices of 0_u and ∞_u in $\mathbb{K}(u, v)$ consist of two 2's and six 1's, so the genus formula gives $2\mathfrak{g}_{xv} - 2 = (-2)m + 6(m - 1) + 2(2 - \gcd(2, m)) \geq 4m - 6 \geq 2$, which is impossible.

Case 2: $F_L(X, Y)$ is reducible

In this case, L are the Laurent polynomials from Theorem V.1. For all of these cases, one of 0_u and ∞_u has an unramified preimage in $\mathbb{K}(u, v)$, so we just consider the $\mathfrak{g}_{uv} = 0$ cases, in other words, case 2, 3 and 4. However, for each case, 0_u and ∞_u have at least 6 unramified preimages in $\mathbb{K}(u, v)$ in total, so $2\mathfrak{g}_{xv} - 2 \geq (-2)m + 6(m - 1) = 4m - 6 \geq 2$, which is impossible. \square

CHAPTER VII

Decomposable case: polynomial composed with genuine Laurent polynomial: Part I

In this chapter $f \in \mathbb{K}[X, X^{-1}]$ is a decomposable genuine Laurent polynomial of the form $f = P \circ L$, where $P \in \mathbb{K}[X]$ is an arbitrary polynomial of degree > 1 and $L \in \mathbb{K}[X, X^{-1}]$ is an indecomposable genuine Laurent polynomial. Note that $\frac{f(X)-f(Y)}{X-Y} = \frac{P \circ L(X) - P \circ L(Y)}{L(X) - L(Y)} \frac{L(X) - L(Y)}{X - Y}$, an irreducible factor of genus at most 1 could come from $F_L(X, Y)$ or from $F_P(L(X), L(Y))$. The case $F_L(X, Y)$ is already solved in Theorem IV.1 and Theorem V.1, so in this chapter we consider when $F_P(L(X), L(Y))$ can have an irreducible factor $H(X, Y)$ of genus at most 1.

The main result of this chapter is Theorem VII.1.

Theorem VII.1. *Let $L \in \mathbb{K}[X, X^{-1}]$ be an indecomposable genuine Laurent polynomial, let $P \in \mathbb{K}[X]$ satisfy $\deg(P) > 1$, and pick any irreducible $H(X, Y) \in \mathbb{K}[X, Y]$ of genus 0 or 1. If $H(X, Y)$ divides $F_P(L(X), L(Y))$ then $P = P_2 \circ P_1$ for some polynomials $P_1, P_2 \in \mathbb{K}[X]$, $H(X, Y)$ divides $F_{P_1}(L(X), L(Y))$, and one of the following holds after perhaps replacing H by a constant multiple of itself:*

1. $F_{P_1}(L(X), L(Y))$ is irreducible of genus 1, where $P_1(X) = X^3(X^2 + 5X + 40)$, $\deg(L) = 2$ and $\Lambda(L) = \{\frac{1}{2}(-5 + 3i\sqrt{15})$ or $\frac{1}{2}(-5 - 3i\sqrt{15}), 3\}$.
2. Here $P_1 = X^r(X - 1)^s$ where $\gcd(r, s) = 1$ and $r + s > 3$, and $\deg(L) = 2$. Let

$\Lambda(L) = \{\alpha_1, \alpha_2\}$, and let λ_1, λ_2 be the two simple roots of $L(X) - \frac{r^r(-s)^s}{(r+s)^{r+s}}$, then

(a) $P_1 = (X - a)(X - b)^3$ where $\{a, b\} = \{0, 1\}$, and

i. $\alpha_1 = \lambda_1, \alpha_2 = \lambda_2$, this case the numerator of $F_{P_1}(L(X), L(Y))$ has two factors, each has genus 0.

ii. $\alpha_1 = a, \alpha_2 = \lambda_1$, this case the numerator of $F_{P_1}(L(X), L(Y))$ is irreducible of genus 1.

iii. $L = (X + \frac{1}{16X} + \frac{1}{2}) \circ aX$ for $a \in \mathbb{K}^*$, this case all factor(s) of the numerator of $F_{P_1}(L(X), L(Y))$ have genus 1

(b) $P_1 = (X - a)(X - b)^4$ where $\{a, b\} = \{0, 1\}$, and $\alpha_1 = a, \alpha_2 = \lambda_1$, this case the numerator of $F_{P_1}(L(X), L(Y))$ is irreducible of genus 1

3. Here $P_1 = T_n$, and $H(X, Y)$ is a factor of the numerator of $L(X)^2 + L(Y)^2 - 2L(X)L(Y) \cos(2\pi r/n) - 4 \sin^2(2\pi r/n)$ for some $0 < r < n/2$.

(a) $Br(L) = \{-2, 2, \alpha, \infty\}$ where each branch point has type $(1^1 2^1)$ and $\alpha^2 = 2(1 + \cos(2\pi r/n))$ for some $0 < r < n/2$. This case $F_{T_n}(L(X), L(Y))$ has an irreducible factor $L(X)^2 + L(Y)^2 - 2L(X)L(Y) \cos(2\pi r/n) - 4 \sin^2(2\pi r/n)$ of genus 1.

(b) $L(X) = aX + b/X + c$ where $a, b, c \in \mathbb{K}^*$ and let $\{\beta_1, \beta_2\} := \{2\sqrt{ab} + c, -2\sqrt{ab} + c\}$ be the finite branch points of L . Then $\beta_1 = 2$ or -2 . If $\beta_2^2 \neq 2(1 + \cos(2\pi r/n))$ then $L(X)^2 + L(Y)^2 - 2L(X)L(Y) \cos(2\pi r/n) - 4 \sin^2(2\pi r/n)$ is irreducible of genus 1; otherwise each irreducible factor of $L(X)^2 + L(Y)^2 - 2L(X)L(Y) \cos(2\pi r/n) - 4 \sin^2(2\pi r/n)$ has genus 0.

4. $P_2 = X^n$ for some integer n at least 2, and $H(X, Y)$ is a factor of the numerator of $F_{P_1 \circ L, c}(X, Y)$ where $c \neq 1$ is a n -th root of unity.

Remark VII.2. Due to Theorem VII.1, one can see it is essential to classify when $f(X) - cf(Y)$ has a factor of genus at most 1. We will leave it to Chapter IX and Chapter X.

The strategy is as follows.

We can build a function field tower $\mathbb{K}(x, y) / \{\mathbb{K}(x, v), \mathbb{K}(u, y)\} / \{\mathbb{K}(x), \mathbb{K}(u, v), \mathbb{K}(y)\} / \mathbb{K}(t)$ as shown in Figure 7.1 where all the function fields in this tower have genus at most 1. Note that in this function field tower, $u = L(x)$, $v = L(y)$, $P(u) = P(v) = t$ and $\mathbb{K}(u) \neq \mathbb{K}(v)$. The possibilities for the polynomial P are described in Theorem VII.3.

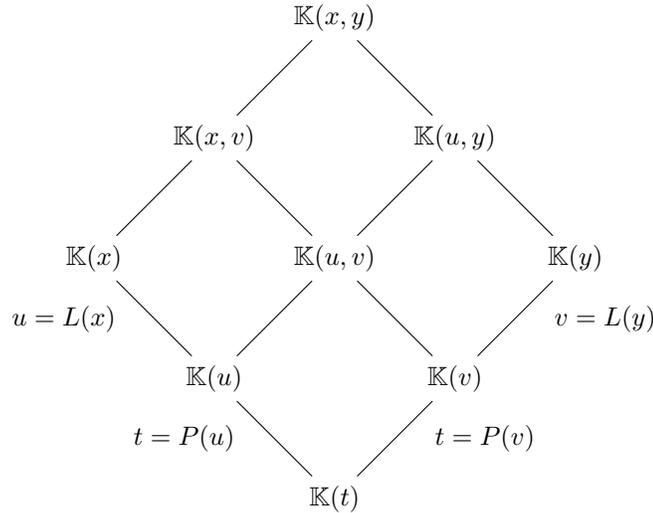


Figure 7.1: Tower of function fields

Theorem VII.3 (Carney–Hortsch–Zieve [2]). *Suppose $P \in \mathbb{K}[X]$ is a polynomial of degree at least 2, then $F_P(X, Y)$ has a genus zero or one factor if and only if P is equivalent to one of the polynomials given below:*

1. *Sporadic cases in Table 7.1. Since we only need their ramification types, we just list the ramification types in the table.*
2. $P_1^n(X)$. *Here $n > 1$ and $F_{P_1, c}(X)$ has an irreducible factor of genus at most 1,*

and $c \in \mathbb{K}^* \setminus \{1\}$ is a n -th root of unity.

3. X^n

4. $T_n(X)$

5. $T_2^n(X)$

6. $X^r(X-1)^s$ where $r > 0$, $s > 0$ and $r + s > 3$

Case	$\deg(P)$	Ramification type of P	Genus of $F_P(X, Y)$
1	4	$(1^2 2^1), (1^2 2^1), (1^2 2^1)$	1
2	5	$(1^2 3^1), (1^2 3^1)$	1
3	5	$(1^2 3^1), (1^1 2^2)$	0
4	5	$(1^1 2^2), (1^3 2^1), (1^3 2^1)$	1
5	6	$(1^2 4^1), (1^2 2^2)$	1
6	6	$(1^1 2^1 3^1), (1^2 2^2)$	1
7	7	$(1^1 2^1 4^1), (1^3 2^2)$	1
8	7	$(1^3 4^1), (1^1 2^3)$	1
9	7	$(1^1 3^2), (1^4 3^1)$	1
10	7	$(1^1 3^2), (1^3 2^2)$	0
11	7	$(2^2 3^1), (1^3 2^2)$	1
12	7	$(1^2 2^1 3^1), (1^1 2^3)$	1
13	8	$(2^1 3^2), (1^4 2^2)$	1
14	8	$(1^2 3^2), (1^2 2^3)$	1
15	9	$(1^1 4^2), (1^5 2^2)$	1
16	9	$(1^3 3^2), (1^1 2^4)$	1
17	10	$(1^1 3^3), (1^4 2^3)$	1

Table 7.1: Sporadic cases

7.1 When P satisfies case 1 or case 6 (where $\gcd(r, s) = 1$) in Theorem VII.3

In this section, case 1 is done in Proposition VII.6, and case 6 (when $\gcd(r, s) = 1$) is done in Proposition VII.7.

The outline is as follows. In Lemma VII.4 we show the left and the right squares cannot be reducible, so we can use Riemann–Hurwitz on the left and right squares, and in Lemma VII.5 we show that $\mathfrak{g}_{uv} = 0$. Then in Proposition VII.6 we deal with case 1 and in Proposition VII.7 we deal with case 6 (when $\gcd(r, s) = 1$).

Lemma VII.4. *Both the left and the right square are irreducible.*

Proof. By symmetry, we just need to show that the left square cannot be reducible.

If the left square is reducible, then by Theorem III.15, there is an intermediate field L' in between $\mathbb{K}(x)$ and $\mathbb{K}(u)$, and M' in between $\mathbb{K}(u, v)$ and $\mathbb{K}(u)$, such that $L'/\mathbb{K}(u)$ and $M'/\mathbb{K}(u)$ have the same Galois closure, and then by Theorem III.16, any place in $\mathbb{K}(u)$ should have the same lcm for its ramification indices in $\mathbb{K}(x)$ and $\mathbb{K}(u, v)$. Consider ∞_u , it is unramified in M' , so lcm= 1, this means it is also unramified in L' , but in L' , it can have at most two preimages, so the only possibility is that ∞_u has two unramified preimages in L' , so $[L' : \mathbb{K}(u)] = 2$. Thus $L'/\mathbb{K}(u)$ is Galois, so that $M' = L'$.

Therefore

1. $d = [\mathbb{K}(u, v) : \mathbb{K}(u)]$ is even.
2. $[M' : \mathbb{K}(u)] = 2$ implies that there are at least two places in $\mathbb{K}(u)$, which are totally ramified in M' , therefore there are at least two places in $\mathbb{K}(u)$ whose ramification indices in $\mathbb{K}(u, v)$ are all even.

Let R be such a place in $\mathbb{K}(u)$, and let S be the place of $\mathbb{K}(t)$ lying under R .

Then exactly one of the ramification indices of S in $\mathbb{K}(u)$ is odd.

Finally, we check that neither case 1 nor case 6 (where $\gcd(r, s) = 1$) satisfies both of these conditions. □

The following lemma shows that \mathfrak{g}_{xv} can only be 0.

Lemma VII.5. $\mathfrak{g}_{uv} = 0$.

Proof. If $\mathfrak{g}_{uv} = 1$, then there will not be any ramifications between $\mathbb{K}(x, v)$ and $\mathbb{K}(u, v)$. So $\deg(L) = 2$, and ∞_u is unramified in $\mathbb{K}(x)$. Note Riemann–Hurwitz

says between $\mathbb{K}(x)$ and $\mathbb{K}(u)$, we still need contribution 2, so there are two places, say Q_1, Q_2 , in $\mathbb{K}(u)$ which are totally ramified in $\mathbb{K}(x)$. To avoid ramification in $\mathbb{K}(x, v)/\mathbb{K}(u, v)$, Q_1, Q_2 must be ramified in $\mathbb{K}(u, v)$ and their ramification indices must be all even. Suppose Q_i is over T_i in $\mathbb{K}(t)$, then T_i is ramified in $\mathbb{K}(v)$, with all indices even except at most one. So there are two places in $\mathbb{K}(t)$, whose ramification indices in $\mathbb{K}(v)$ are all even except at most one, this rules out all the genus 1 cases in case 1 (Table 7.1). For case 6 when $\gcd(r, s) = 1$, $\mathfrak{g}_{uv} = 0$ so we do not need to consider it. \square

The previous lemma shows $\mathfrak{g}_{uv} = 0$, so P is either case 6, or one of sub-case 3 and sub-case 10 of case 1 in Theorem VII.3. The following two lemmas gives all the possibilities of the ramification of L .

Proposition VII.6. *If P is sub-case 3 or sub-case 10 of case 1 in Theorem VII.3, and L is an indecomposable Laurent polynomial such that $F_P(L(X), L(Y))$ has a genus zero or one component, then*

1. $f = P \circ L$ and $F_P(L(X), L(Y))$ is irreducible of genus 1. Here $P(X) = X^3(X^2 + 5X + 40)$, $\deg(L) = 2$ and $\Lambda(L) = \{\frac{1}{2}(-5 + 3i\sqrt{15}) \text{ or } \frac{1}{2}(-5 - 3i\sqrt{15}), 3\}$.

Proof. Let $m = \deg(P)$ and $n = \deg(L)$. Apply Riemann–Hurwitz to $\mathbb{K}(x, v)/\mathbb{K}(u, v)$, then $2\mathfrak{g}_{xv} - 2 = (-2)n + (m - 1)(n - 2) + C$, where $(m - 1)(n - 2)$ is the contribution of places in $\mathbb{K}(u, v)$ over ∞_u , and C is the sum of all other contributions. Here $C = (3 - m)n + 2(m - 1) + 2\mathfrak{g}_{xv} - 2$.

Sub-case 10 of Case 1

In this case $m = 7$, so $C = 12 - 4n + 2\mathfrak{g}_{xv} - 2$. Therefore $n = 2$ or $n = 3$.

If $n = 2$, then $C = 4$ if $\mathfrak{g}_{xv} = 1$; $C = 2$ if $\mathfrak{g}_{xv} = 0$. Since $n = 2$, $\mathbb{K}(x)/\mathbb{K}(u)$ has two totally ramified places, say P_1 and P_2 . Let Q_1, Q_2, Q_3 be the three unramified places

in $\mathbb{K}(u)$ lying over the place in $\mathbb{K}(t)$ which has type $(1^3 2^2)$; let R be the unramified place in $\mathbb{K}(u)$ lying over the place in $\mathbb{K}(t)$ which has type $(1^1 3^2)$. If $P_i = Q_j$ or R , then its contribution to Riemann–Hurwitz is 2; if P_i is any other place, the contribution is 6. Therefore, one of P_i , say P_1 must equal some Q_j and $\mathfrak{g}_{xv} = 1$. Now in order $\mathfrak{g}_{xy} = 1$, regardless of the reducibility of the top square, $\mathbb{K}(x, v)/\mathbb{K}(u, v)$ and $\mathbb{K}(y, u)/\mathbb{K}(u, v)$ must have the same set of branch points. This implies Q_1, Q_2, Q_3 are all totally ramified in $\mathbb{K}(x)$, contradiction.

If $n = 3$, then $C = 0$ and $\mathfrak{g}_{xv} = 1$. Since $n = 3$, $\mathbb{K}(u)$ must have a place which has type $(1^1 2^1)$ in $\mathbb{K}(x)$, however, the place in $\mathbb{K}(x)$ lying over it with index 2 contributes at least 2 to Riemann–Hurwitz by the argument above, so $n \neq 3$.

Sub-case 3 of Case 1

In this case $m = 5$, so $C = 8 - 2n + 2\mathfrak{g}_{xv} - 2$ and $n = 2, 3$ or 4 .

Let Q_1, Q_2 be the two unramified place in $\mathbb{K}(u)$ lying over the place in $\mathbb{K}(t)$ which has type $(1^2 3^1)$; let R be the unramified place in $\mathbb{K}(u)$ lying over the place in $\mathbb{K}(t)$ which has type $(1^1 2^2)$.

When $n = 2$, let P_1, P_2 be the two places in $\mathbb{K}(u)$ which are totally ramified in $\mathbb{K}(x)$. Then P_i contributes 2 if $P_i = Q_1$ or Q_2 , and contributes 0 if $P_i = R$, and contributes 4 in all other cases. When $n = 2$, $C = 4$ if $\mathfrak{g}_{xv} = 1$ and $C = 2$ if $\mathfrak{g}_{xv} = 0$. Therefore if $\mathfrak{g}_{xv} = 0$, we must have $P_1 = R$, P_2 is Q_1 or Q_2 , say $P_2 = Q_1$. Then the top square must be irreducible, since the place in $\mathbb{K}(u, v)$ lying over both Q_1 in $\mathbb{K}(u)$ and Q_2 in $\mathbb{K}(v)$ is ramified in $\mathbb{K}(x, v)$ but unramified in $\mathbb{K}(u, y)$. Now just apply Riemann–Hurwitz on $\mathbb{K}(x, y)/\mathbb{K}(y, u)$, we have $\mathfrak{g}_{x,y} = 1$, so $F_P(L(X), L(Y))$ is irreducible of genus 1. We have the following example:

1. $f = P \circ L$, and $F_P(L(X), L(Y))$ is irreducible of genus 1. Here P is sub-case 3 of

case 1 in Theorem VII.3, so $P(X) = X^3(X^2 + 5X + 40)$ and $\Lambda(P) = \{0, 1728\}$ where 0 has type (1^23^1) and 1728 has type (1^12^2) . $\deg(L) = 2$ and $\Lambda(L) = \{\alpha_1, \alpha_2\}$ where $\alpha_1 = \frac{1}{2}(-5 \pm 3i\sqrt{15})$ is a simple root of $L(X)$ and $\alpha_2 = 3$ is a simple root of $L(X) - 1728$.

If $\mathfrak{g}_{xv} = 1$, then there are two cases. The first scenario is $P_1 = Q_1$ and $P_2 = Q_2$. Since $n = 2$ and $\mathfrak{g}_{xv} = 1$, using the same argument as before, we know that all the three places lying over the place in $\mathbb{K}(t)$ which has type (1^23^1) are totally ramified in $\mathbb{K}(x)$, contradiction. The second scenario is one P_i is either the place in $\mathbb{K}(u)$ of index 3 lying over the place in $\mathbb{K}(t)$ which has type (1^23^1) , or one place in $\mathbb{K}(u)$ of index 2 lying over the place in $\mathbb{K}(t)$ which has type (1^12^2) . In the former case, it is easy to see Q_1, Q_2 are also branch points of L , which is impossible. In the latter case, it is easy to see R in $\mathbb{K}(v)$ has an index of at least 4 in $\mathbb{K}(y)$, which is also impossible.

When $n = 3$, then $C = 2$ if $\mathfrak{g}_{xv} = 1$ and $C = 0$ if $\mathfrak{g}_{xv} = 0$. This case one finite branch point of L must have type (1^12^1) , and this point in $\mathbb{K}(u)$ does not contribute to C if and only if this point is R ; it contributes 2 if and only if it is Q_1 or Q_2 ; otherwise its contribution is bigger than 2. If L has a branch point of type (3^1) , then this point in $\mathbb{K}(u)$ contributes 2 to C if and only if this point is Q_1 or Q_2 ; otherwise its contribution is bigger than 2. Since L have at least two finite branch points, we have C must be positive, and $\mathfrak{g}_{xv} = 1$. Since $C = 2$, the above arguments show that L has two finite branch points: R and Q_1 (in fact, R and one of Q_1, Q_2 , where we use Q_1 here). R has type (1^12^1) and Q_1 has type (3^1) . Regardless the top square is reducible or not, in order $\mathfrak{g}_{xy} = 1$, we must also have Q_2 is a branch point of L of type (3^1) , contradiction.

When $n = 4$, then $C = 0$ and $\mathfrak{g}_{xv} = 1$. Any place in $\mathbb{K}(u)$ with type (4^1) or

$(1^1 3^1)$ in $\mathbb{K}(x)$ has nonzero contribution, so we must have at least two places which has either (2^2) or $(1^2 2^1)$, this kind of place contributes zero if and only if it is R , therefore we cannot get zero contribution from both of them. Thus this case is impossible. \square

Proposition VII.7. *If $P = X^r(X - 1)^s$ where $\gcd(r, s) = 1$ and $r + s > 3$. Let L be an indecomposable genuine Laurent polynomial. If $F_P(L(X), L(Y))$ has a factor of genus at most 1, then $\deg(L) = 2$. Let $\Lambda(L) = \{\alpha_1, \alpha_2\}$, and let λ_1, λ_2 be the two simple roots of $P(X) - \frac{r^r(-s)^s}{(r+s)^{r+s}}$, then*

1. $P = (X - a)(X - b)^3$ where $\{a, b\} = \{0, 1\}$, and

(a) $\alpha_1 = \lambda_1, \alpha_2 = \lambda_2$, this case $F_P(L(X), L(Y))$ has two factors, each has genus 0

(b) $\alpha_1 = a, \alpha_2 = \lambda_1$, this case $F_P(L(X), L(Y))$ is irreducible of genus 1

(c) $L = (X + \frac{1}{16X} + \frac{1}{2}) \circ aX$ for $a \in \mathbb{K}^*$, this case all factor(s) of $F_P(L(X), L(Y))$ have genus 1

2. $P = (X - a)(X - b)^4$ where $\{a, b\} = \{0, 1\}$, and $\alpha_1 = a, \alpha_2 = \lambda_1$, this case $F_P(L(X), L(Y))$ is irreducible of genus 1

Proof. This case $P = X^r(X - 1)^s$, so P has two finite branch points $\{0, \frac{r^r(-s)^s}{(r+s)^{r+s}}\}$. Here 0 has preimages 0 with index r and 1 with index s ; here $\frac{r^r(-s)^s}{(r+s)^{r+s}}$ has preimage $\frac{r}{r+s}$ with index 2, and Q_1, \dots, Q_{r+s-2} with index 1. Therefore in $\mathbb{K}(u, v)/\mathbb{K}(u)$, the type of $u = 0$ is $(1^{r-1}s^1)$, the type of $u = 1$ is $(1^{s-1}r^1)$, the type of Q_i is $(1^{m-3}2^1)$ and for the rest the type is (1^{m-1}) .

Note that $C = (3 - m)n + 2(m - 1) + 2\mathfrak{g}_{xv} - 2 \geq 0$, and $\mathfrak{g}_{xv} = 0, 1$, so $4 \leq m \leq 3 + \frac{4}{n-2}$. So $2 \leq n \leq 6$. If $n > 2$, then m is bounded, this is a finite problem. The only possible large degree case is $n = 2$ for case 6.

When $n = 2$

Suppose the finite branch points of L are α_1 and α_2 . The point α_i contributes (to C) $r - 1 + 2 - \gcd(2, s) = r + 1 - \gcd(2, s)$, $s + 1 - \gcd(r, 2)$, $m - 3$ and $m - 1$, if $\alpha_i = 0, 1$, some Q_j and some any other value respectively.

Now let us look at the minimum of C , it is either $m - 3 + \min\{r, s\} + 1 - \max\{\gcd(2, s), \gcd(s, r)\} \geq m - 3$ or $s + 1 - \gcd(r, 2) + r + 1 - \gcd(s, 2) \geq m - 1$. Therefore $C \geq m - 3$, and then $4 \leq m \leq 5$ if $\mathfrak{g}_{xv} = 0$ and $4 \leq m \leq 7$ if $\mathfrak{g}_{xv} = 1$.

If $\mathfrak{g}_{xv} = 0$ and $m = 4$, we must have $r = 1$ and $s = 3$. Then the contributions $m - 1$, $m - 3$, $r + 1 - \gcd(2, s)$ and $s + 1 - \gcd(r, 2)$ are 3, 1, 1 and 3 respectively. If $\mathfrak{g}_{xv} = 0$ we need $C = 2$, so there are two cases.

1. The two places in $\mathbb{K}(u)$ ramified in $\mathbb{K}(x)$ are the two unramified places lying over the branch point $(\frac{27}{256})_t$ in $\mathbb{K}(t)$. This case $\deg(L) = 2$, $P = X(X - 1)^3$ or $P = X^3(X - 1)$ and $\mathfrak{g}_{xv} = 0$. If the top square is irreducible, then by applying Riemann–Hurwitz to the top square, we can show that $\mathfrak{g}_{xy} < 0$. Therefore the top square must be reducible. This means $F_P(L(X), L(Y))$ has two factors, each one has genus 0. This case is case 1(a) in the proposition.
2. For the two places in $\mathbb{K}(u)$ ramified in $\mathbb{K}(x)$, one place is 0_u , the other is an unramified place lying over the branch point $(\frac{27}{256})_t$ in $\mathbb{K}(t)$. This case $\deg(L) = 2$, $P = X(X - 1)^3$ and $\mathfrak{g}_{xv} = 0$. The top square must be irreducible since the place in $\mathbb{K}(u, v)$ lying over the the two unramified places of $(\frac{27}{256})_t$ is ramified in $\mathbb{K}(x)$ but unramified in $\mathbb{K}(y)$. Using Riemann–Hurwitz we can find $\mathfrak{g}_{xy} = 1$. So this case $F_P(L(X), L(Y))$ is irreducible of genus 1. The same thing is still true if we replace 0_u with 1_u , and use $P = X^3(X - 1)$. This is case 1(b) in the proposition.

If $\mathfrak{g}_{xv} = 0$ and $m = 5$, either $(r, s) = (1, 4)$ or $(r, s) = (2, 3)$. In the first case, the contributions $m - 1$, $m - 3$, $r + 1 - \gcd(2, s)$ and $s + 1 - \gcd(r, 2)$ are 4, 2, 0 and 4 respectively. We need $C = 2$, so there is one example.

1. For the two places in $\mathbb{K}(u)$ ramified in $\mathbb{K}(x)$, one place is 0_u , the other place is unramified over the branch point in $\mathbb{K}(t)$ which has type $(1^3 2^1)$. This case, $P = X(X - 1)^4$, $\deg(L) = 2$ and $\mathfrak{g}_{xv} = 0$. The top is irreducible and $\mathfrak{g}_{xy} = 1$. So this case $F_P(L(X), L(Y))$ is irreducible of genus 1. The same thing is still true if we replace 0_u with 1_u , and use $P = X^4(X - 1)$. This is case 2 in the proposition.

In the second case, the contributions $m - 1$, $m - 3$, $r + 1 - \gcd(2, s)$ and $s + 1 - \gcd(r, 2)$ are 4, 2, 2 and 2 respectively. It is impossible to get $C = 2$.

Now we deal with the case that $\mathfrak{g}_{xv} = 1$, this case m could be 4, 5, 6 or 7, and $C = 4$. As before, we let α_1, α_2 be the two places in $\mathbb{K}(u)$ which is totally ramified in $\mathbb{K}(x)$, then

- $\alpha_1, \alpha_2 \neq Q_i$ when $m \geq 5$ for the following reason: no matter the top square is reducible or not, $\mathbb{K}(x, v)/\mathbb{K}(u, v)$ and $\mathbb{K}(y, u)/\mathbb{K}(u, v)$ have the same set of branch points, then if $m \geq 5$, then there are at least three Q_j 's, and each one must be a branch point of $\mathbb{K}(x)/\mathbb{K}(u)$, which is impossible since $\mathbb{K}(x)/\mathbb{K}(u)$ only has two branch points.
- $\alpha_1, \alpha_2 \neq \frac{r}{r+s}$. For any place in $\mathbb{K}(u, v)$ lying over $u = \frac{r}{r+s}$, it is unramified over $\mathbb{K}(u)$ but totally ramified over some place T in $\mathbb{K}(v)$, and this T must have a ramification index 4 in $\mathbb{K}(y)$, which is impossible.
- α_1, α_2 cannot lie over some place T in $\mathbb{K}(u)$ which is unramified in $\mathbb{K}(x)$. Since otherwise, all the places in $\mathbb{K}(u)$ lying over $\mathbb{K}(t)$ are totally ramified in $\mathbb{K}(x)$,

contradiction.

- If r is even, s is odd, then $\alpha_i \neq 0$. Similarly, if r is odd, s is even, then $\alpha_i \neq 1$.

In the first case, 1_v will have a index at least 4 in $\mathbb{K}(y)$, contradiction. The second case is similar.

When $m \geq 5$, the above conditions imply that $\alpha_1 = 0$, $\alpha_2 = 1$ and r, s are both odd. This can only happen when $m = 6$, where $r = 1$ and $s = 5$. Now contribution $C = (r + 1 - \gcd(2, s)) + (s + 1 - \gcd(2, r)) = 6$, which is bigger than 4, so this cannot happen.

The only case left is $m = 4$, and $(r, s) = (1, 3)$. By the arguments above, we know α_i can only be Q_j ($j = 1, 2$), 0 or 1, and the contribution will be 1, 1, 3. In order to get $C = 4$, we must have some Q_j (say Q_1) equals 1, in this case, it is easy to see $v = 0$ is totally ramified in $\mathbb{K}(y)$, so $Q_2 = 0$. We get one example

1. $P = X(X - 1)^3$, $\deg(L) = 2$ and $\Lambda(L) = \{0, 1\}$. This case $\mathfrak{g}_{xv} = 1$, and $\mathfrak{g}_{xy} = 1$. Note that the same thing is also true for $P = X^3(X - 1)$. This case $L = (X + \frac{1}{16X} + \frac{1}{2}) \circ aX$ for $a \in \mathbb{K}^*$, and all factor(s) of $F_P(L(X), L(Y))$ have genus 1. This is case 1(c) in the proposition.

When $n > 2$

We first consider the case $\mathfrak{g}_{xv} = 0$. This case $4 \leq m \leq 3 + \frac{2}{n-2}$, so we have either $n = 3$, $m = 4, 5$ or $n = 4$, $m = 4$. If $(n, m) = (3, 5)$ or $(4, 4)$, then $C = 0$ and there is no ramification in $\mathbb{K}(x, v)/\mathbb{K}(u, v)$ from the finite branch points of L , but we can show this cannot happen for the following reasons. For $(n, m) = (4, 4)$, the finite branch points of $\mathbb{K}(u, v)/\mathbb{K}(u)$ have one of type (3^1) , two of type $(1^1 2^1)$; but $\mathbb{K}(x)/\mathbb{K}(u)$ has at least two finite branch points, so at least one of them has one unramified place in $\mathbb{K}(u, v)$ lying over it, this implies that $C > 0$, contradiction. For $(n, m) =$

$(3, 5)$, the finite branch points of $\mathbb{K}(u, v)/\mathbb{K}(u)$ have either $\{(4^1), (1^2 2^1), (1^2 2^1)\}$ or $\{(1^1 3^1), (1^2 2^1), (1^2 2^1), (1^2 2^1)\}$, so all of them have unramified place in $\mathbb{K}(u, v)$ lying over except at most one; but $\mathbb{K}(x)/\mathbb{K}(u)$ have at least two finite branch points, so $C > 0$, contradiction.

Thus we just need to consider $(n, m) = (3, 4)$, then $C = 1$. This case the finite branch points of $\mathbb{K}(u, v)/\mathbb{K}(u)$ have type $\{(3^1), (1^1 2^1), (1^1 2^1)\}$; the finite branch points of $\mathbb{K}(x)/\mathbb{K}(u)$ have type $\{(3^1), (1^1 2^1)\}$ or $\{(1^1 2^1), (1^1 2^1), (1^1 2^1)\}$. The second case is impossible since each finite branch point of $\mathbb{K}(x)/\mathbb{K}(u)$ contributes 1 to C . For the first case, the branch point of $\mathbb{K}(x)/\mathbb{K}(u)$ with type (3^1) must have the same type in $\mathbb{K}(u, v)/\mathbb{K}(u)$, so it must be 0_u ; the other branch point must have type $(1^1 2^1)$ in $\mathbb{K}(u, v)$, so it must be λ_u where λ is a simple root of $X(X - 1)^3 - 27/256$ (since $P(X) = X(X - 1)^3$, and $P(r/(r + s)) = P(1/4) = 27/256$). Now let us calculate the genus of \mathfrak{g}_{xy} . First of all, the top square is irreducible since the place in $\mathbb{K}(u, v)$ over $u = \lambda_1$ and $v = \lambda_2$ (where λ_1, λ_2 are the two simple roots of $P(X) = 27/256$) is totally ramified in one of $\mathbb{K}(x, v)$ and $\mathbb{K}(y, u)$ but unramified in the other. Now the Riemann–Hurwitz shows $\mathfrak{g}_{xy} = 4 > 1$, so this case cannot happen. \square

7.2 When P satisfies case 4 in Theorem VII.3

When $P = T_n$, then except the factor $X + Y$ when n is even, each factor of $F_P(X, Y)$ is quadratic of the form $X^2 + Y^2 - 2XY \cos(\frac{2\pi r}{n}) - 4 \sin^2(\frac{2\pi r}{n})$, where $0 < r < \frac{n}{2}$. For the factor $X + Y$, $H(X, Y)$ will be a factor of $L(X) + L(Y)$, and this case will be studied in Theorem IX.6. In this section we just need to consider these quadratic factors.

Let $u = L(x) \neq v = L(y)$, then u, v satisfy $u^2 + v^2 - 2uv \cos(\frac{2\pi r}{n}) - 4 \sin^2(\frac{2\pi r}{n}) = 0$. Treat this equation as an equation in v , then it has a double root if and only if

$u = \pm 2$, and this double root is $v = u \cos(2\pi r/n) \neq \pm u$, so there is no pair (u_0, v_0) such that if $u = u_0, v = v_0$ is a double root and if $v = v_0, u = u_0$ is a double root. In terms of function fields, this means any place in $\mathbb{K}(u, v)$ cannot be totally ramified over $\mathbb{K}(u)$ and $\mathbb{K}(v)$ at the same time.

Note that the left and the right squares are both irreducible, since otherwise $\mathbb{K}(u, v)$ will be a proper intermediate field of $\mathbb{K}(x)/\mathbb{K}(u)$ or $\mathbb{K}(y)/\mathbb{K}(v)$, which violates the indecomposability of L .

Lemma VII.8. *Suppose $[\mathbb{K}(u, v) : \mathbb{K}(u)] = 2$ and $u = \infty$ is unramified in $\mathbb{K}(u, v)$. Let the two finite branch points of $\mathbb{K}(u, v)/\mathbb{K}(u)$ be $u = \alpha_1$ and $u = \alpha_2$. If $\mathbb{K}(x, v)$ has genus at most 1, then the multi-sets of ramification indices of $u = \alpha_1$ and $u = \alpha_2$ in $\mathbb{K}(x)/\mathbb{K}(u)$ and the ramification of any additional finite branch point(s) in $\mathbb{K}(x)/\mathbb{K}(u)$ must be one of these in Table 7.2.*

item	Union of the multisets	ramification of the additionally finite branch point(s)	\mathbf{g}_{xv}
1	$1^2, 2^{m-1}$	$(2^1 1^{m-2})$	0
2	$1^2, 4, 2^{m-3}$	none	0
3	$1, 3, 2^{m-2}$	none	0
4	$1^4, 2^{m-2}$	either $\{(2^1 1^{m-2}), (2^1 1^{m-2})\}$ or $(3^1 1^{m-3})$ or $(2^2 1^{m-4})$ or $(4^1 1^{m-4})$	1
5	$1^4, 4, 2^{m-4}$	$(2^1 1^{m-2})$	1
6	$1^4, 4^2, 2^{m-6}$	none	1
7	$1^4, 6, 2^{m-5}$	none	1
8	$1^3, 3, 2^{m-3}$	$(2^1 1^{m-2})$	1
9	$1^3, 3, 4, 2^{m-5}$	none	1
10	$1^2, 3^2, 2^{m-4}$	none	1

Table 7.2: $T_n \circ L$ case, ramification in $\mathbb{K}(x)/\mathbb{K}(u)$

Proof. There are two branch points of $\mathbb{K}(u, v)/\mathbb{K}(u)$, which are at $u = \alpha_1$ and at $u = \alpha_2$. Consider the Riemann–Hurwitz formula on $\mathbb{K}(x, v)/\mathbb{K}(u, v)$, we have $2\mathbf{g}_{xv} - 2 = (-2)m + 2(m - 2) + C$, where C is the contribution from the places in $\mathbb{K}(u, v)$ not lying over ∞_u . Therefore $C \leq 4$. The set of the ramification indices of all the finite places of $\mathbb{K}(u)$ (other than $u = \alpha_1$ and $u = \alpha_2$) in $\mathbb{K}(x)$ can only have several

1's, along with perhaps one 3 or one 2, or two 2's.

Now consider the ramification indices of $u = \alpha_1$ and $u = \alpha_2$ in $\mathbb{K}(x)/\mathbb{K}(u)$, there are at most 4 odd indices, since each odd index contributes 1 to the Riemann–Hurwitz on $\mathbb{K}(x, v)/\mathbb{K}(x)$, which requires at most 4. Now consider the contribution of $u = \alpha_1$ and $u = \alpha_2$ to the Riemann–Hurwitz of $\mathbb{K}(x, v)/\mathbb{K}(u, v)$, for all the even indices of $u = \alpha_1$ and $u = \alpha_2$ in $\mathbb{K}(x)$ not equal to 2, we have at most one 6, or two 4's.

Therefore, there are only a few possibilities of the ramification types between $\mathbb{K}(x)$ and $\mathbb{K}(u)$, and they are listed in Table 7.2. \square

By Theorem V.2, we know the monodromy group of L of degree m can only be A_m , S_m , $S_{\sqrt{m}} \wr S_2$ or a few small size groups. The following lemma gives the ramification of L when $\text{Mon}(L) = S_{\sqrt{m}} \wr S_2$.

Lemma VII.9. *Let L be an indecomposable genuine Laurent polynomial of degree m with $\text{Mon}(L) = S_{\sqrt{m}} \wr S_2$, then one of the following is true*

1. L has two finite branch points, whose ramification types are $(1^{\sqrt{m}} 2^{\frac{m-\sqrt{m}}{2}})$ and $(1^{\sqrt{m}-2} 2^{\frac{(\sqrt{m}-2)(\sqrt{m}-3)}{2}} 4^{\sqrt{m}-1})$.
2. L has three finite branch points, whose ramification types are $(1^{\sqrt{m}} 2^{\frac{m-\sqrt{m}}{2}})$, $(1^{\sqrt{m}} 2^{\frac{m-\sqrt{m}}{2}})$ and $(1^{m-2\sqrt{m}} 2^{\sqrt{m}})$.

Proof. From Lemma V.5 we know the structure of the group elements corresponding to the finite branch points. For each element, its action on $\{(a, b) | a, b \in \{1, \dots, \sqrt{m}\}\}$ yields an element in S_m , whose set of cycle lengths equals to set of ramification indices of the corresponding branch point. The class of ξ yields $(1^{\sqrt{m}} 2^{\frac{m-\sqrt{m}}{2}})$; the class of $(1^{\sqrt{m}-2} 2^1 \times 1^{\sqrt{m}})\xi$ yields $(1^{\sqrt{m}-2} 2^{\frac{(\sqrt{m}-2)(\sqrt{m}-3)}{2}} 4^{\sqrt{m}-1})$; the class of $(1^{\sqrt{m}-2} 2^1) \times (1^{\sqrt{m}})$ and $(1^{\sqrt{m}}) \times (1^{\sqrt{m}-2} 2^1)$ both yield $(1^{m-2\sqrt{m}} 2^{\sqrt{m}})$. The lemma then directly follows from Lemma V.5. \square

In the following lemma, we study the case when $\text{Mon}(L) = S_{\sqrt{m}} \wr S_2$.

Lemma VII.10. *The monodromy group $\text{Mon}(L)$ cannot be the wreath product $S_{\sqrt{m}} \wr S_2$ where $\deg(L) = m$ is a square.*

Proof. Firstly we rule out all cases in Table 7.2 with index 3 or 6, since by Lemma VII.9, the finite branch points of L cannot have ramification index 3 or 6.

Secondly when there are two finite branch points, they must correspond to ξ and $((1^{\sqrt{m}-2}2^1) \times (1^{\sqrt{m}}))\xi$, so there are $2\sqrt{m} - 2$ many 1's, $\sqrt{m} - 1$ many 4's. In the following cases, we can get the prescribed ramification types:

1. Case 6 with $m = 9$. There are one (1^32^3) at $u = 2$ and one (1^14^2) at $u = -2$ and $\mathfrak{g}_{xv} = 1$. This case $\mathfrak{g}_{xy} > 1$ since the place in $\mathbb{K}(u, v)$ lying over $u = -2$ is unramified in $\mathbb{K}(y, u)$ but ramified in $\mathbb{K}(x, v)$.
2. Case 4 with $m = 4$. There are one (4^1) at $u = 2$, one (1^22^1) at $u \neq \pm 2$ and $\mathfrak{g}_{xv} = 1$. This case $\mathfrak{g}_{xy} > 1$ for the same reason as the case above.
3. Case 2 with $m = 4$. There are one (4^1) at $u = 2$, one (1^22^1) at $u = -2$ and $\mathfrak{g}_{xv} = 0$. This case $k = 2$, and either $\mathfrak{g}_{xy} = 1$ if the top square irreducible, or $\mathfrak{g}_{xy} = 0$ for both factors if the top square reducible. However, one can check in this case the genuine Laurent polynomial L has the form $L = -T_2 \circ (X - 1 + 1/(4X)) \circ (cX \text{ or } c/X)$ for some $c \in \mathbb{K}^*$, so L is decomposable, contradiction. contradicts

Thirdly when there are more than two branch points, there must be three, corresponding to two ξ and one $(1^{\sqrt{m}-2}2^1) \times (1^{\sqrt{m}})$ or $(1^{\sqrt{m}}) \times (1^{\sqrt{m}-2}2^1)$, so there are two $(1^{\sqrt{m}}2^{\frac{m-\sqrt{m}}{2}})$ and one $(1^{m-2\sqrt{m}}2^{\sqrt{m}})$; in total there are m many 1's and m many 2's. In the following cases, we can get the prescribed ramification types:

1. Case 4 with $m = 4$ and $\mathfrak{g}_{xv} = 1$. There are one (2^2) at $u = \alpha_1$ and two $(1^2 2^1)$ at α_2, α_3 . Either $\alpha_1 \neq \pm 2$ and $\{\alpha_2, \alpha_3\} = \{2, -2\}$, or $\alpha_1 \in \{2, -2\}$ and α_2, α_3 both $\neq \pm 2$. In the first case, since it is impossible that there are places in $\mathbb{K}(u, v)$ lying over $u = \alpha_1$ and $v = \alpha_1$, one of the places lying over $u = \alpha_1$ must be ramified in $\mathbb{K}(x, v)$ but unramified in $\mathbb{K}(y, u)$ and then $\mathfrak{g}_{xy} > 1$. In the second case, any place lying over $u = \alpha_2$ must ramified in $\mathbb{K}(x, v)$ but have an unramified place in $\mathbb{K}(y, u)$ lying over it, so $\mathfrak{g}_{xy} > 1$.
2. Case 1 with $m = 4$ and $\mathfrak{g}_{xv} = 0$. There are one $(1^2 2^1)$ at $u \neq \pm 2$ and $\{(1^2 2^1), (2^2)\}$ at $u = \pm 2$. This case $k = 2$, $\mathfrak{g}_{xy} = 0, 1$ if the top square is irreducible and $\mathfrak{g}_{xy} = 0$ for both factors if the top square is reducible. However, by Lemma III.20 any genuine Laurent polynomial of the prescribed ramification is decomposable, so this case cannot happen.

□

Lemma VII.11. *Let P be a nonconstant polynomial, and let L be an indecomposable genuine Laurent polynomial. Let x, y be transcendental over \mathbb{K} , and suppose that $u := L(x)$ and $v := L(y)$ satisfy $t = P(u) = P(v)$. If $[\mathbb{K}(x, v) : \mathbb{K}(x)] = [\mathbb{K}(u, v) : \mathbb{K}(u)] = [\mathbb{K}(u, y) : \mathbb{K}(y)] = 2$ and both $\mathbb{K}(u, y)$ and $\mathbb{K}(x, v)$ have genus at most 1, and $[\mathbb{K}(x, y) : \mathbb{K}(x, v)] < [\mathbb{K}(u, y) : \mathbb{K}(u, v)]$, then $\text{Mon}(L)$ can only be S_m ($m \neq 6$) or A_m ($m \neq 6$) or $S_{\sqrt{m}} \wr S_2$.*

Proof. Theorem V.2 shows that an indecomposable degree- m genuine complex Laurent polynomial has monodromy group G being either S_m or A_m or $S_{\sqrt{m}} \wr S_2$ or one of 35 small groups which can only occur for certain values of m which are all at most 40. In some cases Theorem V.2 also gives the information about the orders of the inertia groups (in the Galois closure) at points over each branch point of $\mathbb{K}(x)/\mathbb{K}(L(x))$.

We use a computer program to determine all these finite groups, for each of them

- (1) which subgroups of G can be a one-point stabilizer when G is monodromy group of an indecomposable Laurent polynomial of the specified degree with the specified orders of inertia groups?
- (2) if L is a Laurent polynomial corresponding to G , and u is transcendental over \mathbb{K} , then for every v not equal to u for which $L(u) = L(v)$, what is $[\mathbb{K}(u, v) : \mathbb{K}(u)]$, what is the Galois group of the Galois closure of $\mathbb{K}(u, v)/\mathbb{K}(u)$, what are the degrees of the intermediate fields between $\mathbb{K}(u, v)$ and $\mathbb{K}(u)$, for each such field what is its ramification over $\mathbb{K}(u)$ and what is the Galois group of its Galois closure over $\mathbb{K}(u)$, and what are the possible ramification types of $\mathbb{K}(u)/\mathbb{K}(L(u))$ and the possible ramification types of $\mathbb{K}(u, v)/\mathbb{K}(u)$?
- (3) if H is an index-2 subgroup of G , can H be imprimitive? If so, what are the sizes of the groups between H and G ?

We first build the list of groups which match the data in items 1 and 3 of Theorem V.2, where when convenient we assume that G is primitive. We get one group from each case, except for $C_2^4 \rtimes S_5$ (in degree 16) which yields two groups.

We then compute all faithful primitive permutation representations of the prescribed degree for each group in the list— there is exactly one such representation for each isomorphism class of groups in the list, except for $C_2^4 \rtimes S_5$ which yields two.

We then check that if $L(X)$ is a degree-6 Laurent polynomial L with monodromy group S_6 or A_6 for which there is a polynomial $P(X)$ and transcendentals x, y over \mathbb{K} such that $u := L(x)$ and $v := L(y)$ satisfy $P(u) = P(v)$ and $[\mathbb{K}(x, v) : \mathbb{K}(x)] = [\mathbb{K}(u, v) : \mathbb{K}(u)] = [\mathbb{K}(u, y) : \mathbb{K}(y)] = 2$ and both $\mathbb{K}(u, y)$ and $\mathbb{K}(x, v)$ have genus at most 1, then $[\mathbb{K}(x, y) : \mathbb{K}(x, v)] = 6$. By the argument we used for other S_n 's and

A_n 's, we just need to deal with the case that both $\mathbb{K}(x, v)/\mathbb{K}(u, v)$ and $\mathbb{K}(u, y)/\mathbb{K}(u, v)$ have ramification $(2^1, 1^4)$, $(2^1, 1^4)$, $(2^2, 1^2)$ (but where the branch points might not be listed in the same order, that is, the $(2^2, 1^2)$ point for one extension does not need to be the $(2^2, 1^2)$ point for the other extension). Note that the existence of a 2-cycle in the monodromy group forces the group to be S_6 rather than A_6 . Now, deal with this case by showing that any point of $\mathbb{K}(u, v)$ which has ramification type $(2, 1^4)$ in $\mathbb{K}(x, v)/\mathbb{K}(u, v)$ would have ramification type (2^3) in $\mathbb{K}(u, y)/\mathbb{K}(y)$ if $Gal(\Omega/\mathbb{K}(u, y))$ were not conjugate to $Gal(\Omega/\mathbb{K}(x, v))$, where Ω is the Galois closure of $\mathbb{K}(u, y)/\mathbb{K}(u, v)$.

We next check that none of the groups on the list can occur for an indecomposable Laurent polynomial L such that there are transcendentals x, v over \mathbb{K} such that $u := L(x)$ satisfies $[\mathbb{K}(x, v) : \mathbb{K}(x)] = [\mathbb{K}(u, v) : \mathbb{K}(u)] = 2$ and $\mathbb{K}(u, v)/\mathbb{K}(u)$ is unramified over $u = \infty$ and $\mathbb{K}(x, v)$ has genus 0 or 1. \square

Proposition VII.12. *If the top square is reducible, then $\mathbb{K}(x, v)$ and $\mathbb{K}(u, y)$ are isomorphic field extensions of $\mathbb{K}(u, v)$. Thus any place in $\mathbb{K}(u, v)$ has the same ramification type in $\mathbb{K}(x, v)$ and $\mathbb{K}(u, y)$.*

Proof. By Lemma VII.11, $\text{Mon}(L)$ can only possibly be S_m ($m \neq 6$) or A_m ($m \neq 6$) or $S_{\sqrt{m}} \wr S_2$ where $m = \deg(L)$. The wreath product case is ruled out in Lemma VII.10.

Now $\text{Mon}(L)$ is either S_m or A_m where $m \neq 6$. Since $[\mathbb{K}(u, v) : \mathbb{K}(u)] = 2$, we know the Galois group of $\mathbb{K}(x, v)/\mathbb{K}(u, v)$ is either $\text{Mon}(L)$ or an index-2 subgroup of $\text{Mon}(L)$, but S_m or A_m does not have index-2 subgroups, so the Galois group of $\mathbb{K}(x, v)/\mathbb{K}(u, v)$ is also S_m or A_m where $m \neq 6$. The Galois group of $\mathbb{K}(x, v)/\mathbb{K}(u, v)$ implies this is a minimal extension, and by symmetry, so is $\mathbb{K}(y, u)/\mathbb{K}(u, v)$. If the top square is reducible, then by Theorem III.15, $\mathbb{K}(x, v)$ and $\mathbb{K}(u, y)$ must have the

same Galois closure, and then since all the index- m subgroups of S_m (respectively, A_m) are conjugate, it follows $\mathbb{K}(x, v)$ and $\mathbb{K}(u, y)$ are isomorphic field extensions over $\mathbb{K}(u, v)$, which implies any place in $\mathbb{K}(uv)$ has the same ramification type in $\mathbb{K}(x, v)$ and $\mathbb{K}(u, y)$. \square

Proposition VII.13. *The top square is irreducible, and $\mathfrak{g}_{xv} = \mathfrak{g}_{uy} = 0$.*

Proof. Assume the top square is reducible, and we apply Proposition VII.12 to Table 7.2. We show that it is impossible that any place in $\mathbb{K}(u, v)$ have the same ramification type in $\mathbb{K}(x, v)$ as in $\mathbb{K}(u, y)$, so this implies the top square is irreducible. Note that this also implies $\mathfrak{g}_{xv} = \mathfrak{g}_{uy} = 0$, since if $\mathfrak{g}_{xv} = 1$, then $\mathfrak{g}_{xy} = 1$ and we have no ramification in $\mathbb{K}(x, y)/\mathbb{K}(x, v)$, but then any place in $\mathbb{K}(u, v)$ would have the same ramification indices in $\mathbb{K}(x, v)$ as in $\mathbb{K}(u, y)$, which is impossible.

Firstly we can rule out cases where there are no additional branch points, since in those cases every branch point of $\mathbb{K}(x, v)/\mathbb{K}(u, v)$ ramifies over $\mathbb{K}(u)$ and hence does not ramify over $\mathbb{K}(v)$, contradiction.

Next, if there is one additional branch point but the union of the multisets is just 1's and 2's then we are done because the additional branch point of $\mathbb{K}(x)/\mathbb{K}(u)$ is some $u = u_0$ which lies under two places of $\mathbb{K}(u, v)$, but these are the only places of $\mathbb{K}(u, v)$ which ramify in $\mathbb{K}(x, v)/\mathbb{K}(u, v)$ so they are also the only places of $\mathbb{K}(u, v)$ which ramify in $\mathbb{K}(u, y)/\mathbb{K}(u, v)$, so (since $v = u_0$ is a branch point of $\mathbb{K}(y)/\mathbb{K}(v)$) these two places must both lie over $v = u_0$, which is not possible.

Next, if there is one additional finite branch point and also the union of the multisets contains a number bigger than 2, then the union of the multisets contains a unique such number, so exactly one of the two places of $\mathbb{K}(u, v)$ which ramifies over $\mathbb{K}(u)$ is in addition a branch point of $\mathbb{K}(x, v)/\mathbb{K}(u, v)$. Call this branch point P . The ramification type of P in $\mathbb{K}(x, v)/\mathbb{K}(u, v)$ is either $(3^1 1^{m-3})$ or $(2^2 1^{m-4})$. But the

other two branch points Q_1, Q_2 of $\mathbb{K}(u, v)$ both lie over the same value $u = u_0$ and both have ramification type $(2^1 1^{m-2})$ in $\mathbb{K}(x, v)/\mathbb{K}(u, v)$. Crucially, this ramification type is different from the ramification type of $\mathbb{K}(x, v)/\mathbb{K}(u, v)$ over P . Then do the same thing for $\mathbb{K}(u, y)/\mathbb{K}(u, v)$ to get that it also has three branch points, with the same ramification types as P, Q_1, Q_2 , and finally it follows that P must ramify over $\mathbb{K}(v)$, contradiction (and also Q_1, Q_2 must lie over the same place of $\mathbb{K}(v)$, giving a second contradiction).

The final possibility is that there are two additional finite branch points of $\mathbb{K}(x)/\mathbb{K}(u)$, which lie under four places of $\mathbb{K}(u, v)$. These four places are the only places of $\mathbb{K}(u, v)$ which ramify in $\mathbb{K}(x, v)/\mathbb{K}(u, v)$ (we are ignoring places of $\mathbb{K}(u, v)$ which lie over $u = \infty$, but those do not matter at all because that also lie over $v = \infty$). Now we have a set of four places of $\mathbb{K}(u, v)$ which all lie over either $u = u_0$ or $u = u_1$, and since they are the only places of $\mathbb{K}(u, v)$ which ramify in $\mathbb{K}(x, v)/\mathbb{K}(u, v)$ (except places over $u = \infty$, it follows that each of these places lies over either $v = u_0$ or $v = u_1$. But that is impossible for the following reasons: first if there are two places in $\mathbb{K}(u, v)$ lying over $u = u_0$ and $v = u_0$, then when $u = u_0$, v has a double root $v = u_0$, then $2u_0 \cos(2\pi r/n) = u_0 + u_0$, but this cannot happen; second if two places in $\mathbb{K}(u, v)$ lying over $u = u_0$ (respectively $u = u_1$) lie over $v = u_0$ and $v = v_1$, then we must have $2u_0 \cos(2\pi r/n) = u_0 + u_1$ and $2u_1 \cos(2\pi r/n) = u_0 + u_1$, and this cannot happen either. \square

By Proposition VII.13, we only need to consider the case when the top square is irreducible and $\mathfrak{g}_{xv} = \mathfrak{g}_{uy} = 0$.

Proposition VII.14. *Let L be an indecomposable genuine Laurent polynomial of degree m with denominator X^k , and T_n be the Chebyshev polynomial of degree $n > 2$. If $H(X, Y)$ is an irreducible factor of genus 0 or 1 of $L(X)^2 + L(Y)^2 - 2L(X)L(Y) \cos(2\pi r/n) -$*

$4\sin^2(2\pi r/n)$ for some $0 < r < n/2$, then one of the following holds

- (1) $Br(L) = \{-2, 2, \alpha, \infty\}$ where each branch point has type $(1^1 2^1)$ and $\alpha^2 = 2(1 + \cos(2\pi r/n))$ for some $0 < r < n/2$. This case $F_{T_n}(L(X), L(Y))$ has an irreducible factor $L(X)^2 + L(Y)^2 - 2L(X)L(Y)\cos(2\pi r/n) - 4\sin^2(2\pi r/n)$ of genus 1.
- (2) $L(X) = aX + b/X + c$ where $a, b, c \in \mathbb{K}^*$ and let $\{\beta_1, \beta_2\} := \{2\sqrt{ab} + c, -2\sqrt{ab} + c\}$ be the finite branch points of L . Then $\beta_1 = 2$ or -2 . If $\beta_2^2 \neq 2(1 + \cos(2\pi r/n))$ then $L(X)^2 + L(Y)^2 - 2L(X)L(Y)\cos(2\pi r/n) - 4\sin^2(2\pi r/n)$ is irreducible of genus 1; otherwise each factor of $L(X)^2 + L(Y)^2 - 2L(X)L(Y)\cos(2\pi r/n) - 4\sin^2(2\pi r/n)$ has genus 0.

Proof. We only consider the case when $\mathfrak{g}_{xv} = 0$, so the ramification type of L can only be the first three cases in table 7.2.

For case 2 and 3 in Table 7.2, suppose P_{uv} over 2_u has contribution in $\mathbb{K}(x, v)$, then P_{uv} must be unramified in $\mathbb{K}(y, u)$, since P_{uv} is over a place in $\mathbb{K}(v)$ which is unramified in $\mathbb{K}(y)$. Now apply Riemann-Hurwitz formula on $\mathbb{K}(x, y)/\mathbb{K}(u, y)$, the two infinity places in $\mathbb{K}(u, v)$ contributes $m - 2\gcd(m, k)$ each to Riemann-Hurwitz, the two places in $\mathbb{K}(u, v)$ which are ramified in $\mathbb{K}(x, v)$ and which are over (± 2) contributes $2m$ each to Riemann-Hurwitz, so the Riemann-Hurwitz formula is now $2\mathfrak{g}_{xy} - 2 = m(-2) + 2(m - 2\gcd(m, k)) + 4m \geq 2m > 2$, so $\mathfrak{g}_{xy} > 1$.

For case 1 in Table 7.2, say α_u has type $(2^1 1^{m-2})$ in $\mathbb{K}(x)$, then there is a place P_{uv} over α_u which lies over a β_v , where $\alpha \neq \beta$, so P_{uv} is ramified in $\mathbb{K}(x, v)$, but unramified in $\mathbb{K}(u, y)$. Now apply Riemann-Hurwitz formula on $\mathbb{K}(x, y)/\mathbb{K}(u, y)$, the two infinity places in $\mathbb{K}(u, v)$ contributes $m - 2\gcd(m, k)$ each to Riemann-Hurwitz. The two places in $\mathbb{K}(u, v)$ lying over α_u both have type $(2^1 1^{m-2})$ in $\mathbb{K}(x, v)$. If both places

are unramified in $\mathbb{K}(y, u)$, then they contribute $2m$, so $2\mathfrak{g}_{xy} - 2 = m(-2) + 2(m - 2\gcd(m, k)) + 2m$, so $\mathfrak{g}_{xy} = m + 1 - 2\gcd(m, k)$. The only solution is $k = m/2$ and $\mathfrak{g}_{xy} = 1$. This case (α, α) is not solution to $u^2 + v^2 - 2uv \cos(2\pi r/n) - 4 \sin^2(2\pi r/n) = 0$, so $\alpha^2 \neq 2(1 + \cos(2\pi r/n))$.

If $\alpha^2 = 2(1 + \cos(2\pi r/n))$, then the place in $\mathbb{K}(u, v)$ lying over $u = \alpha$ and $v = \alpha$ has ramification type $(1^{m-2}2^1)$ in $\mathbb{K}(x, v)$ and $\mathbb{K}(u, y)$, so the Riemann–Hurwitz is now $2\mathfrak{g}_{xy} - 2 = m(-2) + 2(m - 2\gcd(m, k)) + (2m - 2)$, so $\mathfrak{g}_{xy} = m - 2\gcd(m, k)$, this case $(m, k, \mathfrak{g}_{xy}) = (3, 1, 1)$ or $(m, k, \mathfrak{g}) = (m, m/2, 0)$.

However, for all the genuine Laurent polynomial we find above except the case where $(m, k) = (3, 1)$, all of them have ramification $\{(1^{m-2}2^1), (1^1 2^{\frac{m-2}{2}}), (2^{\frac{m}{2}})\}$ at the finite branch points and $((\frac{m}{2})^2)$ at ∞ . By Lemma III.20 all such Laurent polynomials are decomposable unless $m = 2$. Therefore we get the following cases,

- (1) $(m, k) = (3, 1)$. This case $Br(L) = \{-2, 2, \alpha, \infty\}$ where all the branch points have type $(1^1 2^1)$ and $\alpha^2 = 2(1 + \cos(2\pi r/n))$ for some $0 < r < n/2$. This case $F_{T_n}(L(X), L(Y))$ has an irreducible factor $L(X)^2 + L(Y)^2 - 2L(X)L(Y) \cos(2\pi r/n) - 4 \sin^2(2\pi r/n)$ of genus 1.
- (2) $\deg(L) = 2$ which has one of 2 and -2 as a branch point. This case all irreducible factors of $L(X)^2 + L(Y)^2 - 2L(X)L(Y) \cos(2\pi r/n) - 4 \sin^2(2\pi r/n)$ have genus at most 1. Let $L(X) = aX + b/X + c$, then the two finite branch points are $\{\pm 2\sqrt{ab} + c\}$. This set is not $\{\pm 2\}$ if and only if $c \neq 0$. If $L(X)^2 + L(Y)^2 - 2L(X)L(Y) \cos(2\pi r/n) - 4 \sin^2(2\pi r/n)$ has genus 1, then it must be irreducible and $\alpha^2 \neq 2(1 + \cos(2\pi r/n))$ where α is the finite branch point not equal to ± 2 ; in all other cases all of its irreducible factor(s) have genus 0.

□

7.3 Proof of Theorem VII.1

Proof of Theorem VII.1. We build the function field tower as in Figure 7.1. Since $\mathfrak{g}_{xy} \leq 1$, we must have $\mathfrak{g}_{uv} \leq 1$, thus $\mathbb{K}(u, v)$ corresponds to an irreducible factor of $F_P(X, Y)$ of genus at most 1. All such polynomials P are given in Theorem VII.3. In the case where P is a power of another polynomial, say $P = P_1^n$ where $n > 1$, we choose the integer n as large as possible, then

$$F_P(L(X), L(Y)) = F_{P_1}(L(X), L(Y)) \cdot \prod_{c^n=1, c \neq 1} (P_1(L(X)) - cP_1(L(Y))).$$

If $H(X, Y)$ is a factor of one of the polynomials $P_1(L(X)) - cP_1(L(Y))$, then it falls into case 5 in the theorem. Therefore from now on we can assume P is not a power of another polynomial, and thus P can only be one of the polynomials in Table 7.1, T_n or $X^r(X-1)^s$ where $\gcd(r, s) = 1$ and $r + s > 3$ (When $r + s = 2$ or $r + s = 3$, $X^r(X-1)^s$ is T_2 or T_3 up to composition with linear polynomials at the left side and at the right side).

If P is in Table 7.1, then in Lemma VII.5 we proved $\mathfrak{g}_{uv} = 0$, so P can only be case 3 or case 10 in the table. This case is solved in Proposition VII.6, and it is case 1 in the theorem.

If P is $X^r(X-1)^s$ where $\gcd(r, s) = 1$ and $r + s > 3$, this case is solved in Proposition VII.7, and it is case 2 in the theorem.

If P is T_n , then all factors of $F_P(X, Y)$ are quadratic except $X + Y$ when n is even. Now $H(X, Y)$ may be from $L(X) + L(Y)$ (using the factor $X + Y$ of $F_P(X, Y)$) and this is case 4. We then just need to consider the case where $\mathbb{K}(u, v)$ corresponds a quadratic factor of $F_P(X, Y)$.

In Lemma VII.10, we show that the monodromy group of L cannot be the wreath product. Then we consider the monodromy groups listed in Theorem V.2 (for $S_m \wr S_2$,

just consider the case $\deg(L) = m^2 > 4$). In Proposition VII.13, using these groups, we show that the top square must be irreducible and $\mathfrak{g}_{xv} = \mathfrak{g}_{uy} = 0$, then we solve the case in Proposition VII.14. This case is case 3(b) in the theorem. \square

CHAPTER VIII

Decomposable case: polynomial composed with genuine Laurent polynomial: Part II

In this chapter we assume the genuine Laurent polynomial f is decomposable, in the form that $f = P \circ L \circ X^m$, where $P \in \mathbb{K}[X]$ is an arbitrary polynomial of degree > 1 , $L \in \mathbb{K}[X, X^{-1}]$ is an indecomposable genuine Laurent polynomial and $m \geq 2$ is a positive integer. For $f = P \circ L \circ X^m$, $\frac{f(X)-f(Y)}{X-Y} = \frac{P \circ L(X^m) - P \circ L(Y^m)}{X^m - Y^m} \frac{X^m - Y^m}{X - Y}$ and in this chapter we study when $F_{P \circ L}(X^m, Y^m)$ has a genus zero or one irreducible factor. Note that $F_{P \circ L}(X, Y)$ necessarily has a genus zero or one irreducible factor, so that the pair (P, L) must be listed in Theorem VII.1.

Proposition VIII.1. *Let $P \in \mathbb{K}[X]$ be any polynomial of degree at least 2, let $L \in \mathbb{K}(X)$ be any genuine Laurent polynomial and let m be an integer at least 2. If $F_{P \circ L}(X^m, Y^m)$ has an irreducible factor $H(X, Y)$ of genus at most one, then one of the following holds:*

1. $P = T_n$ where n is even and $F_{L, -1}(X^m, Y^m)$ has an irreducible factor of genus 0 or 1. This case $H(X, Y)$ is this irreducible factor.
2. $P = P_1^n$ where $n > 1$ and $H(X, Y)$ is a factor of $P_1(L(X^m)) - cP_1(L(Y^m))$ where $c \neq 1$ is a n -th root of unity.

Proof. Note that $F_P(X, Y)$ must have a genus zero or one factor, so $P \circ L$ is one of those in Theorem VII.1. Let r be a root of $X^m - x$ and s be a root of $X^m - y$, then we want to know when $\mathbb{K}(r, s)$ has genus zero or one.

For the first two cases in Theorem VII.1, since $\deg(L) = 2$ we know that $x = 0$ and $x = \infty$ are both unramified in $\mathbb{K}(x, y)$ but totally ramified in $\mathbb{K}(r)$, so $[\mathbb{K}(r, y) : \mathbb{K}(x, y)] = [\mathbb{K}(r) : \mathbb{K}(x)]$. If $\mathfrak{g}_{xy} = 1$ then \mathfrak{g}_{ry} must be bigger than 1. If $\mathfrak{g}_{xv} = 0$ then the case is case 2(a) in Theorem VII.1, here $[\mathbb{K}(x, y) : \mathbb{K}(x)] = [\mathbb{K}(x, v) : \mathbb{K}(x)] = 3$, so there are 6 unramified places in $\mathbb{K}(x, y)$ lying over $x = 0$ or $x = \infty$. By Riemann–Hurwitz, $2\mathfrak{g}_{ry} - 2 = (-2)m + 6(m - 1) = 4m - 6$ so $\mathfrak{g}_{ry} = 2m - 2 > 1$. Therefore we get no examples from the first two cases of Theorem VII.1.

For case 3 in Theorem VII.1 $\mathbb{K}(x, y)$ has genus 1 and there is at least one place in $\mathbb{K}(x, y)$ which is unramified over $x = 0$ or $x = \infty$, so $[\mathbb{K}(r, y) : \mathbb{K}(x, y)] = [\mathbb{K}(r) : \mathbb{K}(x)]$ and therefore $\mathfrak{g}_{rs} \geq \mathfrak{g}_{ry} > 1$.

□

CHAPTER IX

The case that $f(X) - cf(Y)$ is irreducible

In this chapter and the next chapter we study the problem: when can $F_{f,c}(X, Y)$ (the numerator of $f(X) - cf(Y)$) have a genus 0 or 1 component, where $f(X) \in \mathbb{K}[X, X^{-1}]$ is a genuine Laurent polynomial and $c \in \mathbb{K}^* \setminus \{1\}$. This is essential since we reduced some cases in Theorem VII.1 to this problem.

In this chapter we address this problem for the case that $f(X) - cf(Y)$ is irreducible. We use the Riemann-Hurwitz formula to get the possible ramification types of f , and find the matching patterns between the branch points of f and cf that makes $F_{f,c}(X, Y)$ have genus at most 1. Note that here f is not required to be indecomposable.

This chapter is organized in the following way. In the first section we establish the Riemann–Hurwitz formula and define what we mean by reduced sequence and matching sequence. In the next section we state Theorem IX.6, the main result of this chapter, which gives all the genuine Laurent polynomials f for which $F_{f,c}(X, Y)$ is irreducible of genus at most 1. In the subsequent sections we prove Theorem IX.6.

9.1 Riemann-Hurwitz genus formula and reduced sequences

First of all we introduce some notations, formulas and inequalities related to the genus of $f(X) - cf(Y)$.

Let $\Lambda_c = \Lambda(f) \cup \Lambda(cf)$, in other words, the union of the finite branch points of f and cf . Let $n := \deg(f)$ and \mathbf{g} be the genus of $F_{f,c}(X, Y)$, then we have the following formula

$$(9.1) \quad \sum_{\lambda \in \Lambda_c} \sum_{f(a)=cf(b)=\lambda} (e_f(a) - \gcd(e_f(a), e_{cf}(b))) = n + 2 \gcd(n, k) + 2\mathbf{g} - 2.$$

By adding this formula to the corresponding formula in which the roles of f and cf are switched, we obtain the following formula.

$$(9.2) \quad \sum_{\lambda \in \Lambda_c} \sum_{f(a)=cf(b)=\lambda} (e_f(a) + e_{cf}(b) - 2 \gcd(e_f(a), e_{cf}(b))) = 2n + 4 \gcd(n, k) + 4\mathbf{g} - 4.$$

Moreover, we have

$$(9.3) \quad \sum_{\lambda \in \Lambda(f)} \sum_{f(a)=\lambda} (e_f(a) - 1) = \sum_{\lambda \in \Lambda(cf)} \sum_{cf(b)=\lambda} (e_{cf}(b) - 1) = n.$$

All of these formulas are derived from Riemann-Hurwitz formula (See the preliminaries in chapter III for the background). A simple example is provided in Example IX.2 to show how Equation 9.1 works (Equation 9.2 will work the same way). We will define matching sequence and reduced sequence later, where the idea behind is illustrated in Example IX.2.

Definition IX.1. Given two places P, P' , with ramification type Q and Q' respectively, define

$$C(P, P') := C(Q, Q') := \sum_{\substack{\text{index } a \in Q \\ \text{index } b \in Q'}} (a - \gcd(a, b)).$$

Example IX.2. Let $c \neq 1$ be a 3-rd root of unity, and suppose $f(X)$ is ramified at $\lambda = 1$. On the left side of Equation 9.1, we will consider $\lambda, \lambda/c, \lambda/c^2, \dots$ until it becomes 1 again, in this case, we consider $1, 1/c, 1/c^2, 1/c^3 = 1$.

λ	$e_f(a)$'s	$e_{cf}(b)$'s
1	ramification indices of $f(X) = 1$	ramification indices of $f(X) = 1/c$
$1/c$	ramification indices of $f(X) = 1/c$	ramification indices of $f(X) = 1/c^2$
$1/c^2$	ramification indices of $f(X) = 1/c^2$	ramification indices of $f(X) = 1/c^3 = 1$

Let P_0, P_1, P_2 be the places corresponding to $1, 1/c, 1/c^2$ respectively, and Q_0, Q_1, Q_2 be the ramification indices of $f(X) = 1, 1/c, 1/c^2$. The matching in the table contributes $C(Q_0, Q_1) + C(Q_1, Q_2) + C(Q_2, Q_0)$ to the left side of Equation 9.1.

Let us furthermore consider the case that $1/c$ and $1/c^2$ are both unramified for $f(X)$, so $Q_1 = Q_2 = (1^n)$. In this case, $C(Q_0, (1^n)) + C((1^n), (1^n)) + C((1^n), Q_0) = C(Q_0, (1^n)) + C((1^n), Q_0) = C(Q_0, Q_2) + C(Q_2, Q_0)$ since $C((1^n), (1^n)) = 0$. Note that this means we can drop Q_1 and replace every remaining Q_1 in the sum with Q_2 . Now only Q_0, Q_2 are left, and for these two places, either f or cf is ramified. At the place Q_1 we dropped, neither f nor cf is ramified.

Example IX.2 illustrates the procedure to get the left side of Equation 9.1, and the idea of the definition of matching sequence and reduced sequence, defined as follows.

Definition IX.3 (Matching sequence/reduced sequence). For any $\lambda \in \mathbb{K}^*$, we get the sequence $\lambda, \lambda/c, \lambda/c^2, \dots, \lambda/c^n$ (where n is the smallest positive integer such that $c^n = 1$). Let Q_i be the ramification type of $f(X) = \lambda/c^i$, then the above sequence yields the sequence of ramification types $\mathcal{S} := Q_0 \rightarrow Q_1 \rightarrow \dots \rightarrow Q_{n-1} \rightarrow Q_n = Q_0$. We call this sequence the *Matching sequence*, and say the place P_i corresponding to λ/c^i is the *Underlying place* of Q_i . The matching sequence contributes $C(\mathcal{S}) := \sum_{i=0}^{n-1} C(Q_i, Q_{i+1})$ to the left side of Equation 9.1.

If the matching sequence has consecutive (1^n) 's, among them we keep the last

(1^n) and its underlying place, and remove the remaining (1^n) 's and their underlying places. The resulting sequence will have no consecutive (1^n) 's, and we call this sequence *Reduced sequence* of \mathcal{S} , write as \mathcal{S}^{red} .

Note that in this reduction process, what we in fact did is we kept all places where either f or cf is ramified, and removed all places where neither f nor cf is ramified, so all the places in the reduced sequence are from Λ_c .

Moreover, we have $C(\mathcal{S}) = C(\mathcal{S}^{red})$ since $C((1^n), (1^n)) = 0$.

The following lemma will be useful to estimate $C(Q_i, Q_{i+1})$.

Lemma IX.4. $C(Q, Q') \geq A(Q)B(Q')$ where $A(Q) = n - \#$ of indices in Q , and $B(Q) = \#$ of 1's in Q .

Proof. Suppose Q has ramification indices (a_i) 's, and Q' has ramification indices (b_j) 's, then $C(Q, Q') = \sum_i \sum_j (a_i - \gcd(a_i, n_j)) \geq \sum_i \sum_{b_j=1} (a_i - 1) = A(Q)B(Q')$, since $\sum_i (a_i - 1) = n$ by Riemann-Hurwitz. \square

9.2 Main result: Classification of f for which $F_{f,c}(X, Y)$ is irreducible of genus at most 1

Let $P(\lambda)$ be the place in $\mathbb{K}(t)$ corresponding to λ . Let $S(f, c) = \{P(c^i \lambda) | \lambda \in \Lambda(f), i \geq 0\}$, then $S(f, c)$ can be divided into several disjoint sets of the form $\{c^i \lambda | i \geq 0\}$, and for each set, one can form a matching sequence. Form one matching sequence for each set, and say all the sequences we get are $\mathcal{S}_1, \dots, \mathcal{S}_m$, then Equation 9.1 becomes

$$2n \geq n + 2 \gcd(n, k) + 2\mathbf{g} - 2 = \sum_{i=1}^m C(\mathcal{S}_i) = \sum_{i=1}^m C(\mathcal{S}_i^{red})$$

If we define \mathcal{S}_i^{-1} to be the reversed sequence of \mathcal{S}_i , then Equation 9.2 becomes

$$4n \geq 2n + 4 \gcd(n, k) + 4\mathbf{g} - 4 = \sum_{i=1}^m (C(\mathcal{S}_i) + C(\mathcal{S}_i^{-1})) = \sum_{i=1}^m (C(\mathcal{S}_i^{red}) + C((\mathcal{S}_i^{-1})^{red}))$$

Why do we define a reduced sequence? It is in fact a very natural definition.

1. $\{\lambda | P(\lambda) \text{ is in a reduced sequence}\} = \Lambda_c = \Lambda(f) \cup \Lambda(cf)$. This means the reduced sequences are formed by the places in Λ_c , and all the reduced sequences use all the places in Λ_c .
2. Solving Equation 9.2, Equation 9.3 and Equation 9.1 is the same as finding all the reduced sequences.

Why do we use a matching sequence, if what we want is reduced sequence?

1. It naturally arises in the thinking process, as in Example IX.2.
2. Reduced sequence will not tell us the order of c , if the length is l , then the order of c is at least $l - 1$. In contrast, a matching sequence has length either 1 (if the underlying place is $P(0)$), or $n + 1$ (where n is the order of c)

Remark IX.5. From now on, all sequences are considered REDUCED.

Our goal here is to get all possible configurations of the reduced sequences under the constraint of Equation 9.1, Equation 9.2 and Equation 9.3. A few inequalities (Lemma III.22, Lemma III.23 and Lemma III.24) from the preliminaries in Chapter III will be used to estimate the size of $|\Lambda_c|$.

In this chapter, we prove Theorem IX.6. For the definition of strongly equivalent, the reader can refer to Definition III.25.

Theorem IX.6. *Let $f(X) \in \mathbb{K}[X, X^{-1}]$ be a genuine Laurent polynomial of degree n with denominator X^k , and $c \in \mathbb{K} \setminus \{1\}$. If $F_{f,c}(X, Y)$ is irreducible with genus 0 or 1, then f satisfies one of the following.*

(1) f is strongly equivalent to $\frac{(X+1)^n}{X^k}$ where $n > k$, $\gcd(n, k) = 1$, and $c \neq 1$. This case $F_{f,c}(X, Y)$ has genus 0.

(2) f has degree at most 6 and (f, c) satisfies one row of conditions in Table 9.1.

Table 9.1: $F_{f,c}$ is irreducible of genus at most 1

item	n	k	\mathfrak{g}	order of c	reduced sequences
(1)	2	1	0	≥ 3	$(1^2) \rightarrow (2^1) \rightarrow (2^1) \rightarrow (1^2)$
(2)	2	1	1	≥ 2 ≥ 5	$(1^2) \leftrightarrow (2^1), (1^2) \leftrightarrow (2^1)$ or $(1^2) \rightarrow (2^1) \rightarrow (1^2) \rightarrow (2^1) \rightarrow (1^2)$
(3)	3	1, 2	0	4	$(1^1 2^1) \rightarrow (1^1 2^1) \rightarrow (1^1 2^1) \rightarrow (1^1 2^1)$
(4)	3	1, 2	1	≥ 5 ≥ 4 2	$(1^3) \rightarrow (1^1 2^1) \rightarrow (1^1 2^1) \rightarrow (1^1 2^1) \rightarrow (1^3)$ or $(1^3) \rightarrow (1^1 2^1) \rightarrow (1^1 2^1) \rightarrow (1^3), (1^1 2^1)$ or $(1^3) \leftrightarrow (1^1 2^1), (1^1 2^1) \leftrightarrow (1^1 2^1)$
(5)	4	1, 3	0	2	$(1^2 2^1) \leftrightarrow (1^2 2^1), (2^2)$
(6)	4	1, 3	1	≥ 2	$P_1 = P_2 = (1^2 2^1), P_3 = (2^2)$, any matching pattern
(7)	4	1, 3	1	≥ 4	$(1^4) \rightarrow (1^2 2^1) \rightarrow (1^2 2^1) \rightarrow (1^4), (2^2)$
(8)	4	1, 3	1	2	$(1^2 2^1) \leftrightarrow (1^2 2^1), (1^1 3^1)$
(9)	4	2	0	2	$(1^2 2^1) \leftrightarrow (1^2 2^1), (1^1 3^1)$
(10)	4	2	0	≥ 4	$(1^2 2^1) \rightarrow (1^2 2^1) \rightarrow (2^2) \rightarrow (1^2 2^1)$
(11)	4	2	1	2	$(1^2 2^1) \leftrightarrow (4^1)$
(12)	4	2	1	2	$(1^1 3^1) \leftrightarrow (2^2)$
(13)	4	2	1		four $(1^2 2^1)$, any matching pattern
(14)	4	2	1	2 ≥ 5	$(1^4) \leftrightarrow (1^2 2^1), (1^2 2^1) \leftrightarrow (2^2)$ or $(1^4) \rightarrow (1^2 2^1) \rightarrow (2^2) \rightarrow (1^2 2^1) \rightarrow (1^4)$
(15)	4	2	1	≥ 4	$(1^4) \rightarrow (1^2 2^1) \rightarrow (1^2 2^1) \rightarrow (1^4), (1^1 3^1)$
(16)	6	1, 5	1	2	$(3^2), (1^4 2^1) \leftrightarrow (1^4 2^1)$
(17)	6	2, 4	0	2	$(3^2), (1^4 2^1) \leftrightarrow (1^4 2^1)$
(18)	6	2, 4	1	2	$(1^4 2^1), (2^3) \leftrightarrow (1^2 2^2)$
(19)	6	3	0	2	$(2^1 4^1), (1^4 2^1) \leftrightarrow (1^4 2^1)$
(20)	6	3	1	2	$(1^1 5^1), (1^4 2^1) \leftrightarrow (1^4 2^1)$
(21)	6	3	1	4	$(1^4 2^1) \rightarrow (1^4 2^1) \rightarrow (1^4 2^1) \rightarrow (1^4 2^1), (2^3)$
(22)	6	3	1	≥ 2	three $(1^2 2^2)$, any matching pattern
(23)	6	3	1	≥ 4	$(1^n) \rightarrow (1^{n-2} 2^1) \rightarrow (1^{n-2} 2^1) \rightarrow (1^n), (2^1 4^1)$

1. A sequence $Q_0 \leftrightarrow Q_1$ is the same as $Q_0 \rightarrow Q_1 \rightarrow Q_0$.
2. A single point Q is the same as $Q \rightarrow Q$ and Q is the ramification of f at branch point 0.
3. If there is a reduced sequence with $l \geq 2$ many arrows but without (1^n) , then c has order l ; if this reduced sequence has (1^n) then the order of c is at least l or c is not a root of unity.

9.3 The case $|\Lambda_c|=2$

Lemma IX.7. *If $f(X) + f(Y) = 0$ is irreducible with genus 0 or 1, then $f^{-1}(0)$ has at most 4 unramified preimages.*

Proof. Suppose $f^{-1}(0)$ has m many unramified preimages, P_1, \dots, P_m . Since the field $\mathbb{K}(x, y)$ is preserved by the automorphism which swaps x and y , let K be the subfield of $\mathbb{K}(x, y)$ fixed by this automorphism, then $[\mathbb{K}(x, y) : K] = 2$.

There are at least m places in $\mathbb{K}(x, y)$ which is totally ramified with index 2 over K . Apply Riemann–Hurwitz formula to $\mathbb{K}(x, y)/K$, it says $0 \geq 2\mathfrak{g}(\mathbb{K}(x, y)) - 2 \geq 2(\mathfrak{g}(K) - 2) + m$, so $\mathfrak{g}(K) \leq 2 - \frac{m}{2}$, this implies $m \leq 4$. \square

Say $\Lambda_c = \{P, Q\}$, we must have $c = -1$ and $Q = -P \neq 0$, therefore $f^{-1}(0)$ has n many unramified preimages, by the lemma, we have $n \leq 4$.

When $n \leq 4$, by a computer program, the following are all the possibilities:

- $\{P, -P, \infty\}$ has type $\{(1^1 3^1), (1^1 3^1), (1^1 3^1)\}$, $n = 4$, $k = 1$, $\mathfrak{g} = 0$
- $\{P, -P, \infty\}$ has type $\{(1^1 3^1), (2^2), (2^2)\}$, $n = 4$, $k = 2$, $\mathfrak{g} = 1$
- $\{P, -P, \infty\}$ has type $\{(2^2), (1^1 3^1), (2^2)\}$, $n = 4$, $k = 2$, $\mathfrak{g} = 1$
- $\{P, -P, \infty\}$ has type $\{(1^2 2^1), (4^1), (2^2)\}$, $n = 4$, $k = 2$, $\mathfrak{g} = 1$

9.4 The case $|\Lambda_c| \geq 3$

Let $|\Lambda_c| = m$, and $\Lambda_c = \{\lambda_1, \dots, \lambda_m\}$. Let $P_i = P(\lambda_i)$, and let Q_i be the ramification type of $f(X) = \lambda_i$, then we define $A(Q_i) := A(P(\lambda_i)) := A_i := n$ minus the number of distinct places over P_i , and $B(Q_i) := B(P_i) := B_i :=$ the number of unramified places, in other words, the number of 1's in Q_i .

Let $A := \min\{A_1, \dots, A_m\}$, and suppose $A = A_m$. For any place P_i , we can form a unique reduced sequence, and say the underlying places are $P_i^{(0)} = P_i, P_i^{(1)}, \dots, P_i^{(l-1)}, P_i^{(l)} = P_i^{(0)}$ in order, and let $A_i^{(j)} := A(P_i^{(j)})$, $B_i^{(j)} := B(P_i^{(j)})$.

Lemma IX.8. *One of the following holds*

1. $A = A_m = 1$ and $m = 3$
2. $A = A_m = 1$ and $m = 4$
3. $A = A_m = 2$ and $m = 3$

4. $A = A_m = 0$ and $A_m^{(1)} = 1$ or 2

Proof. We have $A_i \geq \frac{n-B_i}{2}$, so $n = \sum A_i \geq \frac{mn}{2} - \frac{\sum B_i}{2}$, and this implies $\sum B_i \geq (m-2)n$. Moreover, the genus formula and Lemma IX.4 imply $2n \geq \sum B_i A_i^{(1)}$.

Since A is the minimum, it follows $2n \geq \sum B_i A_i^{(1)} \geq A \sum B_i \geq A(m-2)n$, therefore either $A = 1, m = 3, 4$, or $A = 2, m = 3$, or $A = 0$.

If $A = 0$, by assumption, $A = A_m$, so $A_m = 0, B_m = n$. This implies P_m is unramified, so $P_m^{(1)}$ must be ramified, and $A_m^{(1)} > 0$. Now the genus formula says $2n \geq B_m A_m^{(1)} = n A_m^{(1)}$, so $A_m^{(1)}$ must be 1 or 2. \square

Now we consider the possible configurations of the reduced sequence \mathcal{S}_m , which starts and ends at P_m . We will use the following lemma.

Lemma IX.9. *Suppose P has type $(\dots a_i \dots)$ and $\gcd_i(a_i) = a > 1$. Then $A(P) \geq n/2$, and there is at most one such P in Λ_c . Moreover, $C(P, P) = 0$ if all $a_i = a$, and $C(P, P) \geq \frac{n}{3}$ otherwise.*

Proof. P has at most n/a many distinct places lying over it in $\mathbb{K}(X)$, and a is at most $n/2$, so $A(P) \geq n - n/a \geq n/2$. Due to the fact that $\sum P_i = n$, there are at most two such P 's, and if there are two, they are both of type $((\frac{n}{2})^2)$, and no other points. Now the genus formula says $n + 2 \gcd(n, k) + 2\mathfrak{g} - 2 = 0$ since $C(((\frac{n}{2})^2), ((\frac{n}{2})^2)) = 0$. Clearly it has no solution, so there is at most one such P .

For the second part, see the proof of Lemma III.23. \square

Lemma IX.10. *If \mathcal{S} be a reduced sequence of length $l \geq 2$, then*

$$C(\mathcal{S}) + C(\mathcal{S}^{-1}) \geq l(n-1).$$

Proof. Let $\dots \rightarrow P \rightarrow Q \rightarrow \dots$ be a subsequence of \mathcal{S} , then $\dots \rightarrow Q \rightarrow P \rightarrow \dots$ is a subsequence of \mathcal{S}^{-1} . Note that at most one of P and Q have non-trivial gcd since the sequence \mathcal{S} contains at most one point whose ramification indices have non-trivial gcd. Now by Lemma III.22 and Lemma III.24, we have that $C(P, Q) + C(Q, P) \geq n - 1$. Then the lemma follows from the condition that \mathcal{S} has length l . \square

9.4.1 The case $A = A_m = 1$, $m = 4$, and the case $A = A_m = 2$, $m = 3$

Note that in the proof of Lemma IX.8, we have three inequalities $A_i \geq \frac{n-B_i}{2}$, $\sum B_i \geq (m-2)n$ and $2n \geq \sum B_i A_i^{(1)} \geq A \sum B_i \geq A(m-2)n$. In the two cases concerned, the last inequality becomes equality, so the first two are also equalities.

The first equality $A_i = \frac{n-B_i}{2}$ implies each P_i can only have 1's and 2's.

The third equality implies that, for each i , either $A_i^{(1)} = A$ or $B_i = 0$. If $B_i = 0$, then $A_i = \frac{n-B_i}{2} = \frac{n}{2}$, so P_i has type $(2^{\frac{n}{2}})$, and by lemma 6, there is at most one such point. If $A_i^{(1)} = A = 1$, then $P_i^{(1)}$ has type $(1^{n-2}2^1)$; if $A_i^{(1)} = A = 2$, then $P_i^{(1)}$ has type $(1^{n-4}2^2)$.

The case $A = A_m = 1$, $m = 4$

If there is no $(2^{\frac{n}{2}})$, then there are four $(1^{n-2}2^1)$ points, so $n = \sum A_i = 3$. $C((1^{n-2}2^1), (1^n)) = n$, $C((1^{n-2}2^1), (1^{n-2}2^1)) = n - 2$. Then $2n \geq n + 2 \gcd(n, k) + 2\mathbf{g} - 2 = 4(n - 2)$, we have $n \leq 4$. One can check the following solutions,

$$(n, k, \mathbf{g}) = (4, 2, 1), \text{ four } (1^2 2^1), \text{ any matching pattern}$$

If there is one $(2^{\frac{n}{2}})$ (say it is P_1), then the other three are all $(1^{n-2}2^1)$ (say they are P_2, P_3, P_4). In this case, $\sum A_i = \frac{n}{2} + 3 = n$, so $n = 6$.

If P_1 does not match itself, then $6 + 2 \gcd(6, k) + 2\mathbf{g} - 2 = 20$, no solution. If P_1 matches itself, then $6 + 2 \gcd(6, k) + 2\mathbf{g} - 2 = 12$, we get one solution.

$$(n, k, \mathbf{g}) = (6, 3, 1), P_1 = (2^3), P_2 = P_3 = P_4 = (1^4 2^1), P_2 \rightarrow P_3 \rightarrow P_4 \rightarrow P_2 \text{ and } P_1$$

The case $A = A_m = 2$, $m = 3$

If there is no $(2^{\frac{n}{2}})$, then there are three $(1^{n-4}2^2)$ points, so $n = \sum A_i = 6$. This case $6 + 2 \gcd(6, k) + 2\mathbf{g} - 2 = 12$. We get one solution.

$$(n, k, \mathbf{g}) = (6, 3, 1), P_1 = P_2 = P_3 = (1^22^2), \text{ any matching pattern}$$

If there is one $(2^{\frac{n}{2}})$, then the rest are two $(1^{n-4}2^2)$, so $n = \sum A_i = \frac{n}{2} + 4$, so $n = 8$. If the $(2^{\frac{n}{2}})$ point does not match itself, then $8 + 2 \gcd(8, k) + 2\mathbf{g} - 2 = 24$, no solution. If the $(2^{\frac{n}{2}})$ point matches itself, then $8 + 2 \gcd(8, k) + 2\mathbf{g} - 2 = 16$. We get one solution:

$$(n, k, \mathbf{g}) = (8, 4, 1), P_1 = (2^4), P_2 = P_3 = (1^42^2), P_2 \leftrightarrow P_3 \text{ and } P_1$$

9.4.2 The case $A = A_m = 0$, $A_m^{(1)} = 1$, **with** $n \geq 5$

In this case, P_m has type (1^n) , $P_m^{(1)}$ has type $(1^{n-2}2^1)$, so $C(P_m, P_m^{(1)}) = n$. Now the genus formula says $2n \geq n + C(P_m^{(1)}, P_m^{(2)}) \geq n + (n-2)A_m^{(2)}$. This implies $A_m^{(2)} = 0$ or 1.

The case $A_m^{(2)} = 1$

Then $P_m^{(2)}$ has type $(1^{n-2}2^1)$ and it cannot equal P_m , so there is $P_m^{(3)}$. Now the genus formula says $2 \geq (n-2)A_m^{(3)}$, now $n \geq 5$ implies $A_m^{(3)} = 0$. If $P_m^{(3)} = P_m$, we get the following matching sequence

$$\mathcal{S}_m = P_m \rightarrow P_m^{(1)} \rightarrow P_m^{(2)} \rightarrow P_m, (1^n) \rightarrow (1^{n-2}2^1) \rightarrow (1^{n-2}2^1) \rightarrow (1^n)$$

$\sum_{P_i \in \mathcal{S}_m} A_i = 2$, we still need $n - 2$ more. $C(\mathcal{S}_m) = 2n - 2$.

Now $\Lambda_c - \mathcal{S}_m$ has more points, so there is at least one more sequence, the sequence could be

1. Q , of type $(a^1(n-a)^1)$

2. $Q \leftrightarrow (1^n)$

3. $Q_0 \rightarrow Q_1 \rightarrow \dots \rightarrow Q_l \rightarrow Q_0$, where $l \geq 2$ and at most one (1^n)

For case 1, the genus formula is $n + 2 \gcd(n, k) + 2\mathfrak{g} - 2 = 2n - 2 + n - 2 \gcd(a, n)$, so $\mathfrak{g} = n - \gcd(a, n) - \gcd(k, n)$. If one of a, k is not $n/2$, then $\mathfrak{g} \geq n - \frac{n}{2} - \frac{n}{3} = \frac{n}{6}$. We get one example,

$$n = 6, k = 3, \mathfrak{g} = 1, (1^n) \rightarrow (1^{n-2}2^1) \rightarrow (1^{n-2}2^1) \rightarrow (1^n), (2^14^1)$$

If a, k are both $\frac{n}{2}$, then we have the following example

$$n \text{ even}, n \geq 6, k = \frac{n}{2}, \mathfrak{g} = 0, (1^n) \rightarrow (1^{n-2}2^1) \rightarrow (1^{n-2}2^1) \rightarrow (1^n), \left(\frac{n}{2}\right)^2$$

For case 2, $C(Q, (1^n)) + C((1^n), Q) = n(n-2) \geq 5 \cdot 3 = 15$ is too much.

For case 3, by Lemma IX.10, $C(\mathcal{S}_Q) + C(\mathcal{S}_Q^{-1}) \geq (l+1)(n-1) \geq 3n-3$. We also have $C(\mathcal{S}_m) + C(\mathcal{S}_m^{-1}) = 4n-4$, so the genus formula

$$4n \geq C(\mathcal{S}_m) + C(\mathcal{S}_m^{-1}) + C(\mathcal{S}_Q) + C(\mathcal{S}_Q^{-1}) \geq 7n - 7$$

which violates the assumption that $n \geq 5$.

If $P_m^{(3)} \neq P_m$, then we must have $P_m^{(4)}$, and now $C(\mathcal{S}_m) \geq 2n-2 + nA_m^{(4)} \geq 3n-2$, which is too big for the genus formula, so this cannot happen.

The case $A_m^{(2)} = 0$

Then $P_m^{(2)}$ has type (1^n) , and it is possible that $P_m^{(2)} = P_m$.

If $P_m^{(2)} \neq P_m$, then there must be $P_m^{(3)}$, and $A_m^{(3)} > 0$ (unramified). Now the genus formula says $2n \geq n + 0 + nA_m^{(3)}$, this implies $A_m^{(3)} = 1$. We also have $P_m^{(4)}$, but since there is no room for the genus formula, $P_m^{(4)}$ must equal P_m . We get a sequence $(1^n) \rightarrow (1^{n-2}2^1) \rightarrow (1^n) \rightarrow (1^{n-2}2^1) \rightarrow (1^n)$. For these points, $\sum A_i = 2$, we still need $n-2$, and we need points whose ramification indices are all the same to avoid

contribution. Since we can only have one such point, we know this point must be $((\frac{n}{2})^2)$. So we get one solution.

$$n \text{ even, } n \geq 6, k = \frac{n}{2}, \mathfrak{g} = 1, ((\frac{n}{2})^2), (1^n) \rightarrow (1^{n-2}2^1) \rightarrow (1^n) \rightarrow (1^{n-2}2^1) \rightarrow (1^n)$$

If $P_m^{(2)} = P_m$.

Now for \mathcal{S}_m , $\sum A_i = 1$, we still need $n - 1$. $C(\mathcal{S}_m) = C(\mathcal{S}_m^{-1}) = n$. There are two cases.

Case 1: If all the remaining sequences do not have unramified points.

Let \mathcal{S} be any such sequence of length $l > 1$. Since $4n \geq 2n + C(\mathcal{S}_m) + C(\mathcal{S}_m^{-1}) \geq 2n + l(n - 1)$ and $n \geq 5$, it follows $l = 2$. Thus $c = -1$. Say the sequence is $Q \leftrightarrow -Q$, then $2n \geq n + 2 \gcd(n, k) + 2\mathfrak{g} - 2 = n + C(Q, -Q) + C(-Q, Q) \geq 2n - 1$, so we must have $n = 2k$, and $C(Q, -Q) + C(-Q, Q) = n - 1$ or n . Since $\pm Q$ are both ramified, and n is odd, by Lemma III.22 and lemma III.24, it follows Q has type $(2^{\frac{n}{2}})$, and $-Q$ has type $(1^2 2^{\frac{n-2}{2}})$. Now $A(Q) + A(-Q) = n - 1$, which is exactly needed. We have one solution.

$$n \text{ even, } n \geq 6, k = \frac{n}{2}, \mathfrak{g} = 1, c = -1, (2^{\frac{n}{2}}) \leftrightarrow (1^2 2^{\frac{n-2}{2}}), (1^n) \leftrightarrow (1^{n-2}2^1)$$

If no such sequence has length 2, then each sequence must be a fixed point, so we can only have one such sequence. Since we still need $n - 1$ for $\sum A_i$, this fixed point should be (n^1) . Now the genus formula is $n + 2 \gcd(n, k) + 2\mathfrak{g} - 2 = C(\mathcal{S}_m) + 0 = n + 0$, note it is true for $n \geq 2$, so the solution is

$$n \geq 2, \gcd(n, k) = 1, \mathfrak{g} = 0, (1^n) \leftrightarrow (1^{n-2}2^1), (n^1)$$

Case 2: If at least one of the remaining sequences has unramified points.

Let $\mathcal{S} = Q_0 = (1^n) \rightarrow Q_1 \rightarrow \dots$ be such a sequence. This sequence can contribute

at most n to the genus formula, so $C(\mathcal{S}) \leq n$. This forces the sequence to be $(1^n) \leftrightarrow (1^{n-2}2^1)$, which contributes exactly n .

Now for the remaining sequences, we need $n - 2$ for $\sum A_i$, and no contribution to genus formula. But this implies all points must have the same $((\frac{n}{a})^a)$ type. We can only have one such point, and since $A = n - a = n - 2$, $a = 2$ and the point is $((\frac{n}{2})^2)$. This point must match itself. We get one solution.

$$n \text{ even, } n \geq 6, k = \frac{n}{2}, \mathfrak{g} = 1, ((\frac{n}{2})^2), (1^n) \leftrightarrow (1^{n-2}2^1), (1^{n-2}2^1) \leftrightarrow (1^n)$$

9.4.3 The case $A = A_m = 1$, $m = 3$, with $n \geq 7$

Note that $A_3 = 1$ implies P_3 has type $(1^{n-2}2^1)$, since P_3 has $n - 2 \geq 5$ unramified preimages, $P_3 \neq cP_3$ (otherwise $c = -1$, $P_3 = 0$). Therefore $P_3^{(1)} \neq P_3$. The genus formula says $2n \geq (n - 2)A_3^{(1)}$, and $n \geq 7$ implies $A_3^{(1)} \leq 2$. Since $A_3^{(1)} \geq A = 1$, it can only be 1 or 2.

The case $A_3^{(1)} = 1$

This case $P_3^{(1)}$ has type $(1^{n-2}2^1)$, now consider $P_3^{(2)}$. The genus formula says $2n \geq (n - 2) + (n - 2)A_3^{(2)}$, so $A_3^{(2)} = 1$ (otherwise, we will have $n \leq 6$). Now there are two cases, depending on if $P_3^{(2)}$ equals P_3 .

If $P_3^{(2)} = P_3$, then $c = -1$, and the remaining point must be 0. Since $A(0) = n - 2$, 0 must have type $(a^1(n - a)^1)$, and $A(0) = n - 2 \gcd(n, a)$. Now the genus formula becomes $n + 2 \gcd(n, k) + 2\mathfrak{g} - 2 = (n - 2) + (n - 2) + (n - 2 \gcd(n, a))$, simplify we get $1 \leq n - \gcd(n, a) - \gcd(n, k) = \mathfrak{g} + 1 \leq 2$. Note that $n > 6$, so $\frac{n}{3} > 2$, therefore we must have $n > \gcd(n, a) + \gcd(n, k) \geq \frac{2}{3}n$. There are only a handful cases of the pair $(\gcd(n, a), \gcd(n, k))$, which are $\{(\frac{n}{2}, \frac{n}{3}), (\frac{n}{2}, \frac{n}{4}), (\frac{n}{2}, \frac{n}{5}), (\frac{n}{2}, \frac{n}{6}), (\frac{n}{3}, \frac{n}{3})\}$. We test each one of them and solve for n, \mathfrak{g}, a, k (here $n \geq 7$). The solutions are

$(n, \mathbf{g}, a, k) = (12, 1, 6, 4), (8, 1, 4, 2)$. Therefore we have the following solutions.

$$n = 12, \mathbf{g} = 1, c = -1, k = 4, (6^2), (1^{10}2^1) \rightarrow (1^{10}2^1) \rightarrow (1^{10}2^1)$$

$$n = 8, \mathbf{g} = 1, c = -1, k = 4, (2^16^1), (1^62^1) \rightarrow (1^62^1) \rightarrow (1^62^1)$$

If $P_3^{(2)} \neq P_3$, then $c = \omega = e^{\frac{2\pi}{3}i}$, then each one of P_1, P_2, P_3 has type $(1^{n-2}2^1)$, but now $\sum A_i = 3 < n$. So no solution is from this case.

The case $A_3^{(1)} = 2$

This case $P_3^{(1)}$ has type $(1^{n-4}2^2)$ or $(1^{n-3}3^1)$.

In the first case, $C(P_3, P_3^{(1)}) = 2(n-2)$, so $2n \geq n + 2\gcd(n, k) + 2\mathbf{g} - 2 \geq 2(n-2) + (n-4)A_3^{(2)}$, so $4 \geq (n-4)A_3^{(2)}$, since $n \geq 7$ and $A_3^{(2)} > 0$, the only possibilities are $n = 7$ or 8 , and $A_3^{(2)} = 1$, but one can check $n = 7$ does not satisfy the genus inequality, so $n = 8$.

Note now the genus inequality become equality, which means $k = n/2 = 4$, and we have no contributions to the genus formula except $C(P_3, P_3^{(1)})$ and $C(P_3^{(1)}, P_3^{(2)})$. If $P_3^{(2)} \neq P_3$, then $P_3^{(2)}$ contributes $C(P_3^{(2)}, P_3) = n-2 > 0$, so we must have $P_3^{(2)} = P_3$ and $c = -1$. The remaining point must be 0, and $A(0) = n-1-2 = 5$, however, $C(0, 0) = 0$ implies there are 2 or 4 places, so $A(0) = 6$ or 4 , but not 5. Thus we get no solution.

In the second case, $C(P_3, P_3^{(1)}) = 2(n-2)$, so $2n \geq n + 2\gcd(n, k) + 2\mathbf{g} - 2 \geq 2(n-2) + (n-3)A_3^{(2)}$, so $4 \geq (n-3)A_3^{(2)}$. The only possibility is $n = 7$ and $A_3^{(2)} = 1$, but one can check $n = 7$ does not make the genus inequality work, so no solution.

9.4.4 The remaining cases

The remaining cases are

1. $A = A_m = 0, A_m^{(1)} = 1, n \leq 4$

2. $A = A_m = 1, m = 3, n \leq 6$

$A = A_m = 0, A_m^{(1)} = 1, n \leq 4$

If $n = 2$, then $P_m = (1^2), P_m^{(1)} = (2^1)$, since $\sum A_i = n = 2$, we must have two (2^1) 's and at least one (1^2) 's. The matching pattern can only be $(1^2) \leftrightarrow (2^1)$, $(1^2) \leftrightarrow (2^1)$, or $(1^2) \rightarrow (2^1) \rightarrow (1^2) \rightarrow (2^1) \rightarrow (1^2)$, or $(1^2) \rightarrow (2^1) \rightarrow (2^1) \rightarrow (1^2)$. Now check each possibility, we get the following solutions.

$$(n, k, \mathbf{g}) = (2, 1, 1), (1^2) \leftrightarrow (2^1), (1^2) \leftrightarrow (2^1) \text{ or } (1^2) \rightarrow (2^1) \rightarrow (1^2) \rightarrow (2^1) \rightarrow (1^2)$$

$$(n, k, \mathbf{g}) = (2, 1, 0), (1^2) \rightarrow (2^1) \rightarrow (2^1) \rightarrow (1^2)$$

If $n = 3$, there are two cases.

Case 1: we have three $(1^1 2^1)$, and at least one (1^3) . Since $C((1^3), (1^1 2^1)) = 3$, $C((1^1 2^1), (1^1 2^1)) = 1$, and the contribution $3 + 2 \gcd(3, 1) + 2\mathbf{g} - 2$ is either 3 or 5, we have the following examples.

$$(n, k, \mathbf{g}) = (3, 1, 1), (1^3) \rightarrow (1^1 2^1) \rightarrow (1^1 2^1) \rightarrow (1^1 2^1) \rightarrow (1^3) \text{ or}$$

$$(1^3) \rightarrow (1^1 2^1) \rightarrow (1^1 2^1) \rightarrow (1^3), (1^1 2^1), \text{ or } (1^3) \leftrightarrow (1^1 2^1), (1^1 2^1) \leftrightarrow (1^1 2^1)$$

Case 2: we have one $(1^1 2^1)$, one (3^1) , and at least one (1^3) . Since $(1^3) \rightarrow (1^1 2^1)$ already contributes 3, we can have a additional 2 or 0. Since $(1^3) \rightarrow (3^1)$ or $(1^1 2^1) \rightarrow (3^1)$ contributes larger than 2, (3^1) should be a fixed point, we get one solution, $(n, k, \mathbf{g}) = (3, 1, 0), (1^3) \leftrightarrow (1^1 2^1), (3^1)$, but this is a speical case of a known example.

If $n = 4$, then we already have two points, $(1^4) \rightarrow (1^2 2^1)$. For the remaining point, $\sum A_i = 3$. Now there are three cases.

If it has another (1^4) , then we must have $(1^4) \rightarrow (1^2 2^1)$, the two $(1^4) \rightarrow (1^2 2^1)$ already contribute $2n$ to the genus formula, so $k = n/2 = 2$ and $\mathbf{g} = 1$, and there is no room for more contributions. Now the sum of A_i value of these four points is

2, we need 2 more, so there is (are) more point(s). To get 0 contribution, we must have only one additional point, and its ramification type can only be (2^2) . Thus we have one example.

$$n = 4, k = 2, \mathfrak{g} = 1, (1^4) \leftrightarrow (1^2 2^1), (1^4) \leftrightarrow (1^2 2^1), (2^2)$$

If it has a (4^1) , then only one solution, $(n, k, \mathfrak{g}) = (4, 1, 0), (1^4) \leftrightarrow (1^2 2^1), (4^1)$, but this is a known example.

If it does not have additional (1^4) or (4^1) , since $A((1^2 2^1)) = 1$, $A((1^1 3^1)) = A((2^2)) = 2$ and the remaining points have $\sum A_i = 3$, these points have the following possibilities:

(1) three $(1^2 2^1)$. Impossible since the total contribution of all points is $10 > 2n = 8$.

(2) one $(1^2 2^1)$ and one (2^2) . All the possible pairs of (k, \mathfrak{g}) we can get are $(1, 1), (2, 1), (2, 0)$,

we have the following examples:

$$(n, k, \mathfrak{g}) = (4, 2, 1), (1^4) \leftrightarrow (1^2 2^1), (1^2 2^1) \leftrightarrow (2^2) \text{ or}$$

$$(1^4) \rightarrow (1^2 2^1) \rightarrow (2^2) \rightarrow (1^2 2^1) \rightarrow (1^4)$$

$$(n, k, \mathfrak{g}) = (4, 2, 0) \text{ or } (4, 1, 1), (1^4) \rightarrow (1^2 2^1) \rightarrow (1^2 2^1) \rightarrow (1^4), (2^2)$$

(3) one $(1^2 2^1)$ and one $(1^1 3^1)$. $C((1^2 2^1) \rightarrow (1^1 3^1)) = 6$, but there is room for at most 4, so this cannot happen, so $(1^1 3^1)$ is a fixed point, this contributes 2. The remaining three points include one (1^4) and two $(1^2 2^1)$, since we will not have more fixed point, they must form the sequence $(1^4) \rightarrow (1^2 2^1) \rightarrow (1^2 2^1) \rightarrow (1^4)$, which contributes 6. Therefore total contribution is 8, this means $k = 2, \mathfrak{g} = 1$, we have one example.

$$(n, k, \mathfrak{g}) = (4, 2, 1), (1^4) \rightarrow (1^2 2^1) \rightarrow (1^2 2^1) \rightarrow (1^4), (1^1 3^1)$$

The case $A = A_m = 1$, $m = 3$, $n \leq 6$

We have $P_3 = (1^{n-2}2^1)$, and $A_1 + A_2 = n - 1$, $n + 2 \gcd(n, k) + 2\mathbf{g} - 2 = \text{contribution}$. The matching pattern can only be either one point matches itself and the other two match each other, or they form a chain (e.g. $P_1 \rightarrow P_2 \rightarrow P_3 \rightarrow P_1$). Use a computer program, we have the following solutions.

- (1) $(n, k, \mathbf{g}) = (3, 1, 0)$, $P_1 = P_2 = P_3 = (1^12^1)$, any matching pattern.
- (2) $(n, k, \mathbf{g}) = (4, 1, 1)$ or $(4, 2, 0)$, $P_1 = P_2 = (1^22^1)$, $P_3 = (1^13^1)$, matching pattern,
 $P_3 \leftrightarrow P_3, P_1 \leftrightarrow P_2$
- (3) $P_1 = P_2 = (1^22^1)$, $P_3 = (2^2)$
 $(n, k, \mathbf{g}) = (4, 1, 0)$ for matching pattern $P_1 \leftrightarrow P_2, P_3$
 $(n, k, \mathbf{g}) = (4, 1, 1)$ or $(4, 2, 0)$ for any matching pattern
- (4) $(n, k, \mathbf{g}) = (5, 1, 1)$ or $(5, 2, 1)$, $P_1 = (1^32^1)$, $P_2 = P_3 = (1^12^2)$, matching pattern,
 $P_1, P_2 \leftrightarrow P_3$
- (5) $(n, k, \mathbf{g}) = (6, 3, 1)$, $P_1 = (1^15^1)$, $P_2 = P_3 = (1^42^1)$, matching pattern, $P_1, P_2 \leftrightarrow$
 P_3
- (6) $(n, k, \mathbf{g}) = (6, 2, 1)$ or $(6, 3, 0)$, $P_1 = (2^14^1)$, $P_2 = P_3 = (1^42^1)$, matching pattern,
 $P_1 \leftrightarrow P_1, P_2 \leftrightarrow P_3$
- (7) $(n, k, \mathbf{g}) = (6, 1, 1)$ or $(6, 2, 0)$, $P_1 = (3^2)$, $P_2 = P_3 = (1^42^1)$, matching pattern,
 $P_1 \leftrightarrow P_1, P_2 \leftrightarrow P_3$
- (8) $(n, k, \mathbf{g}) = (6, 2, 1)$ or $(6, 3, 0)$, $P_1 = (1^42^1)$, $P_2 = (2^3)$, $P_3 = (1^22^2)$, matching
pattern, $P_1, P_2 \leftrightarrow P_3$ or $P_2, P_1 \leftrightarrow P_3$

9.5 Summary and proof of Theorem IX.6

Theorem IX.11. *The reduced sequences, the values of n , k and genus can only be one the following cases. However, the following cases do not necessarily correspond to a genuine Laurent polynomial f such that $f(X) - cf(Y)$ is irreducible, for some root of unity $c \in \mathbb{K} \setminus \{1\}$.*

1. $(n, k, \mathfrak{g}) = (4, 1, 0), (1^1 3^1) \leftrightarrow (1^1 3^1)$

2. $(n, k, \mathfrak{g}) = (4, 2, 1), (1^1 3^1) \leftrightarrow (2^2)$

3.

$$(n, k, \mathfrak{g}) = (4, 2, 1), \text{ four } (1^2 2^1), \text{ any matching pattern}$$

4.

$$(n, k, \mathfrak{g}) = (6, 3, 1), P_1 = (2^3), P_2 = P_3 = P_4 = (1^4 2^1), P_2 \rightarrow P_3 \rightarrow P_4 \rightarrow P_2 \text{ and } P_1$$

5.

$$(n, k, \mathfrak{g}) = (6, 3, 1), P_1 = P_2 = P_3 = (1^2 2^2), \text{ any matching pattern}$$

6.

$$(n, k, \mathfrak{g}) = (8, 4, 1), P_1 = (2^4), P_2 = P_3 = (1^4 2^2), P_2 \leftrightarrow P_3 \text{ and } P_1$$

7.

$$n = 6, k = 3, \mathfrak{g} = 1, (1^n) \rightarrow (1^{n-2} 2^1) \rightarrow (1^{n-2} 2^1) \rightarrow (1^n), (2^1 4^1)$$

8.

$$n \text{ even}, n \geq 6, k = \frac{n}{2}, \mathfrak{g} = 0, (1^n) \rightarrow (1^{n-2} 2^1) \rightarrow (1^{n-2} 2^1) \rightarrow (1^n), \left(\left(\frac{n}{2}\right)^2\right)$$

9.

$$n \text{ even}, n \geq 6, k = \frac{n}{2}, \mathfrak{g} = 1, \left(\left(\frac{n}{2}\right)^2\right), (1^n) \rightarrow (1^{n-2} 2^1) \rightarrow (1^n) \rightarrow (1^{n-2} 2^1) \rightarrow (1^n)$$

10.

$$n \text{ even}, n \geq 6, k = \frac{n}{2}, \mathfrak{g} = 1, c = -1, (2^{\frac{n}{2}}) \leftrightarrow (1^2 2^{\frac{n-2}{2}}), (1^n) \leftrightarrow (1^{n-2} 2^1)$$

11.

$$n \text{ even}, n \geq 6, k = \frac{n}{2}, \mathfrak{g} = 1, ((\frac{n}{2})^2), (1^n) \leftrightarrow (1^{n-2} 2^1), (1^{n-2} 2^1) \leftrightarrow (1^n)$$

12.

$$n = 12, \mathfrak{g} = 1, c = -1, k = 4, (6^2), (1^{10} 2^1) \rightarrow (1^{10} 2^1) \rightarrow (1^{10} 2^1)$$

13.

$$n = 8, \mathfrak{g} = 1, c = -1, k = 4, (2^1 6^1), (1^6 2^1) \rightarrow (1^6 2^1) \rightarrow (1^6 2^1)$$

14.

$$(n, k, \mathfrak{g}) = (2, 1, 1), (1^2) \leftrightarrow (2^1), (1^2) \leftrightarrow (2^1) \text{ or } (1^2) \rightarrow (2^1) \rightarrow (1^2) \rightarrow (2^1) \rightarrow (1^2)$$

15.

$$(n, k, \mathfrak{g}) = (2, 1, 0), (1^2) \rightarrow (2^1) \rightarrow (2^1) \rightarrow (1^2)$$

16.

$$(n, k, \mathfrak{g}) = (3, 1, 1), (1^3) \rightarrow (1^1 2^1) \rightarrow (1^1 2^1) \rightarrow (1^1 2^1) \rightarrow (1^3) \text{ or}$$

$$(1^3) \rightarrow (1^1 2^1) \rightarrow (1^1 2^1) \rightarrow (1^3), (1^1 2^1), \text{ or } (1^3) \leftrightarrow (1^1 2^1), (1^1 2^1) \leftrightarrow (1^1 2^1)$$

17.

$$n = 4, k = 2, \mathfrak{g} = 1, (1^4) \leftrightarrow (1^2 2^1), (1^4) \leftrightarrow (1^2 2^1), (2^2)$$

18.

$$(n, k, \mathfrak{g}) = (4, 2, 1), (1^4) \leftrightarrow (1^2 2^1), (1^2 2^1) \leftrightarrow (2^2) \text{ or}$$

$$(1^4) \rightarrow (1^2 2^1) \rightarrow (2^2) \rightarrow (1^2 2^1) \rightarrow (1^4)$$

19.

$$(n, k, \mathbf{g}) = (4, 2, 0) \text{ or } (4, 1, 1), (1^4) \rightarrow (1^2 2^1) \rightarrow (1^2 2^1) \rightarrow (1^4), (2^2)$$

20.

$$(n, k, \mathbf{g}) = (4, 2, 1), (1^4) \rightarrow (1^2 2^1) \rightarrow (1^2 2^1) \rightarrow (1^4), (1^1 3^1)$$

21. $(n, k, \mathbf{g}) = (3, 1, 0)$, $P_1 = P_2 = P_3 = (1^1 2^1)$, any matching pattern.22. $(n, k, \mathbf{g}) = (4, 1, 1)$ or $(4, 2, 0)$, $P_1 = P_2 = (1^2 2^1)$, $P_3 = (1^1 3^1)$, matching pattern,

$$P_1 \leftrightarrow P_2, P_3$$

23. $P_1 = P_2 = (1^2 2^1)$, $P_3 = (2^2)$

$$(n, k, \mathbf{g}) = (4, 1, 0) \text{ for matching pattern } P_1 \leftrightarrow P_2, P_3$$

$$(n, k, \mathbf{g}) = (4, 1, 1) \text{ or } (4, 2, 0) \text{ for any matching pattern}$$

24. $(n, k, \mathbf{g}) = (5, 1, 1)$ or $(5, 2, 1)$, $P_1 = (1^3 2^1)$, $P_2 = P_3 = (1^1 2^2)$, matching pattern,

$$P_1, P_2 \leftrightarrow P_3$$

25. $(n, k, \mathbf{g}) = (6, 3, 1)$, $P_1 = (1^1 5^1)$, $P_2 = P_3 = (1^4 2^1)$, matching pattern, $P_1, P_2 \leftrightarrow$

$$P_3$$

26. $(n, k, \mathbf{g}) = (6, 2, 1)$ or $(6, 3, 0)$, $P_1 = (2^1 4^1)$, $P_2 = P_3 = (1^4 2^1)$, matching pattern,

$$P_1, P_2 \leftrightarrow P_3$$

27. $(n, k, \mathbf{g}) = (6, 1, 1)$ or $(6, 2, 0)$, $P_1 = (3^2)$, $P_2 = P_3 = (1^4 2^1)$, matching pattern,

$$P_1, P_2 \leftrightarrow P_3$$

28. $(n, k, \mathbf{g}) = (6, 2, 1)$ or $(6, 3, 0)$, $P_1 = (1^4 2^1)$, $P_2 = (2^3)$, $P_3 = (1^2 2^2)$, matching

$$\text{pattern, } P_1, P_2 \leftrightarrow P_3 \text{ or } P_2, P_1 \leftrightarrow P_3$$

29. $(1^2 2^1) \leftrightarrow (4^1)$, $n = 4$, $k = 2$, $\mathbf{g} = 1$ 30. $n \geq 2$, $\gcd(n, k) = 1$, $\mathbf{g} = 0$, $(1^n) \leftrightarrow (1^{n-2} 2^1)$, (n^1)

Proof. The theorem is just a summary of all the cases found in the $|\Lambda_c| = 2$, $|\Lambda_c| \geq 3$ in the last two sections. \square

Now we see which is not corresponding to a genuine Laurent polynomial, or $f(X) - cf(Y)$ is reducible.

Lemma IX.12. *If there is a point $P \in \mathbb{K}$ and a number $N > 1$ for which every ramification index over each of ∞ , P and cP is divisible by N , then $f(X) - cf(Y)$ is reducible.*

Proof. Say the gcd is $a > 1$, then there is rational functions $g_1(X)$ and $g_2(X)$, such that $f(X) - cP = g_1(X)^a$ and $f(X) - P = g_2(X)^a$, therefore $f(X) - cf(Y) = g_1(X)^a - cg_2(Y)^2 = g_1(X)^a - (c^{\frac{1}{a}}g_2(Y))^a$, which obviously has a factor $g_1(X) - c^{\frac{1}{a}}g_2(Y)$, so $f(X) - cf(Y)$ is reducible. \square

Lemma IX.13. *If $c = -1$ and $f(X) - cf(Y)$ is irreducible with genus \mathfrak{g} , then 0 has at most $2\mathfrak{g} + 2$ distinct preimages under f .*

Proof. Suppose 0 has distinct preimages P_1, \dots, P_l , then in $\mathbb{K}(x, y)$, there is only one place Q_i over both P_i in $\mathbb{K}(x)$ and P_i in $\mathbb{K}(y)$, for $i = 1, \dots, l$. Let τ be the degree-2 automorphism which swaps x and y , and let K be the subfield of $\mathbb{K}(x, y)$ fixed by τ , then $[\mathbb{K}(x, y) : K] = 2$ and each Q_i must be totally ramified of index 2. Now apply Riemann-Hurwitz to $\mathbb{K}(x, y)/K$, we have

$$2\mathfrak{g} - 2 = 2(2\mathfrak{g}_K - 2) + \sum (e_p - 1) \geq 2(2\mathfrak{g} - 2) + l$$

so $l \leq 2\mathfrak{g} + 2 - 4\mathfrak{g}_K \leq 2\mathfrak{g} + 2$.

If $l > 2\mathfrak{g} + 2$, then $\mathfrak{g}_K < 0$, which is impossible, so $f(X) - cf(Y)$ must be reducible in this case. \square

Now we are ready to prove Theorem IX.6.

Proof of Theorem IX.6. Lemma IX.12 rules out the following cases in Theorem IX.11: 6,8,9,11,12,13, 17,19 (for $(n, k, \mathfrak{g}) = (4, 2, 0)$), 23(for $(n, k, \mathfrak{g}) = (4, 2, 0)$ with a fixed point), 26(for $(n, k, \mathfrak{g}) = (6, 2, 1)$), 28(for $(n, k, \mathfrak{g}) = (6, 2, 1)$ with P_2 fixed).

Lemma IX.13 rules out case 1, 10, 21 (if P_1 is fixed), 23 (for $(4, 2, 0)$ and P_1 fixed), 24, 28 (for $(6, 3, 0)$).

For case 30 in Theorem IX.11 we know 0 is a branch point so $f(X) = (c_1X) \circ \frac{(X-c_2)^n}{X^k}$ for some $c_1, c_2 \in \mathbb{K}^*$, and in order $f(X) - cf(Y)$ is irreducible we must have $\gcd(n, k) = 1$. In this case $f(X)$ has only two finite branch points, one is 0 with type (n^1) and the other is $f(\frac{a}{1-n})$ with type $(1^{n-2}2^1)$. The only condition we need for c is $c \neq 1$. This is the first case in Theorem IX.6. For the remaining cases in Theorem IX.11, we reorganize them and form Table 9.1. □

CHAPTER X

The case that $f(X) - cf(Y)$ is reducible

In this chapter we classify all genuine Laurent polynomials $f(X) \in \mathbb{K}[X, X^{-1}]$ for which $F_{f,c}(X, Y)$ is reducible with an irreducible factor of genus zero or one where $c \in \mathbb{K}^* \setminus \{1\}$. In the first section we study the case when f is indecomposable. In the subsequent sections we assume f is decomposable. There are three cases: $f = P \circ L$, $f = L \circ X^m$ and $f = P \circ L \circ X^m$, where $P \in \mathbb{K}[X]$ has degree at least 2, $L \in \mathbb{K}[X, X^{-1}]$ is an indecomposable genuine Laurent polynomial and $m \geq 2$ is an integer. In the second section we solve the case that $f = P \circ L$. In the last section we solve the remaining two cases together where we use \tilde{f} for L and $P \circ L$, in other words, $\tilde{f} = \tilde{P} \circ L$ for some nonconstant polynomial $\tilde{P} \in \mathbb{K}[X]$.

10.1 Indecomposable case

We first prove Proposition X.3, which says for any indecomposable genuine Laurent polynomial $f(X) \in \mathbb{K}[X, X^{-1}]$, if $F_{f,c}(X, Y)$ is reducible with an irreducible factor of genus zero or one then $f(X) - cf(Y) = f(X) - f(\mu(Y)) = (X - \mu(Y))F_f(X, \mu(Y))$ where $\mu(X) = aX$ or a/X for some $a \in \mathbb{K}^*$. The numerator of $X - \mu(Y)$ is an irreducible factor of genus 0, and we may get more irreducible factors of genus at most 1 from $F_f(X, \mu(Y))$. Note that every irreducible factor of $F_f(X, \mu(Y))$ can be obtained from replacing Y with $\mu(Y)$ in an irreducible factor of $F_f(X, Y)$ and the genus

remains the same. Therefore $f(X)$ must be one of the Laurent polynomials listed in Theorem IV.1 and we can find the pair (f, c) which yields additional irreducible factor(s) of genus at most 1, and these pairs are listed in Proposition X.4.

We first show two lemmas that are used to prove Proposition X.3.

Lemma X.1. *For $m > 6$, every automorphism of each group $G \in \{S_m, S_m, S_m \wr S_2\}$ is induced by conjugation by an element of G .*

Proof. The assertion is well-known in case $G \in \{S_m, A_m\}$, so we assume that $G = S_m \wr S_2$. We claim that the only normal subgroups of G which are isomorphic to A_m are $A_m \times 1$ and $1 \times A_m$.

Let N be a normal subgroup of G which is isomorphic to A_m . Since $A_m \times A_m$ is a normal subgroup of G , it follows that $N \cap (A_m \times A_m)$ is a normal subgroup of N . But $[N : N \cap (A_m \times A_m)] \leq [G : A_m \times A_m] = 8$, so $N \cap (A_m \times A_m)$ is a normal subgroup of N having index at most 8; since N is isomorphic to A_m , the index must be 1, so that N is contained in $A_m \times A_m$.

Next, the image of N under projection to the first coordinate is a normal subgroup of A_m , and hence is either 1 or A_m . We may assume that the image is A_m . Likewise we may assume that the image of N under projection to the second coordinate is A_m . But then, for any $g \in A_m$, N contains a unique element of the form (h, g) with $h \in A_m$, and moreover $h \neq 1$ and $g \neq 1$. But also N contains any conjugate of this element by $A_m \times 1$, so that A_m centralizes h , whence $h = 1$, contradiction. This proves the claim.

Next, any automorphism $\sigma \in G$ must preserve the set of normal subgroups of G which are isomorphic to A_m , and must induce an automorphism of the group they generate, namely $A_m \times A_m$. This gives a homomorphism $\text{Aut}(G) \rightarrow \text{Aut}((A_m)^2)$. We will be done once we show that this homomorphism is injective, since by composing

with conjugation by an element of S_2 we may assume that σ induces an automorphism of both $A_m \times 1$ and $1 \times A_m$, whence σ acts on each of these groups as an element of S_m , so that σ acts on G as conjugation by an element of G .

Now suppose that σ acts as the identity on $(A_m)^2$. For any $g \in G$ and any $h \in (A_m)^2$ we have $g^{-1}hg \in (A_m)^2$ (since $(A_m)^2$ is normal in G) so that σ fixes $g^{-1}hg$, whence $g^{-1}hg = \sigma(g^{-1}hg) = \sigma(g)^{-1}h\sigma(g)$, but then $\sigma(g)g^{-1}h = h\sigma(g)g^{-1}$ so that $\sigma(g)g^{-1}$ is an element of G which commutes with every element $h \in (A_m)^2$. To conclude the proof, it suffices to show that the centralizer of $(A_m)^2$ in G is trivial, since that implies that $\sigma(g) = g$ for every $g \in G$, so that $\sigma = 1$.

Now suppose that some element of G centralizes $(A_m)^2$. If the element is (a, b) with $a, b \in S_m$ then both a and b must centralize A_m , and hence must be 1. If the element is $(a, b)s$ with $a, b \in S_m$ and s swapping the two copies of S_m , then $(a, b)s(g, 1) = (a, b)(1, g)s = (a, bg)s$, and $(g, 1)(a, b)s = (ga, b)s$, so that $ga = a$ for every $g \in A_m$, contradiction. \square

Lemma X.2. *Let $p(X)$ be an indecomposable Laurent polynomial with monodromy group $G = S_m$, $G = A_m$, or $G = S_m \wr S_2$, where $m > 6$, and let $c \in \mathbb{K} \setminus \{0, 1\}$. If $p(X) - cp(Y)$ is reducible and has a factor which defines a curve of genus 0 or 1, then this factor has degree 1.*

Proof. Suppose otherwise. Let u, v be transcendental over \mathbb{K} such that $p(u) = cp(v)$ and the genus of $\mathbb{K}(u, v)$ is genus 0 or 1. Put $t = p(u)$, and let Ω be the Galois closure of $\mathbb{K}(u)/\mathbb{K}(t)$. By Theorem III.15, Ω is also the Galois closure of $\mathbb{K}(v)/\mathbb{K}(t)$. Extend the \mathbb{K} -isomorphism $\mathbb{K}(u) \rightarrow \mathbb{K}(v)$ which maps $u \rightarrow v$ to an embedding $\sigma \in \Omega$ into the algebraic closure of $\mathbb{K}(t)$. Then $\sigma(t) = \sigma(p(u)) = p(\sigma(u)) = p(v) = p(u)/c = t/c$, so $\sigma(\Omega)$ is the Galois closure of $\sigma(\mathbb{K}(u))/\sigma(\mathbb{K}(t))$, in other words, $\mathbb{K}(v)/\mathbb{K}(t)$, whence $\sigma(\Omega) = \Omega$. Therefore σ is an automorphism of Ω which maps $\mathbb{K}(t)$ to itself; this

means that σ normalizes $G := Gal(\Omega/\mathbb{K}(t))$ in $Aut(\Omega/\mathbb{K})$. In particular, σ induces an automorphism of G , so by Lemma X.1 σ must act on G as conjugation by an element of G . Finally, since $\sigma(u) = v$, we have $\sigma Gal(\Omega/\mathbb{K}(u))\sigma^{-1} = Gal(\Omega/\mathbb{K}(v))$, so that $Gal(\Omega/\mathbb{K}(u))$ and $Gal(\Omega/\mathbb{K}(v))$ are conjugate subgroups of G . This means that there is an element of G which maps $\mathbb{K}(u)$ to $\mathbb{K}(v)$. Let w be the image of u under this element of G , so that $p(w) = t$. Then $[\mathbb{K}(w) : \mathbb{K}(t)] = \deg(p) = [\mathbb{K}(v) : \mathbb{K}(t)]$, so that $\mathbb{K}(w) = \mathbb{K}(v)$. Then $\mathbb{K}(u, w) = \mathbb{K}(u, v)$ has genus 0 or 1, so by what we proved about the genus of factors of $(p(X) - p(Y))/(X - Y)$, the only possibility is that $w = u$. Therefore $\mathbb{K}(u, v) = \mathbb{K}(u, w) = \mathbb{K}(u)$, so that the minimal polynomial of v over $\mathbb{K}(u)$ has degree 1, as desired. \square

Proposition X.3. *Let $f(X) \in \mathbb{K}[X, X^{-1}]$ be an indecomposable genuine Laurent polynomial for which $F_{f,c}(X, Y)$ is reducible with a genus zero or one irreducible factor. Then one of the following conditions holds:*

1. $f(X) = -f(a/X)$ for some $a \in \mathbb{K}^*$ and $c = -1$.
2. $f(X) = X^l h(X^b)$ where $h \in \mathbb{K}[X, X^{-1}]$ is some genuine Laurent polynomial, $a^l = c$, and c is a root of unity of order b . In this case $cf(X) = f(aX)$.

Proof. First we assume that if $F_{f,c}(X, Y)$ is reducible with a genus zero or one irreducible factor then $cf(Y) = f(\mu(Y))$ where $\mu(X) = aX$ or a/X for some $a \in \mathbb{K}^*$, and we prove the second part of the proposition. Let a_i be the coefficient of f for any integer i . If $\mu(X) = a/X$ then we have $a_{-i} = ca_i a^i$ and $a_i = -a_{-i} a^{-i}$, so $c^2 = 1$ and therefore $c = -1$. If $\mu(X) = aX$ then $a_i(a^i - c) = 0$, so if $a_i \neq 0$ then $a_i = c$. Note that f has at least two nonzero coefficients so c and a_i are both root of unity. Therefore if $a_i \neq 0$ then $i \equiv l \pmod{b}$ where $a^l = c$ and b is the order of c . This implies $f(X) = X^l h(X^b)$ for some genuine Laurent polynomial h .

We now prove the first part of the proposition. We work on the monodromy group $G := \text{Mon}(f)$. The case when the monodromy group of G is S_m , A_m or $S_m \wr S_2$ where $m > 6$ is proved in Lemma X.2. By Theorem V.2, there are only a few groups of size at most 40 remaining. We show that for each group, if $f(X) - cf(Y)$ is reducible then either $\mathbb{K}(x, v)/\mathbb{K}(u, v)$ and $\mathbb{K}(y, u)/\mathbb{K}(u, v)$ are isomorphic extensions so $cf(Y) = f(\mu(Y))$, or the genus of each factor of $f(X) - cf(Y)$ is bigger than 1. We leave this to a program and we compute in the following way:

We first check that no groups G in Theorem V.2 (and also not $G = A_6$ or S_6) can occur as monodromy group of a genuine Laurent polynomial L such that there is a constant $c \neq 1$ for which $L(X) = cL(Y)$ is reducible and has a component of genus 0 or 1, unless $cL(Y) = L(\mu(Y))$ for some linear fractional μ . By Theorem III.15, this setup implies that there are transcendentals u, v over \mathbb{K} such that $L(u) = cL(v)$ (call this common value t) and $\mathbb{K}(u, v)$ has genus 0 or 1 and $\mathbb{K}(u)/\mathbb{K}(t)$ and $\mathbb{K}(v)/\mathbb{K}(t)$ have the same Galois closure. The condition on having the same Galois closure forces $\mathbb{K}(u)/\mathbb{K}(t)$ and $\mathbb{K}(v)/\mathbb{K}(t)$ to have the same branch points. Hence multiplication by c induces a permutation of the branch points of $\mathbb{K}(u)/\mathbb{K}(t)$, and we know that infinity is a branch point of $\mathbb{K}(u)/\mathbb{K}(t)$ which is fixed by multiplication by c , while at most one other branch point of $\mathbb{K}(u)/\mathbb{K}(t)$ is fixed (namely $t = 0$, if it is a branch point). If exactly one finite branch point of $\mathbb{K}(t)$ has the same ramification type in $\mathbb{K}(u)/\mathbb{K}(t)$ as does ∞ , then this point must be fixed by multiplication by c and hence must be $t = 0$. Now, since $cL(v) \neq L(\mu(v))$, the extensions $\mathbb{K}(u)/\mathbb{K}(t)$ and $\mathbb{K}(v)/\mathbb{K}(t)$ are not isomorphic, whence the Galois groups $\text{Gal}(\Omega/\mathbb{K}(u))$ and $\text{Gal}(\Omega/\mathbb{K}(v))$ are not conjugate, where Ω is the Galois closure of $\mathbb{K}(u)/\mathbb{K}(t)$. Note that these two Galois group both have index $\deg(L)$ in G . So we first restrict to the cases where G has more than one conjugacy class of maximal subgroups of index $\deg(L)$, and for

each such group H which is not a one-point stabilizer of G we compute for every element of G (up to conjugacy) the contribution that that element would make to Riemann-Hurwitz for $\mathbb{K}(u)/\mathbb{K}(t)$ and for $\mathbb{K}(u, v)/\mathbb{K}(t)$ if H were $\text{Gal}(\Omega/\mathbb{K}(v))$.

We find that there is no batch of elements which make the proper contributions to both Riemann-Hurwitz formulas, unless either $(|G|, \deg(L)) = (1344, 8)$ or $(\deg(L), G) = (6, A_6)$ or $(\deg(L), G) = (6, S_6)$. But in these cases we compute all tuples of elements of G having the required cycle structures, and also having product 1, and we find that no such tuple generates G . So these ramification types do not actually occur.

Next determine all possibilities for the branch cycles for each group in Theorem V.2 of order $< 10^5$. Show that this includes all groups on his list which are not doubly transitive. In case the group is not doubly transitive, check that there is a degree- n Laurent polynomial $f(X)$ with this group such that $(f(X) - f(Y))/(X - Y) = 0$ has a component of genus 0 or 1. This can only occur if $n = 10$, when one of the following occurs:

1. $G = A_5$, genus 0, ramification type $(1, 3^3), (1^2, 2^4), (5^2)$.
2. $G = S_5$, genus 0 in degree 6, genus 1 in degree 12, ramification type $(1^4, 2^3), (2, 4^2), (5^2)$.
3. $G = S_5$, genus 1, ramification type $(1, 3, 6), (1^4, 2^3), (5^2)$.

But we can check that none of these can happen. □

Proposition X.4. *Let $f(X) \in \mathbb{K}[X, X^{-1}]$ be a genuine Laurent polynomial and $c \in \mathbb{K}^* \setminus \{1\}$ for which $cf(Y) = f(\mu(Y))$ and $F_f(X, \mu(Y))$ has a genus zero or one irreducible factor, where $\mu(Y) = aY$ or a/Y for some $a \in \mathbb{K}^*$. Then f is strongly*

equivalent to some Laurent polynomial \hat{f} for which (\hat{f}, c) satisfy the conditions in one of the cases in Table 10.1.

Table 10.1: $cf(Y) = f(\mu(Y))$ and $F_f(X, \mu(Y))$ has an irreducible factor of genus 0 or 1

item	f	$\text{Mon}(f)$	c	$\mu(X)$	\mathfrak{g}
(1)	$X + 1/X$	S_2	-1	$-X$ or $-1/X$	0
(2)	$(X^3 + 1)/X$	S_3	w ($w^3 = 1$ and $w \neq 1$)	$w^2 X$	1
(3)	$(X^2 + 1)^2/X$	S_4	-1	$1/X$	1
(4)	$(X - 1)^3(X + 1)/X^2$	S_4	-1	$1/X$	1
(5)	$(X^4 + 4X^3 + 2X - 1/4)/X^2$	A_4	-1	$-1/(2X)$	0
(6)	$(X^4 - 6X^2 - 3)/X$	A_4	-1	$-X$	1

In all these cases $f \in \mathbb{K}[X, X^{-1}]$ is an indecomposable Laurent polynomial and $c \in \mathbb{K}^* \setminus \{1\}$, and $F_f(X, \mu(Y))$ is irreducible of genus 0 or 1.

Proof. Note that in this case $F_f(X, Y)$ must have an irreducible factor of genus zero or one so f is one of the Laurent polynomials listed in Theorem V.1 (if $F_f(X, Y)$ is reducible) or in Theorem IV.1 (if $F_f(X, Y)$ is irreducible). In order $cf(Y) = f(\mu(Y))$, $f(X)$ must have at two finite branch points with the same ramification types. This condition rules out all the cases in Theorem V.1 and Theorem IV.1 except the first 6 cases in Table 4.2. For all the remaining cases $F_f(X, Y)$ is irreducible, and since we know these Laurent polynomial we can do the calculation explicitly, and we list all the examples in Table 10.1. \square

10.2 Decomposable case I: $f = P \circ L$

Let $P(u) = P(v) = t$ and $L(x) = u \neq v = L(y)$ and build the function field tower as usual. In this case \mathfrak{g}_{uv} must be 0 or 1, so $F_{P,c}(X, Y)$ has an irreducible factor of genus 0 or 1 and all such P are listed in Theorem X.5. The main result we prove in this section is Proposition X.13.

Theorem X.5 (Carney–Hortsch–Zieve [2]). *Let $P(X) \in \mathbb{K}[X]$ be a polynomial of degree at least 2, and let $d \in \mathbb{K}^* \setminus \{1\}$. If $P(X) - dP(Y)$ has a factor $H(X, Y)$ of*

genus at most 1, then $P = g \circ h \circ \mu$ for some $g, h, \mu \in \mathbb{K}[X]$ with $\deg(\mu) = 1$ and $c \in \mathbb{K}^* \setminus \{1\}$, and $H(X, Y)$ is a factor of $h(X) - ch(Y)$ of genus at most 1. The pair (h, c) is one of the following.

1. $h = X^a(X - 1)^b$ for some coprime integers $a, b \geq 1$ and $a + b \geq 3$
2. (h, c) is one of those in Table 10.2. Only the ramification types are listed, since we only need the types.
3. $h = T_2(X)$
4. $h = T_n(X)$ and $c = -1$ for some integer $n > 3$
5. $h = X^n$

10.2.1 The cases where the pair (P, c) is in Table 10.2

Proposition X.6. *Suppose that $P \in \mathbb{K}[X]$ and $c \in \mathbb{K}^* \setminus \{1\}$ satisfy the constraints in some case of Table 10.2. Let $L \in \mathbb{K}[X, X^{-1}]$ be an indecomposable genuine Laurent polynomial, and put $f := P \circ L$. Suppose that $f(X) - cf(Y)$ is reducible with a component of genus at most 1. Then $\deg(L) = 2$ and the pair (P, c) satisfies case 6 of Table 10.3. In this case $c = -1$ and $f(X) + f(Y)$ has two irreducible factors, both of which have genus 1. The finite branch points of $L(X)$ are the two simple roots of $P(X) - \lambda$.*

Proof. First we show that the left and the right squares are irreducible unless P is case 5(a) and case 5(b) in Table 10.2. If the left square is reducible, then by Theorem III.15 and by looking at the ramification of $u = \infty$ in $\mathbb{K}(x)$ and $\mathbb{K}(u, v)$, we have $\deg(L) = 2$ and $\mathbb{K}(x)$ is a subfield of $\mathbb{K}(u, v)$, therefore $\mathbb{K}(u, v)/\mathbb{K}(u)$ must have at least two finite branch points whose ramification indices are all even. If the right square is reducible, then the same argument implies that $\mathbb{K}(u, v)/\mathbb{K}(v)$ must

Table 10.2: $P(X) - cP(Y)$ irreducible sporadic cases

case	order of c	Ramification types and branch points	\mathfrak{g}
1		$P: \lambda: (3^1) \ c\lambda: (1^3)$ $cP: \lambda: (1^3) \ c\lambda: (3^1)$	1
2	$\neq 2$	$P: \lambda: (1^1 2^1) \ c\lambda: (1^1 2^1) \ c^2\lambda: (1^3)$ $cP: \lambda: (1^3) \ c\lambda: (1^1 2^1) \ c^2\lambda: (1^1 2^1)$	0
3		$P: \lambda: (1^1 2^1) \ c\lambda: (1^3) \ Q: (1^1 2^1) \ cQ: (1^3)$ $cP: \lambda: (1^3) \ c\lambda: (1^1 2^1) \ Q: (1^3) \ cQ: (1^1 2^1)$	1
4	2	$P: \lambda: (1^1 3^1) \ c\lambda: (1^2 2^1)$ $cP: \lambda: (1^2 2^1) \ c\lambda: (1^1 3^1)$	1
5a	$\neq 2$	$P: \lambda: (2^2) \ c\lambda: (1^2 2^1) \ c^2\lambda: (1^4)$ $cP: \lambda: (1^4) \ c\lambda: (2^2) \ c^2\lambda: (1^2 2^1)$	1
5b	$\neq 2$	$P: \lambda: (1^2 2^1) \ c\lambda: (2^2) \ c^2\lambda: (1^4)$ $cP: \lambda: (1^4) \ c\lambda: (1^2 2^1) \ c^2\lambda: (2^2)$	1
6	2	$P: 0: (1^2 2^1) \ \lambda: (1^2 2^1) \ c\lambda: (1^2 2^1)$ $cP: 0: (1^2 2^1) \ \lambda: (1^2 2^1) \ c\lambda: (1^2 2^1)$	0
7	3	$P: \lambda: (1^2 2^1) \ c\lambda: (1^2 2^1) \ c^2\lambda: (1^2 2^1)$ $cP: \lambda: (1^2 2^1) \ c\lambda: (1^2 2^1) \ c^2\lambda: (1^2 2^1)$	0
8	$\neq 2$	$P: 0: (1^2 2^1) \ \lambda: (1^2 2^1) \ c\lambda: (1^2 2^1) \ c^2\lambda: (1^4)$ $cP: 0: (1^2 2^1) \ \lambda: (1^4) \ c\lambda: (1^2 2^1) \ c^2\lambda: (1^2 2^1)$	1
9	2	$P: \lambda: (1^2 2^1) \ c\lambda: (1^2 2^1) \ Q: (1^2 2^1) \ cQ: (1^4)$ $cP: \lambda: (1^2 2^1) \ c\lambda: (1^2 2^1) \ Q: (1^4) \ cQ: (1^1 2^1)$	1
10	> 3	$P: \lambda: (1^2 2^1) \ c\lambda: (1^2 2^1) \ c^2\lambda: (1^2 2^1) \ c^3\lambda: (1^4)$ $cP: \lambda: (1^4) \ c\lambda: (1^2 2^1) \ c^2\lambda: (1^2 2^1) \ c^3\lambda: (1^1 2^1)$	1
11	2	$P: 0: (1^2 3^1) \ \lambda: (1^3 2^1) \ c\lambda: (1^3 2^1)$ $cP: 0: (1^2 3^1) \ \lambda: (1^3 2^1) \ c\lambda: (1^3 2^1)$	1
12	2	$P: 0: (1^1 2^2) \ \lambda: (1^3 2^1) \ c\lambda: (1^3 2^1)$ $cP: 0: (1^1 2^2) \ \lambda: (1^3 2^1) \ c\lambda: (1^3 2^1)$	0
13	$\neq 2$	$P: 0: (1^1 2^2) \ \lambda: (1^3 2^1) \ c\lambda: (1^3 2^1) \ c^2\lambda: (1^5)$ $cP: 0: (1^1 2^2) \ \lambda: (1^5) \ c\lambda: (1^3 2^1) \ c^2\lambda: (1^3 2^1)$	1
14	2	$P: 0: (1^3 2^1) \ \lambda: (1^1 2^2) \ c\lambda: (1^3 2^1)$ $cP: 0: (1^3 2^1) \ \lambda: (1^3 2^1) \ c\lambda: (1^1 2^2)$	1
15	3	$P: \lambda: (1^1 2^2) \ c\lambda: (1^3 2^1) \ c^2\lambda: (1^3 2^1)$ $cP: \lambda: (1^3 2^1) \ c\lambda: (1^1 2^2) \ c^2\lambda: (1^3 2^1)$	1
16	2	$P: 0: (1^4 2^1) \ \lambda: (1^2 2^2) \ c\lambda: (1^2 2^2)$ $cP: 0: (1^4 2^1) \ \lambda: (1^2 2^2) \ c\lambda: (1^2 2^2)$	1
17	2	$P: 0: (1^1 3^2) \ \lambda: (1^5 2^1) \ c\lambda: (1^5 2^1)$ $cP: 0: (1^1 3^2) \ \lambda: (1^5 2^1) \ c\lambda: (1^5 2^1)$	1

have at least two finite branch points whose ramification indices are all even. These conditions rule out all the cases in Table 10.2 except case 5(a) and case 5(b).

For case 5(a), if the left square is reducible then $\deg(L) = 2$ and $\Lambda(L)$ must be

the two simple roots of $P(X) - c\lambda$; if the right square is reducible then $\Lambda(L)$ must be two simple roots of $P(X) - \lambda/c$. Since $c \neq -1$, we know one of the left and the right square must be irreducible and then one of \mathfrak{g}_{xv} and $\mathfrak{g}_{u,y}$ is bigger than 1, so $\mathfrak{g}_{xy} > 1$. The same argument holds for case 5(b), so we can ignore case 5(a) and 5(b) from now on.

Then we look at the $\mathfrak{g}_{uv} = 1$ cases in Table 10.2. Since there is no ramification in $\mathbb{K}(x, v)/\mathbb{K}(u, v)$, we must have ∞_u is unramified in $\mathbb{K}(x)$ and $\deg(L) = 2$. This case L has two finite branch points of type (2^1) , therefore $\mathbb{K}(u, v)/\mathbb{K}(u)$ must have at least two finite places whose ramification indices are all even. This rules out all the remaining $\mathfrak{g}_{uv} = 1$ cases in Table 10.2 except case 5(a) and 5(b).

Next we look at the $\mathfrak{g}_{uv} = 0$ cases in Table 10.2, in other words, case 2, 6, 7 and 12. First of all, the left and the right square must be irreducible, so the top square must be reducible. If $l := \deg(L)$ is a prime number, then $\mathbb{K}(x, v) = \mathbb{K}(u, y) = \mathbb{K}(x, y)$. In particular, any place in $\mathbb{K}(u, v)$ has the same ramification type in $\mathbb{K}(x, v)$ and $\mathbb{K}(u, y)$.

For case 2, every finite branch point of $\mathbb{K}(u, v)/\mathbb{K}(u)$ has at least one ramification index 1, so all the contributions from finite branch points in $\mathbb{K}(x)/\mathbb{K}(u)$ are carried over to $\mathbb{K}(x, v)/\mathbb{K}(u, v)$, so we have $2\mathfrak{g}_{xv} - 2 \geq (-2)l + 3(l - 2) + l = 2l - 6$, so $l \leq 3$. If $l = 3$, then this is equality and $\mathfrak{g}_{xv} = 1$. Therefore at least one branch point of L is one simple root of $P(X) - c^2\lambda$. This implies the simple root of $cP - c^2\lambda$ is a branch point of cP , so another branch point of L is the simple root of $P - c\lambda$. Then this implies the simple root of $cP - c\lambda$ is also a branch point, so the third branch point of L is the simple root of $P - \lambda$. But similarly we have all the three simple roots of $P - \lambda/c$ are branch points of L . Now in total there are at least 4 finite branch points, which is impossible. If $l = 2$, then L has two finite branch points. At least

one of them must be a simple root of $P - c^i \lambda$ where $i = 0, 1$ or 2 . Note that if a simple root of $P - c^i \lambda$ is a branch point, then so are all the simple roots of $P - c^{i-1} \lambda$. Thus anyway we will get at least at least three branch points, contradiction.

For case 12, every finite branch point of $\mathbb{K}(u, v)/\mathbb{K}(u)$ has at least three ramification index 1 except one finite branch point. Thus the finite branch points of $\mathbb{K}(x)/\mathbb{K}(u)$ contributes at least $l+2$ to $\mathbb{K}(x, v)/\mathbb{K}(u, v)$, and then we have $2\mathbf{g}_{xv} - 2 \geq (-2)l + 5(l-2) + (l+2) = 4l - 8$, so $l = 2$ and $\mathbf{g}_{xv} = 1$. Since this is equality, one branch point of L is the simple root of $P(X)$, and the other branch point (say α) of L is one simple root of $P(X) - \lambda$. Now since any simple root β of $cP(X) - \lambda$ is not a branch point of L , we have any place lying over $u = \alpha$ and $v = \beta$ is ramified in $\mathbb{K}(x, v)$ but unramified in $\mathbb{K}(y, u)$, contradiction.

Similarly for case 6, 7, every finite branch point of $\mathbb{K}(u, v)/\mathbb{K}(u)$ has at least two ramification index 1, so $2\mathbf{g}_{xv} - 2 \geq (-2)l + 4(l-2) + 2l = 3l - 6$, so $l = 2$ and $\mathbf{g}_{xv} = 1$. If a simple root of $P(X) - \lambda$ is a branch point of L , then so all all the simple roots of $cP(X) - \lambda$. Therefore L will be at least the order of c many finite branch points, so case 7 cannot happen. For case 6, there is only one case:

1. $\deg(L) = 2$ and $\Lambda(L) = \{\alpha_1, \alpha_2\}$, where α_1, α_2 are the two simple roots of $P(X)$.

This case $f = P \circ L$, $c = -1$ and $f(X) + f(Y)$ has two irreducible factors, and each has genus 1.

□

10.2.2 The case $P = T_2$ and $c \in \mathbb{K}^* \setminus \{1\}$

Lemma X.7. *Let u be a root of $T_2(X) - t$ and v be a root of $T_2(Y) - t$, then the finite branch points of $\mathbb{K}(u, v)/\mathbb{K}(u)$ are $u = \pm\sqrt{2 - 2c}$ (where $v = 0$) and the finite branch points of $\mathbb{K}(u, v)/\mathbb{K}(v)$ are $v = \pm\sqrt{2 - 2/c}$ (where $u = 0$).*

Proof. Now we look at the finite branch points of $\mathbb{K}(u, v)/\mathbb{K}(u)$ and $\mathbb{K}(u, v)/\mathbb{K}(v)$. Since $T_2 = X^2 - 2$, we have $T(X, Y) := T_2(X) - cT_2(Y) = (X^2 - 2) - c(Y^2 - 2)$. As a polynomial in X , $T(X, Y)$ has a double root $X = 0$ when $Y = \pm\sqrt{2 - 2/c}$; as a polynomial in Y , $T(X, Y)$ has a double root $Y = 0$ when $X = \pm\sqrt{2 - 2c}$. Thus the finite branch points of $\mathbb{K}(u, v)/\mathbb{K}(u)$ are $u = \pm\sqrt{2 - 2c}$ and the finite branch points of $\mathbb{K}(u, v)/\mathbb{K}(v)$ are $v = \pm\sqrt{2 - 2/c}$. \square

Lemma X.8. *The left and the right square must be irreducible, and the top square must be reducible.*

Proof. The left square cannot be reducible, otherwise by Theorem III.15, we have $\deg(L) = 2$ and therefore $\mathbb{K}(u, v) = \mathbb{K}(x)$, but this is impossible since $\mathbb{K}(x)/\mathbb{K}(u)$ has two finite branch points but $\mathbb{K}(u, v)/\mathbb{K}(u)$ has only one. Therefore the left square and the right square (by symmetry) are both irreducible, and the top square must be reducible since $f(X) - cf(Y)$ is reducible. \square

The following two lemmas say that when $P = T_2$ the monodromy group of L is very restrictive, and the top square have very strict ramification.

Lemma X.9. *$\text{Mon}(L) \neq S_{\sqrt{m}} \wr S_2$ where $m = \deg(L)$.*

Proof. We will crucially use the fact that the four branch points of $\mathbb{K}(u, v)/\mathbb{K}(u)$ and $\mathbb{K}(u, v)/\mathbb{K}(v)$ all have different values, in other words, $\pm\sqrt{(1 - c)/2}$ and $\pm\sqrt{(1 - 1/c)/2}$ are all different.

Now we show that $\text{Mon}(L)$ cannot be the wreath product. Note that the ramification of L (or equivalently the ramification of $\mathbb{K}(x)/\mathbb{K}(u)$ and $\mathbb{K}(y)/\mathbb{K}(v)$) must be one of those in Table 7.2 and Lemma VII.9 lists the ramification of L , we firstly rule out all the cases in Table 7.2 with ramification index 3 or 6. The remaining cases are case 1, 2, 4, 5 and 6. When $m > 4$, for all these cases the finite branch

points of $\mathbb{K}(u, v)/\mathbb{K}(u)$ and $\mathbb{K}(u, v)/\mathbb{K}(v)$ are all finite branch points of L , so L has four finite branch points but L has at most three finite branch points by Lemma VII.9. Therefore $m \leq 4$, but since m is a square so $m = 4$ and then case 6 is ruled out. Now for each remaining case, at least one finite branch point of $\mathbb{K}(u, v)/\mathbb{K}(u)$ and at least one branch point of $\mathbb{K}(u, v)/\mathbb{K}(v)$ is a branch point of L , so in Table 7.2 L must have at least one additional finite branch point, and this rules out case 2. Now the remaining cases are case 1, 4 and 5. If L has ramification index 4 then L has only two finite branch points and they have type $(1^2 2^1)$ and (4^1) , and they must be branch points of $\mathbb{K}(u, v)/\mathbb{K}(u)$ or $\mathbb{K}(u, v)/\mathbb{K}(v)$; suppose $u = \alpha$ is a finite branch point of $\mathbb{K}(u, v)/\mathbb{K}(u)$ and it ramifies in $\mathbb{K}(x)$ with type (4^1) , then the place in $\mathbb{K}(u, v)$ lying over it is ramified in $\mathbb{K}(x, v)$ but unramified in $\mathbb{K}(u, y)$, there $\mathfrak{g}_{xy} > 1$ since $\mathfrak{g}_{xv} = \mathfrak{g}_{uy} = 1$. Thus L must have three finite branch points and their types are $(1^2 2^1)$, $(1^2 2^1)$ and (2^2) , since at least one point is not a branch point of $\mathbb{K}(u, v)/\mathbb{K}(u)$ (or $\mathbb{K}(u, v)/\mathbb{K}(v)$) and this branch point has no trivial contribution to Riemann–Hurwitz in the top square so we must have $\mathfrak{g}_{xv} = \mathfrak{g}_{uy} = 0$. This means we just consider case 1 in Table 7.2 with $m = 4$, but in this case all the finite branch points of $\mathbb{K}(u, v)/\mathbb{K}(u)$ and $\mathbb{K}(u, v)/\mathbb{K}(v)$ are all branch points of L , so L has at least four finite branch points and we get a contradiction. \square

Lemma X.10. *The monodromy group of L can only possibly be S_m or A_m where $m = \deg(L) \neq 6$, so $\mathbb{K}(x, v)/\mathbb{K}(u, v)$ and $\mathbb{K}(y, u)/\mathbb{K}(u, v)$ have the same set of branch points and each branch point has the same ramification type in $\mathbb{K}(x, v)$ and $\mathbb{K}(u, y)$.*

Proof. By Lemma VII.11, $\text{Mon}(L)$ can only possibly be S_m or A_m with $m \neq 6$, or $S_{\sqrt{m}} \wr S_2$, where $m = \deg(L)$. Note that the wreath product case is ruled out in Lemma X.9.

If $\text{Mon}(L) = S_m$ or A_m with $m \neq 6$, then by the same argument in Proposi-

tion VII.12 we have that if the top square is reducible then $\mathbb{K}(x, v)/\mathbb{K}(u, v)$ and $\mathbb{K}(y, u)/\mathbb{K}(u, v)$ have the same set of branch points and each branch point has the same ramification type in $\mathbb{K}(x, v)$ and $\mathbb{K}(u, y)$. \square

Proposition X.11. *If $P = T_2$ and $c \in \mathbb{K}^* \setminus \{1\}$, then for any indecomposable genuine Laurent polynomial L , either $T_2 \circ L(X) - cT_2 \circ L(Y)$ is irreducible, or $T_2 \circ L(X) - cT_2 \circ L(Y)$ is reducible with all factors having genus bigger than 1.*

Proof. By Lemma X.10, any place in $\mathbb{K}(u, v)$ has the same ramification type in $\mathbb{K}(x, v)$ and $\mathbb{K}(u, y)$, and we will this for the top square when necessary. We first study what ramification type of L makes \mathfrak{g}_{xv} and \mathfrak{g}_{uy} at most 1.

In order $\mathfrak{g}_{xv} \leq 1$, $\mathbb{K}(x)/\mathbb{K}(u)$ has to satisfy the ramification constraints in Table 7.2, where the union of the multi-sets are the collection of ramification indices of all places in $\mathbb{K}(x)$ lying over $u = \pm\sqrt{2-2c}$, therefore at least one of $v = \pm\sqrt{2-2c}$ is a branch point of $\mathbb{K}(y)/\mathbb{K}(v)$. Now consider the right square, $\mathbb{K}(y)/\mathbb{K}(v)$ also has to satisfy the ramification constraints in Table 7.2. Note that the finite branch points of $\mathbb{K}(u, v)/\mathbb{K}(v)$ are $v = \pm\sqrt{2-2/c}$, which are different from $v = \pm\sqrt{2-2c}$, so $\mathbb{K}(y)/\mathbb{K}(v)$ has at least one finite branch point which does not ramify in $\mathbb{K}(u, v)/\mathbb{K}(v)$.

Now consider the possible ramification of $\mathbb{K}(y)/\mathbb{K}(v)$. First of all, the above argument rules out all the cases where there is no additional finite branch point (except the branch points of $\mathbb{K}(u, v)/\mathbb{K}(u)$).

If the multi-sets of $\mathbb{K}(y)/\mathbb{K}(v)$ contains a index bigger than 2, then $u = 0$ is also a branch point of $\mathbb{K}(x)/\mathbb{K}(u)$ and $v = \pm\sqrt{2-2/c}$ are both branch points of $\mathbb{K}(y)/\mathbb{K}(v)$, since any place in $\mathbb{K}(u, v)$ lying over $u = 0$ should ramify the same way in $\mathbb{K}(y, u)$ as in $\mathbb{K}(x, v)$. This implies $\mathbb{K}(x)/\mathbb{K}(u)$ has at least three finite branch points ($u = 0, u = \pm\sqrt{2-2/c}$) which are not $u = \pm\sqrt{2-2c}$, but none of the cases in Table 7.2 satisfies this properties.

The final case is that the multi-sets of $\mathbb{K}(y)/\mathbb{K}(v)$ contains only 1's and 2's and there is at least one additional finite branch point, then one of such additional branch points must be $v = \sqrt{2-2c}$ or $v = -\sqrt{2-2c}$, without loss of generality, assume it is $v = \sqrt{2-2c}$. Then there are two places in $\mathbb{K}(u, v)$ lying over $v = \sqrt{2-2c}$, and they lie over $u = \sqrt{2-2c^2}$ and $u = -\sqrt{2-2c^2}$ respectively, so $u = \pm\sqrt{2-2c^2}$ are two finite branch points of $\mathbb{K}(x)/\mathbb{K}(u)$. Therefore $\mathbb{K}(y)/\mathbb{K}(v)$ have at least three additional finite branch points, namely, $v = \pm\sqrt{2-2c^2}$ and $v = \sqrt{2-2c}$, which is impossible. \square

10.2.3 The case $P = X^a(X-1)^b$

Proposition X.12. *Let $P = X^a(X-1)^b$ for some coprime integer $a, b \geq 1$ with $a+b \geq 3$. Let L be any indecomposable genuine Laurent polynomial, and let $c \in \mathbb{K}^* \setminus \{1\}$. Then it is impossible that $P \circ L(X) - cP \circ L(Y)$ is reducible with a factor of genus at most 1.*

Proof. Let $n := \deg(P)$. First of all, $P(X) = 0$ has ramification type (a^1b^1) and $P(X) = \lambda$ where $\lambda := P(a/(a+b))$ has ramification type $(1^{n-2}2^1)$.

The left and the right square must be irreducible, since otherwise by Theorem III.15, $l := \deg(L) = 2$ and $\mathbb{K}(u, v)/\mathbb{K}(u)$ has two finite branch points whose ramification indices are all even numbers. However, for $P = X^a(X-1)^b$, $\mathbb{K}(u, v)/\mathbb{K}(u)$ has no such finite branch point. Therefore, only the top square is reducible.

For the finite branch points of $\mathbb{K}(u, v)/\mathbb{K}(u)$, there are n many of type $(1^{n-2}2^1)$ (corresponding to the n simple roots of $P(X) = c\lambda$), one of type (1^ab^1) (at $u = 0$) and one of type (1^ba^1) (at $u = 1$). Consider the contribution of the finite branch points of $\mathbb{K}(x)/\mathbb{K}(u)$ to the Riemann–Hurwitz of $\mathbb{K}(x, v)/\mathbb{K}(u, v)$. Note that the finite branch points of $\mathbb{K}(x)/\mathbb{K}(u)$ contributes l to the Riemann–Hurwitz of $\mathbb{K}(x)/\mathbb{K}(u)$,

and these contributions can be carried over to $\mathbb{K}(x, v)/\mathbb{K}(u, v)$. The worst case is when the branch points are $u = 0$ and $u = 1$, where the contribution to $\mathbb{K}(x, v)/\mathbb{K}(u)$ is the least, and which is at least $al + (b - a) = al + 2n - a$. Therefore, we have $2\mathfrak{g}_{xv} - 2 \geq (-2)l + n(l - 2) + al + 2n - a$. If $\mathfrak{g}_{xv} = 0$, then $l \leq \frac{n+2a-2}{n+a-2} = 2 + \frac{2-n}{n+a-2} < 2$, which is impossible. Therefore $\mathfrak{g}_{xv} = 1$, and in this case $l \leq \frac{n+2a}{n+a-2} = 2 + \frac{4}{n+a-2}$. Therefore $l = 2, 3$ unless $n + a = 4$, where l could be 4.

If l is prime, then $l = 2$ or $l = 3$. Since the top square is reducible, by Theorem III.15 we have $\mathbb{K}(x, v) = \mathbb{K}(u, y)$, so in particular $\mathbb{K}(x, v)$ and $\mathbb{K}(u, y)$ have the same branch points in $\mathbb{K}(u, v)$ with the same ramification type at each branch point. If any finite branch point $u = \alpha$ of $\mathbb{K}(x)/\mathbb{K}(u)$ is not $u = 0$ or $u = 1$, then any simple root $X = \beta$ of $P(X) = P(\alpha)$ or $cP(X) = P(\alpha)$ yields a finite branch point $u = \beta$ of $\mathbb{K}(x)/\mathbb{K}(u)$, and then $\mathbb{K}(x)/\mathbb{K}(u)$ will have at least $2n - 2$ finite branch points; however, L can only have at most l many finite branch points, so $4 \leq 2n - 2 \leq l$, contradiction. Thus when $l = 2$ or $l = 3$, L has two finite branch points $u = 0$ and $u = 1$. If $l = 2$, since the place in $\mathbb{K}(u, v)$ over $u = 0$ and $v = 1$ have the same ramification type in $\mathbb{K}(x, v)$ and $\mathbb{K}(u, y)$, then a and b must be both odd, so we have $2\mathfrak{g}_{xv} - 2 = (-2)l + n(l - 2) + (a + 2 - \gcd(2, b)) + (b + 2 - \gcd(2, a))$, so $2\mathfrak{g}_{xv} = n$. Since $n > 2$, it is impossible that $\mathfrak{g}_{xv} \leq 1$. If $l = 3$, then $u = 0$ has type $(1^2 2^1)$ in $\mathbb{K}(x)$ but $u = 1$ has type (3^1) in $\mathbb{K}(y)$. In order the place in $\mathbb{K}(u, v)$ over $u = 0$ and $v = 1$ have the same ramification type in $\mathbb{K}(x, v)$ and $\mathbb{K}(u, y)$, we must have b is even and $3 \mid a$. Therefore we have $2\mathfrak{g}_{xv} - 2 = (-2)l + n(l - 2) + a + 2b$, so $\mathfrak{g}_{xv} = n - 2 + b/2 > 1$. Therefore, the above argument shows that l can not be 2 or 3.

The only possibility remaining is $l = 4$, and this case $n = 3$ and $a = 1$. Note that this makes $2\mathfrak{g}_{xv} - 2 \geq (-2)l + n(l - 2) + al + 2n - a$ an equality with $\mathfrak{g}_{xv} = 1$. This implies $\mathbb{K}(x)/\mathbb{K}(u)$ has only two finite branch points, and they are $u = 0$ and $u = 1$,

and the contribution of these two points to $\mathbb{K}(x, v)/\mathbb{K}(u, v)$ is $al + 2n - a = 9$. Note that the ramification types of the two finite branch points are either $\{(4^1), (1^2 2^1)\}$ or $\{(1^1 3^1), (1^1 3^1)\}$. We check each case, and find one solution, $u = 0$ has type $(1^2 2^1)$ and $u = 1$ has type (4^1) in $\mathbb{K}(x)$. In this case the place in $\mathbb{K}(u, v)$ over $u = 0$ and $v = 1$ is unramified in $\mathbb{K}(x, v)$ but totally ramified in $\mathbb{K}(y, u)$, so this case the top square is irreducible. Therefore we get no examples when $l = 4$. \square

10.2.4 The classification of genuine Laurent polynomials f where $f(X) - cf(Y)$ is reducible with a genus zero or one factor

Proposition X.13. *Let $P \in \mathbb{K}[X]$ be a polynomial of degree at least 2. Let $L \in \mathbb{K}(X)$ be any indecomposable genuine Laurent polynomial and $c \in \mathbb{K}^* \setminus \{1\}$. Let $f = P \circ L$. If $f(X) - cf(Y)$ is reducible with a factor $H(X, Y)$ of genus at most 1 then one of the following is true*

1. $P = X^4 + 4X^3 + 3(a + 3)X^2$ with $a^2 = 3$, and $c = -1$, and $\deg(L) = 2$. Let λ be a nonzero finite branch point of P then $\Lambda(L) := \{\alpha_1, \alpha_2\}$ where α_1, α_2 are the two simple roots of $P(X) - \lambda$. In this case $f(X) + f(Y)$ has two irreducible factors, each has genus 1.

2. The polynomial $P = T_n$ with $n > 3$ and $c = -1$, and let $T(X, Y, n, r) := X^2 + Y^2 - 2XY \cos(2\pi r/n) - 4 \sin^2(2\pi r/n)$. In this case $H(X, Y)$ is an irreducible factor of genus 0 or 1 of the numerator of $T(L(X), L(Y), 2n, r)$ where r is odd and one of the following holds

(1) $Br(L) = \{-2, 2, \alpha, \infty\}$ where each branch point has type $(1^1 2^1)$ and $\alpha^2 = 2(1 + \cos(\pi r/n))$. In this case $H(X, Y)$ has genus 1.

(2) $L(X) = aX + b/X + c$ where $a, b, c \in \mathbb{K}^*$ and let $\{\beta_1, \beta_2\} := \{2\sqrt{ab} + c, -2\sqrt{ab} + c\}$ be the finite branch points of L . Then $\beta_1 = 2$ or -2 . If $\beta_2^2 \neq$

$2(1 + \cos(\pi r/n))$ then $H(X, Y)$ is the numerator of $T(L(X), L(Y), 2n, r)$ and it has genus 1; otherwise $H(X, Y)$ has genus 0 and it is either of the two factors of the numerator of $T(L(X), L(Y), 2n, r)$.

3. The polynomial $P = T_n$ with $n > 3$ being odd and $c = -1$. In this case L is any indecomposable Laurent polynomial for which $F_{L,-1}(X, Y)$ has an irreducible factor of genus at most 1 and $H(X, Y)$ is the factor.
4. The polynomial $P = X^n$ with $n \geq 2$. In this case $H(X, Y)$ is a factor of $L(X) - c_1 L(Y)$ where $c_1^n = c$.

Proof. We just look at the three cases in Theorem X.5. The first case in Theorem X.5 is solved in Proposition X.12 and we get no examples. The second case in Theorem X.5 is solved in Proposition X.6, and gives the first case in this proposition. The third case in Theorem X.5 is solved in Proposition X.11 and we get no examples. The fifth case in Theorem X.5 gives the last case in this proposition. For the fourth case in Theorem X.5, note that $T_n(X) + T_n(Y)$ is a factor of $F_{T_{2n}}(X, Y)$. All these quadratic factors in $T_n(X) + T_n(Y)$ has the form $X^2 + Y^2 - 2XY \cos(\pi r/n) - 4 \sin^2(\pi r/n)$ where $0 < r < n$ and r is odd. For the quadratic factors all the possible L are given in case 3 of Theorem VII.1, where we replace $\cos(2\pi r/n)$ and $\sin(2\pi r/n)$ with $\cos(\pi r/n)$ and $\cos(\pi r/n)$. For the factor $X + Y$, then $H(X, Y)$ is an irreducible factor of genus at most 1 of $F_{L,-1}(X, Y)$. □

10.3 Decomposable case II: $f = \tilde{f} \circ X^m$

Here $\tilde{f} = \tilde{P} \circ L$ where \tilde{P} is a nonconstant polynomial and L is an indecomposable Laurent polynomial. The case when $F_{\tilde{f},c}$ is irreducible is solved in Proposition X.14. The case when $F_{\tilde{f},c}$ is reducible is solved in Proposition X.15.

10.3.1 When $F_{\tilde{f},c}$ is irreducible

Proposition X.14. *Let $c \in \mathbb{K}^* \setminus \{1\}$ and let \tilde{f} be a genuine Laurent polynomial for which $F_{\tilde{f},c}$ is irreducible. Let $m \geq 2$ and put $f := \tilde{f} \circ X^m$. If $F_{f,c}$ has an irreducible factor of genus at most 1, then $\deg(\tilde{f}) = 2$, $m = 2$ and each factor of $F_{f,c}(X, Y)$ has genus 0 or 1.*

Proof. We build the function field tower as usual where $\tilde{f}(u) = c\tilde{f}(v) = t$, $u = x^m$ and $v = y^m$.

We first deal with the case when $\deg(\tilde{f}) = 2$ and $m = 2$. Since $\mathbb{K}(x, y)$ has genus 0 or 1, then $\mathbb{K}(u, v)$ must have genus 0 or 1. In the function field tower there is no ramification in $\mathbb{K}(x, v)/\mathbb{K}(u, v)$ and $\mathbb{K}(y, u)/\mathbb{K}(u, v)$ so \mathfrak{g}_{xy} is indeed 0 or 1. This means for any genuine Laurent polynomial \tilde{f} and $c \neq 1$, each irreducible factor of $F_{f,c}(X, Y)$ must have genus at most 1.

From now on we assume $(\deg(\tilde{f}), m) \neq (2, 2)$ and we show that we will get no examples under this assumption. Note that the left and the right squares are irreducible (since 0_u is totally ramified in $\mathbb{K}(x)$ but has at least one unramified preimage in $\mathbb{K}(u, v)$, if the bottom square is reducible then the intermediate field gotten from Theorem III.15 cannot satisfy the conditions in Theorem III.16), and therefore the top square must be reducible. Note that $F_{\tilde{f},c}$ must be irreducible of genus at most 1, so the pair (\tilde{f}, c) must come from Theorem IX.6 and we will check all of them.

Let r be the total number of unramified places in $\mathbb{K}(u, v)$ over 0_u and ∞_u , then $2\mathfrak{g}_{xv} - 2 + (2 - 2\mathfrak{g}_{uv})m \geq r(m - 1)$. Note that there must be ramification between $\mathbb{K}(x, v)$ and $\mathbb{K}(u, v)$, we must have $\mathfrak{g}_{uv} = 0$. Since $\mathfrak{g}_{xv} \leq 1$, we have $2m \geq r(m - 1)$, so $r \leq \frac{2m}{m-1} = 2 + \frac{2}{m-1} \leq 4$.

Note that $r \geq n$ because there are n many places in total in $\mathbb{K}(u, v)$ lying over 0_u

and 0_v or lying over ∞_u and ∞_v , therefore $n \leq r \leq 4$. If $n = 4$ and $k = 2$ then there are 8 places in $\mathbb{K}(u, v)$ over 0_u and ∞_u , so $r \geq 8$; if $k = 1$ then similarly $r \geq 5$, both are impossible.

If $n = 3$, then $k = 1$, $r = 4$ and $m = 2$, and there is no ramification between $\mathbb{K}(x, v)/\mathbb{K}(u, v)$ except the places in $\mathbb{K}(u, v)$ over 0_u and ∞_u . However, in this case the place in $\mathbb{K}(u, v)$ lying over $u = \infty$ and $v = 0$ is unramified in $\mathbb{K}(x, v)$ but totally ramified in $\mathbb{K}(u, y)$, so the top square is irreducible, which is impossible. \square

10.3.2 When $F_{\tilde{f},c}$ is reducible

Proposition X.15. *Let $\tilde{P} \in \mathbb{K}[X]$ be a polynomial, $L \in \mathbb{K}[X, X^{-1}]$ be an indecomposable genuine Laurent polynomial and $c \in \mathbb{K}^* \setminus \{1\}$. Put $\tilde{f} := \tilde{P} \circ L$ and suppose $F_{\tilde{f},c}(X, Y)$ is reducible. Let $m \geq 2$ and put $f := \tilde{f} \circ X^m$. If $F_{f,c}(X, Y)$ has an irreducible factor $H(X, Y)$ of genus at most 1, then one of the following conditions holds:*

1. $\tilde{f}(X) = -\tilde{f}(a/X)$ for $a \in \mathbb{K}^*$. Here $H(X, Y) = XY - \beta$ (up to multiplication by a constant in \mathbb{K}^*), where $\beta^m = a$.
2. $\tilde{f}(aX) = c\tilde{f}(X)$ for some $a \in \mathbb{K}^*$ such that $c \in \langle a \rangle$. Here $H(X, Y) = X - \beta Y$ (up to multiplication by a constant in \mathbb{K}^*), where $\beta^m = a$.
3. $F_{L \circ X^m, c}(X, Y)$ has an irreducible factor of genus 0 or 1, and $H(X, Y)$ is this factor. Here one of the followings conditions holds:
 - (a) $\tilde{P} = T_n$ with $n > 3$ being odd and $c = -1$.
 - (b) $\tilde{P} = X^n$ with $n \geq 2$ and $c^n = 1$.

Proof. First of all we consider the case that \tilde{f} is indecomposable. By Proposition X.3 we have $c\tilde{f}(X) = \tilde{f}(\mu(X))$ where $\mu(Y) = aX$ or a/X for some $a \in \mathbb{K}^*$ (More

precisely either $\tilde{f}(aX) = c\tilde{f}(X)$ or $\tilde{f}(X) = -\tilde{f}(a/X)$. Therefore $H(X, Y)$ is either an irreducible factor of $X^m - \mu(Y^m)$ (where each factor has genus 0) or an irreducible factor of $F_{\tilde{f}}(X^m, \mu(Y^m))$. In the latter case since $F_{\tilde{f}}(X, \mu(Y))$ must have an irreducible factor of genus 0 or 1 so (\tilde{f}, c) must satisfy one of the conditions in Proposition X.4. Since now $F_{\tilde{f}}(X^m, Y^m)$ also has an irreducible factor of genus 0 or 1 so \tilde{f} must be one of the Laurent polynomials listed in Table 6.1, however, none of the cases in Table 6.1 is in Proposition X.4, so $F_{\tilde{f}}(X^m, \mu(Y^m))$ does not have any irreducible factor of genus at most 1.

Next we consider the case that \tilde{f} is decomposable. Note that in this case \tilde{P} is a polynomial of degree at least 2. Since $F_{\tilde{f}, c}(X, Y)$ has an irreducible factor of genus at most 1 we know $\tilde{f} = P \circ L$ satisfies one of the conditions in Proposition X.13. By Proposition VIII.1 we get no examples from case 2 in Proposition X.13. For case 3 and case 4 in Proposition X.13, we get the last case in this proposition.

Now the only case remaining is case 1 in Proposition X.13. Let r be a root of $X^m - x$, note that $\mathbb{K}(x, v)/\mathbb{K}(x)$ is unramified but $\mathbb{K}(r)$ is totally ramified over $x = 0$ and $x = \infty$, we have that $[\mathbb{K}(r, v) : \mathbb{K}(x, v)] = [\mathbb{K}(r) : \mathbb{K}(x)] = m$. Then by Riemann–Hurwitz we know $\mathfrak{g}_{rv} > 1$ when $m > 1$, therefore all factors of $f(X) - cf(Y)$ has genus bigger than 1 and we get no examples from this case. \square

BIBLIOGRAPHY

BIBLIOGRAPHY

- [1] Roberto M. Avanzi and Umberto M. Zannier. The equation $f(X) = f(Y)$ in rational functions $X = X(t)$, $Y = Y(t)$. *Compositio Math.*, 139(3):263–295, 2003.
- [2] Alex Carney, Ruthi Hortsch, and Michael Zieve. Near-injectivity of polynomial functions on number fields. *Preprint*.
- [3] Pierre Dèbes and Michael D. Fried. Integral specialization of families of rational functions. *Pacific J. Math.*, 190(1):45–85, 1999.
- [4] Gerd Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.*, 73(3):349–366, 1983.
- [5] Michael Fried. The field of definition of function fields and a problem in the reducibility of polynomials in two variables. *Illinois J. Math.*, 17:128–146, 1973.
- [6] W. K. Hayman. *Meromorphic functions*. Oxford Mathematical Monographs. Clarendon Press, Oxford, 1964.
- [7] G. Levin and F. Przytycki. When do two rational functions have the same Julia set? *Proc. Amer. Math. Soc.*, 125(7):2179–2190, 1997.
- [8] G. M. Levin. Symmetries on Julia sets. *Mat. Zametki*, 48(5):72–79, 159, 1990.
- [9] Mikhail Lyubich and Yair Minsky. Laminations in holomorphic dynamics. *J. Differential Geom.*, 47(1):17–94, 1997.
- [10] B. Mazur. Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.*, 47:33–186 (1978), 1977.
- [11] Loïc Merel. Bornes pour la torsion des courbes elliptiques sur les corps de nombres. *Invent. Math.*, 124(1–3):437–449, 1996.
- [12] Peter Müller. Permutation groups with a cyclic two-orbits subgroup and monodromy groups of Laurent polynomials. *Ann. Sc. Norm. Super. Pisa Cl. Sci. (5)*, 12(2):369–438, 2013.
- [13] Peter Müller and Michael Zieve. On the factorization of tensor products of field extensions. *Preprint*.
- [14] Rolf Nevanlinna. Einige Eindeutigkeitsätze in der Theorie der Meromorphen Funktionen. *Acta Math.*, 48(3-4):367–391, 1926.
- [15] Emile Picard. Démonstration d’un théorème général sur les fonctions uniformes liées par une relation algébrique. *Acta Math.*, 11(1-4):1–12, 1887.
- [16] A. Schinzel. *Polynomials with special regard to reducibility*, volume 77 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, 2000.
- [17] Henning Stichtenoth. *Algebraic function fields and codes*, volume 254 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, second edition, 2009.

- [18] Helmut Völklein. *Groups as Galois groups, An introduction*, volume 53 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1996.
- [19] Hexi Ye. Rational functions with identical measure of maximal entropy. *arXiv:1211.4303*.